BANCO DE PORTUGAL
EUROSISTEMA

Banco de Portugal Notice no. 1/2022

Table of Contents

Notice Text

Law no. 83/2017, of 18 August, establishes preventive and repressive measures to combat money laundering and terrorist financing, partially transposing into national law Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system and of activities and professions specifically designated for the purposes of money laundering and terrorist financing.

It also lays down the implementing measures for Regulation (EU) 2015/847 of the European Parliament and of the Council, of 20 May 2015, on information on the payer and the payee accompanying transfers of funds, in any currency, for the purposes of preventing, detecting, and investigating money laundering and terrorist financing.

Law 97/2017, of 23 August, regulates the application and enforcement of restrictive measures approved by the United Nations or the European Union and establishes the sanctioning scheme applicable to violations of these measures. Both Law no. 83/2017, of 18 August, in its Article 94, and Law no. 97/2017, of 23 August, in its Article 27, provide for the possibility of sector-specific regulation being approved, primarily aimed at adapting the duties and obligations outlined in those laws, which are of an intersectoral nature, to the specific operational realities to which they apply.

In addition to the general enabling provisions mentioned above, Law no. 83/2017, of 18 August, refers in several of its articles to the regulatory framework to be approved by sector-specific regulations, as is the case in articles 6, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 32, 33, 35, 36, 40, 41, 42, 50, 51, 52, 54, 55, 63, 65, 67, 70, 71, 72, 73, 95, 96, 120, 148, 149, 150, and 154.

Published in: the Official Gazette, 2nd Series, no. 109, of 06-06-2022

In the financial sector, it is the responsibility of the Banco de Portugal, as the supervisory authority for the prevention of money laundering and terrorist financing, to approve, as described, the regulations applicable to the financial entities subject to its supervision.

Through Notice no. 2/2018, of 26 September, the Banco de Portugal regulated Law no. 83/2017, of 18 August, in the context of the activities of the financial entities subject to its supervision. Banco de Portugal Instruction no. 2/2021, of 26 February, supplemented this scheme by outlining factors of low and high risk of money laundering and terrorist financing, as well as specific identification and due diligence measures, whether simplified or enhanced.

Law no. 58/2020, of 31 August, transposed into national law the revision of Directive (EU) 2018/843 of the European Parliament and of the Council, of 30 May 2018, to Directive (EU) 2015/849, amending and republishing Law no. 83/2017, of 18 August.

Despite the new information introduced in various aspects by Law no. 58/2020, of 31 August, it is generally considered that they do not impact the provisions of Law no. 83/2017, of 18 August, applicable to financial entities that should be subject to regulatory implementation by the Banco de Portugal.

Notwithstanding the above, the Banco de Portugal believes that the relevance of the revision of the aforementioned regulatory framework is justified by the need to: purge from the regulatory text the aspects of the scheme that became incorporated into Law no. 83/2017, of 18 August, due to the changes introduced by Law no. 58/2020, of 31 August; consolidate within a single regulatory framework the substantive rules pertaining to the prevention of money laundering and terrorism financing, by incorporating the framework currently resulting from Banco de Portugal Instruction no. 2/2021, of 26 February; to align this framework with the provisions of Banco de Portugal Notice no. 3/2020, of 15 July, which regulates internal governance and control systems and establishes the minimum standards upon which the organisational culture of entities subject to the supervision of the Banco de Portugal should be based; and, in general, and in accordance with a risk-based approach, impart greater simplicity, clarity, and flexibility to the regulatory provisions, without, however, disturbing the substance and stability of the regulatory solutions, considering the expected approval of a new European legal framework on the matter in the medium term.

This Notice repeals and replaces Banco de Portugal Notice no. 2/2018, of 26 September, and Banco de Portugal Instruction no. 2/2021, of 26 February.

This Notice was subject to public consultation, in accordance with Article 101 of the Administrative Procedure Code.

Therefore, exercising the authority granted to it by Article 17 of its Organic Law, approved by Law no. 5/98, of 31 January, by Article 94 of Law no. 83/2017, of 18 August, by Article 27 of Law no. 97/2017, of 23 August, and by Articles 30-B and 33-A of the General Framework for Credit Institutions and Financial Companies, approved by Decree-Law no. 298/92, of 31 December, all in their current wording, the Banco de Portugal determines:

TITLE I
General provisions

Article 1
Object and scope

1. This Notice, in the exercise of the powers conferred by Article 94 of Law no. 83/2017, of 18 August (the Law), regulates the conditions of exercise, the procedures, instruments, mechanisms, application formalities, reporting obligations, and other aspects necessary to ensure compliance with the preventive duties regarding money laundering and terrorist financing, as part of the activities of financial entities subject to the supervision of the Banco de Portugal.
2. In the exercise of the powers conferred by Article 27 of Law no. 97/2017, of 23 August (Law no. 97/2017), this Notice also regulates the means and mechanisms necessary for financial entities subject to the supervision of the Banco de Portugal to comply with the duties outlined in that law.
3. This Notice also regulates the measures that payment service providers adopt to detect transfers of funds where information on the payer or the payee is missing or incomplete, and the procedures they adopt to manage transfers of funds that are not accompanied by the information required by Regulation (EU) 2015/847 of the European Parliament and of the Council, of 20 May, 2015, on the information accompanying transfers of funds (Regulation (EU) 2015/847).

Article 2
Definitions

1. For the purposes of this Notice, the following definitions apply:
   a) 'Real-time monitoring' refers to the monitoring conducted before funds are made available to the payee or, if applicable, to another payment service provider, payee, or intermediary;
   b) 'Ex post" monitoring refers to the monitoring conducted after funds have been made available to the payee or, if applicable, to another payment service provider, payee, or intermediary;
   c) 'Customer' refers to any natural person, legal person, whether corporate or non-corporate, or collective interests without legal personality, who comes into contact with a financial entity for the purpose of receiving a service or

accessing a product from it, either by establishing a business relationship or executing an occasional transaction;

d) 'Collaborator' refers to any natural person who, on behalf of or in the interest of the financial entity, and under its authority or supervision, participates in the execution of any operations, acts, or procedures related to the activity pursued by that entity, regardless of whether they have an employment relationship with it (internal collaborator) or not (external collaborator);

e) 'Relevant collaborator' refers to any collaborator, whether internal or external to the financial entity, who meets at least one of the following conditions:

   i) Being a member of the governing body of the financial entity;

   ii) Holding a position that involves direct, in-person or remote, contact with the customers of the financial entity;

   iii) Holding a position within the financial entity that is related to compliance with the regulatory framework regarding the prevention of money laundering and terrorism financing;

   iv) Being qualified as such by the financial entity.

f) 'Account' refers to a bank account opened to set up one of the types of deposit provided for in Article 1 of Decree-Law no. 430/91, of 2 November, in its current wording, as well as any other payment account within the meaning of Article 2(g) of the Legal Framework for Payment Services and Electronic Money (RJSPME), approved in the annex to Decree-Law no. 91/2018, of 12 November, in its current wording;

g) 'Jumbo account' refers to an account held by the financial entity itself, which it uses on behalf of its customers or counterparties;

h) 'Financial entity' refers to one of the financial entities specified in Article 3 of the Law, provided that it is subject to the supervision of the Banco de Portugal under the terms of Articles 86 and 88 of the Law;

i) 'Jurisdictions associated with a higher risk of money laundering or terrorist financing' refers to jurisdictions that, based on the assessment of potentially higher risk factors, pose a greater risk of money laundering or terrorist financing, including 'high-risk third countries' within the meaning of Article 2(1)(bb) of the Law;

j) 'Remote means of communication' refers to any means of communication - whether by phone, electronic, telematic, or of any other kind - that allows establishing business relationships, the

executing of occasional transactions, or conducting operations in general, without the physical and simultaneous presence of the financial entity and its customer;

k) 'Pooled account' refers to an account opened by a customer to hold the funds from their customers, who do not have the authority to operate the account;

l) 'Private banking' refers to the provision of banking and other financial services to individuals with high net worth, their close family members and entities controlled by them, including asset holding vehicles or asset management vehicles ;

m) 'Representatives' refers to all individuals with decision-making powers in a business relationship or occasional transaction, including the authority to manage funds based on legal or voluntary representation, as well as agents, business managers, or any other natural or legal persons of any kind who act on behalf of or in the interests of their customers in dealings with the financial entity;

n) 'Durable medium' refers to any physical or electronic medium - optical, magnetic, or of any other kind - that has a degree of accessibility, durability, reliability, integrity, and legibility that allows for easy and permanent access to the information, the reliable and complete reproduction thereof, and the correct reading of the data contained therein;

o) 'Trade finance' refers to the provision of financing services for trade, especially used to facilitate the movement of goods at the national or cross-border level, in particular by providing financing instruments that help reduce the risks faced by importers or exporters of traded goods;

p) 'Videoconference' refers to a means of remote communication that enables identifying information of natural persons to be verified and consists of an interactive form of communication that allows for the real-time transmission and capture of audio, video, and data.

2. Notwithstanding the provisions of the preceding paragraph, the definitions contained in the Law, Law no. 97/2017, and Regulation (EU) 2015/847 shall apply to this Notice, and the concepts used in this Notice shall be interpreted in the sense attributed to them in those laws.

TITLE II

Duties

CHAPTER I

Duty of control

Article 3

Regulatory compliance monitoring function

1. Financial entities ensure the existence of a compliance monitoring function for the regulatory framework concerning the prevention of money laundering and terrorism financing (regulatory compliance monitoring function), which guarantees:
   a) The definition and effective implementation of policies, procedures, and controls appropriate to the effective management of money laundering and terrorist financing risks to which the financial organisation is or may be exposed;
   b) The financial entity's compliance with legal and regulatory standards related to the prevention of money laundering and terrorist financing.
2. The regulatory compliance monitoring function can be integrated into the compliance function as provided for in Banco de Portugal Notice no. 3/2020, of 15 July (Notice no. 3/2020).
3. When the nature, size, complexity, and risk of the activities undertaken or the quality of the controls adopted justify it, the Banco de Portugal may require that the regulatory compliance monitoring function be separated from the compliance function.
4. Without prejudice to the specific provisions of this Notice, the requirements outlined in Notice no. 3/2020 regarding the compliance function apply to the regulatory compliance monitoring function, even when this function is separated from the internal control function.
5. Financial entities may turn to the establishment of shared services for the development of responsibilities assigned to the regulatory compliance monitoring function, under the terms set out in Article 50 of Notice no. 3/2020.
6. Financial entities ensure that the selection of collaborators assigned to the regulatory compliance monitoring function is based on high ethical standards and strict technical requirements.

Article 4

Appointment of the member of the management body

1. Financial entities appoint an executive member of the governing body for the purposes of Article 13(4) of the Law, and their responsibilities include:

a) Ensuring the supervision of the regulatory compliance monitoring function and of the person responsible for it, regularly reporting to the management body on the activities carried out by them;

b) Directly monitoring the implementation of the provisions of Articles 12, 14, and 15 of the Law;

c) Ensuring that the management body receives all the necessary information in a timely manner to effectively carry out the tasks set out in Article 13(2) of the Law;

d) Proposing to the management body corrective procedures for deficiencies detected in matters relating to the prevention of money laundering or terrorist financing, ensuring the swift implementation and sufficiency of the measures approved for this purpose, and informing the management body of the progress of their execution;

e) Informing the management body of relevant interactions with the Banco de Portugal, the Financial Intelligence Unit (FIU), and other authorities with responsibilities related to the prevention of money laundering and terrorist financing;

f) Addressing, either directly or by involving the management body when necessary, the opinions and recommendations forwarded to them by the AML/CFT compliance officer, always recording in writing the reasons for not following them when applicable;

g) As provided for in Article 13(3)(b) of the Law, critically reviewing decisions not to exercise the reporting duty, reporting the results of this review to the management body at least on a monthly basis.

2. Financial entities ensure that the member of the governing body appointed to perform the functions set out in the preceding paragraph:

a) Has the necessary knowledge to fully understand the matters covered by those functions;

b) Performs these functions with the availability, decision-making autonomy, and resources necessary for their effective performance;

c) Has unrestricted and timely access to all the internal information and documentation necessary to perform those functions;

d) Performs these functions with an appropriate segregation of potentially conflicting functions, ensuring that any situations of potential conflicts of interest are identified in advance, minimised, and subject to careful and independent monitoring.

3. In the case of financial entities with a limited scope of activity and associated risks and where, due to resource limitations, it is impracticable to fully segregate the

functions outlined in paragraph 1 from potentially conflicting functions, financial entities shall identify, document, keep a record of, and implement alternative control procedures to prevent or minimise the risk of conflicts of interest occurring.

Article 5

AML/CFT compliance officer

1. For the purposes of Article 16 of the Law, financial entities appoint a person responsible for monitoring compliance with the regulatory framework regarding the prevention of money laundering and terrorist financing (AML/CFT compliance officer).
2. Without prejudice to the fulfilment of the other duties set out in Article 16(2) of the Law and in this Notice, the AML/CFT compliance officer is responsible for:
   a) Ensuring the timeliness, sufficiency, accessibility, and comprehensiveness of information about the internal control system concerning the prevention of money laundering and terrorism financing, as well as policies, procedures, and instrumental controls for its execution, which is made available to relevant collaborators of the financial entity;
   b) Supporting the preparation and execution of the assessments provided for in Article 17 of the Law and Article 9 of this Notice;
   c) Coordinating the preparation of reports and other information to be submitted to the Banco de Portugal regarding the prevention of money laundering and terrorist financing;
   d) Ensuring the immediate availability of all communications from the Banco de Portugal made under the Law, this Notice, and other regulatory provisions to all relevant collaborators of the financial entity.
3. The provisions of Article 17 of Notice no. 3/2020 also apply to the AML/CFT compliance officer, even when the regulatory compliance monitoring function is segregated from the compliance function.
4. For the purposes of Article 16(3)(a) of the Law, financial entities ensure that the AML/CFT compliance officer carries out these duties on an exclusive basis.
5. For the purposes of Article 16(9) of the Law, the AML/CFT compliance officer is considered a holder of an essential function within the meaning of Article 33-A of the Legal Framework of Credit Institutions and Financial Companies, approved by Decree-Law no. 298/92 of 31 December, in its current wording (RGICSF).

6. When the financial entity corresponds to a credit institution categorised as 'other systemically important institutions' (O-SII) in accordance with Article 138-Q of the RGICSF, Article 18 of Notice no. 3/2020 applies to the AML/CFT compliance officer.

7. Apart from the cases provided for in the preceding paragraph, when the nature, size, complexity, and risk of the activities pursued by the financial entity justifies it, the Banco de Portugal may, at the time of the incorporation project or the procedure for qualifying to conduct activities in national territory, subject the appointment of the AML/CFT compliance officer to prior authorisation by notifying the financial entity and setting a deadline for submitting the request for prior authorisation to the Banco de Portugal.

8. Apart from the cases provided for in paragraph 6, when the nature, size, complexity, and risk of the activity pursued or the quality of the controls adopted justify it, the Banco de Portugal may subject the replacement of the previously appointed AML/CFT compliance officer to prior authorisation.

Article 6

Review of the internal control system and risk management practices

1. The review of the timeliness of the policies, procedures, and controls referred to in Article 12(3) of the Law, as well as the review of the risk management practices referred to in Article 14(2)(d) of the Law, shall be carried out at intervals not exceeding 12 months.

2. The intervals for the review, either in full or in part, of the policies, procedures, and controls or practices referred to in the preceding paragraph may be extended up to 24 months, when the nature, size, and complexity of the activity pursued by the financial organisation justifies it, and the specific operational reality or the business area in question presents a lower exposure to money laundering and terrorist financing risks.

3. The review of risk management practices adopted in compliance with Article 15 of the Law also complies with the provisions of the preceding paragraphs.

Article 7

Exemption or simplification of individual risk assessments

Whenever, following sector-specific analyses of money laundering and terrorist financing risks conducted by the Banco de Portugal, sectors are identified whose nature, scope, and complexity of the activity pursued justifies it, this supervisory authority may allow for the exemption or simplification referred to in Article 14(5) of the Law and outline the respective alternative procedures, by notifying the financial entities that benefit from them.

Article 8

Information sources

1. In outlining and applying the policies, procedures and controls provided for in Article 12 of the Law, and in identifying, assessing, and mitigating the specific money laundering and terrorist financing risks referred to in Articles 14 and 15 of the Law, financial entities take into account reliable, credible, and diversified sources of information in terms of their origin and type.

2. Without prejudice to the provisions of the following paragraphs, the type and number of information sources that financial entities consider under this article shall be appropriate to their specific operating reality, taking into account, at least, the risks included in Article 14(2)(a) and Article 15 of the Law.

3. For the purpose of complying with the provisions of this article, financial entities shall consider, where applicable, the following sources of information:

   a) Information, guidelines, or alerts issued or disseminated by the Banco de Portugal;

   Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

   b) Information, guidelines or alerts from the FIU or other judicial and police authorities;

   Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

   c) Information, guidelines, or alerts issued by the government, including the Anti-Money Laundering and Counter-Terrorist Financing Coordination Committee (Coordination Committee);

   d) Information, guidelines, or alerts issued by the European Banking Authority, the Financial Action Task Force, or the European Commission;

   Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

   e) The supranational risk assessment carried out by the European Commission, the national risk assessment carried out by the Coordination Committee, and the sectoral risk assessment carried out by the Banco de Portugal and other relevant sectoral authorities;

   f) Lists of relevant functions of a political or public nature or of the respective holders issued by public bodies, including that provided for in Article 116(6) of the Law;

   g) Analyses and internal documents of financial entities, including information gathered during identification and due diligence procedures, as well as internally drawn up and updated lists and databases.

4. For the purpose of complying with the provisions of this article, financial entities shall consider, among others, the following sources of information:

a) Other information published on the Internet portal of the Coordination Committee referred to in Article 121 of the Law;

b) Independent and reliable information from civil society or international organisations, such as:

   i) Corruption indices or specific assessment reports on jurisdictions where financial entities operate;

   ii) Other publicly disclosed reports or documents about the levels of corruption and income associated with the performance of political or public functions in a specific country or jurisdiction;

   iii) Mutual assessment reports from the Financial Action Task Force;

   iv) Any other listings issued by relevant international organisations.

c) Information from the Internet and media outlets, provided it comes from independent and credible sources;

d) Information from databases, lists, risk reports and other analyses from commercial sources available on the market;

e) Official statistical data from national or international sources;

f) Relevant academic production;

g) Information provided by other financial entities or equivalent entities, to the extent legally permissible.

Article 9

Effectiveness assessment

1. For the purposes of Article 17 of the Law, financial entities ensure that periodic and independent assessments of the quality, adequacy, and effectiveness of their policies, procedures, and controls, in addition to the elements listed in Article 17(2)(e) of the Law, cover at least the following:

   a) The identification and due diligence procedures, as well as record-keeping procedures adopted, including those carried out by third parties, credit intermediaries, promoters, and other intermediation relationships;

   b) The integrity, timeliness, and comprehensibility of the reports generated by the information systems provided for in Articles 18 and 19 of the Law;

   c) The adequacy of procedures and controls for monitoring customers and transactions, whether automated, manual or a combination thereof;

d) The adequacy, scope, and timeliness of the procedures for examining and reporting suspicious transactions;

e) The financial entity's training policy, including the adequacy and scope of the training activities provided;

f) The quality, adequacy, and effectiveness of the execution of outsourced processes, services, or activities, in accordance with Article 16(7)(f) of this Notice, where applicable;

g) The timeliness and sufficiency of corrective procedures for deficiencies previously detected in audit or supervisory actions related to the prevention of money laundering or terrorist financing.

2. In order to fulfil the assessment provided for in the preceding paragraph, financial entities shall ensure the existence or outsourcing of an audit function or a duly qualified third-party entity that ensures the independence of this assessment.
3. Where the number of collaborators in the financial entity, excluding directors, is less than 30 and its operating income in the last financial year is less than €20,000,000, the assessment referred to in paragraph 1 does not have to be ensured by an internal audit function or by a duly qualified third-party entity, in which case additional monitoring procedures shall apply.
4. The assessments provided for in this article are carried out at intervals not exceeding 12 months, which may be extended to 24 months when the circumstances provided for in Article 6(2) of this Notice are met.

Article 10

Procedures and information systems in general

1. Financial entities adopt the tools or information systems provided for in Articles 18 and 19 of the Law, including the tools or information systems that are instrumental or ancillary to compliance with the obligations and duties provided for in the Law and in this Notice.
2. In order to comply with the provisions of the preceding paragraph, financial entities:

   a) Adopt information management tools or systems that consolidate records related to business relationships, occasional transactions or operations in general, whether their own or on behalf of customers, including documentary evidence collected in compliance with the duty of identification and due diligence;

b) Process information in restricted-access databases, assigning different classifications and access profiles to prevent its improper sharing or disclosure, both within the financial entity itself and with third parties;

c) Keep their databases up-to-date and fully accessible to ensure compliance with the provisions of Article 18(2)(j) of the Law.

3. Financial entities ensure that the tools and information systems provided for in Articles 18 and 19 of the Law, with the specificities set out in the preceding paragraphs, are adopted in such a way as to guarantee full and immediate access whenever requested by the Banco de Portugal.

Article 11

Specific procedures and information systems

1. For the purposes of the provisions of Article 19(2)(b) of the Law, financial entities shall consider the following sources of information, in addition to those provided for in Article 8 of this Notice, in particular paragraph 3(f), and others that are suitable to their specific operating reality:

   a) The specific information fields included in the documentation or records formalising the business relationship or occasional transaction, as well as under the updating procedures provided for in Article 45 of this Notice;

   b) Wealth control statements relating to the income and assets of holders of relevant political or public positions.

2. The procedures to be adopted for the purposes of Article 19(4)(5) of the Law shall take into account, at least:

   a) The aspects of the activity referred to in Article 14(2)(a) of the Law;

   b) The type and characteristics of the position held, namely the associated yield, the seniority and influence level, even if informal, as well as the business model or characteristics of the organisation where the position was held;

   c) The levels of corruption in the country or jurisdiction where the position was held;

   d) The existence and intensity of any link between the duties performed at the time when the procedures were carried out and the position referred to in point b) was held.

Article 12

Procedures for differentiating occasional transactions from business relationships

1. Financial entities equip their internal control systems with the means and procedures necessary to distinguish between customers engaged in occasional transactions and customers with whom they establish business relationships.
2. In cases where, regardless of any threshold or relationship, the number of transactions carried out by a customer shows a pattern of frequency and regularity, financial entities consider it to be a potentially stable and lasting relationship, classifying it as an actual business relationship thereafter, for the purpose of adopting the required identification and due diligence procedures in accordance with the Law and this Notice.

Article 13

Procedures and centralised records for occasional transactions

1. Financial entities equip their internal control systems with the means and procedures to enable them to verify the existence of seemingly related operations, as provided for in Article 23(1)(b) of the Law.
2. In outlining the means and procedures referred to in the preceding paragraph, financial entities take into account the following indicative criteria for the existence of related transactions:
   a) The parties involved and the apparent existence of relationships among them;
   b) The time elapsed between transactions;
   c) The segmentation of the amounts involved;
   d) The type and number of transactions carried out;
   e) Other criteria deemed appropriate for mitigating the specific risks identified and assessed by the financial entity, as provided for in Article 14 of the Law.
3. Without prejudice to the provisions of the preceding paragraph, financial entities always consider operations carried out by the same customer or by a group of customers recognised as related to each other within a 30-day period counted from the most recent transaction carried out by the customer or group of customers recognised as related to each other.
4. In order to ensure effective control of the two limits provided for in Article 23(1)(b) of the Law, financial entities implement a computerised and centralised record of all occasional transactions, regardless of their amount, in order to identify the splitting of operations.
5. Financial entities ensure that the record referred to in the preceding paragraph:

a) Contains, at least, the date and amount of the transaction, as well as the full name or denomination and the type and number of the identification document of the customer;

b) Is immediately updated whenever financial entities carry out an occasional transaction;

c) Is permanently available to the entire organisational structure of financial entities, as well as to their agents, distributors, and third parties with operational functions relating to payment services and the issuing of electronic money.

6. The provisions of paragraphs 4 and 5 shall not apply to exchange and re-exchange transactions with a unit value of less than €7,500 conducted outside the scope of a business relationship and which do not present an increased risk of money laundering.

7. In order to assess the risk associated with a given exchange and re-exchange transaction, financial entities take into account:

a) The exchange of coins or banknotes for higher denomination banknotes without plausible justification;

b) The exchange of banknotes for coins or banknotes of a lower denomination, when this does not fall within the scope of the customer's activity of the exchange and re-exchange transaction;

c) The purpose and amount of the exchange and re-exchange transaction, taking into account the customer's profession, commercial activity, and other information they have about the customer.

8. The obligation to update immediately referred to in paragraph 5(b) does not apply to manual exchange transactions subject to the terms and limits set out in Banco de Portugal Notice no. 13/2003, of 16 December (Notice no. 13/2003), provided that the financial entities acting as authorised entities for the purposes of said Notice:

a) Ensure that non-financial companies include, in the records referred to in paragraph 6 of Notice no. 13/2003, at least the customer identification data provided for in paragraph 5(a);

b) Access, at least on a monthly basis, the records referred to in the preceding paragraph and integrate their respective data into the centralised record provided for in paragraph 4;

c) Proceed as soon as possible to adopt the legally required identification and due diligence whenever, as a result of their aggregation, the limit set out in Article 23(1)(b)(i) of the Law is reached for a given customer;

d) Prevent non-financial companies from carrying out new manual exchange operations on their behalf until the identification and due diligence procedures are completed, without prejudice to the provisions of Article 48(2) of this Notice.

Article 14

Other centralised records

1. To prevent splitting practices with the intention of not reaching the limit specified in Article 38(1), financial entities shall also implement a computerised and centralised record of cash deposits made by third parties into accounts held by customers.
2. The record mentioned in the preceding paragraph shall contain, at least, the date and amount of the deposit, the destination account, as well as the full name or denomination and the type and number of the identification document of the third-party depositor.
3. Cash deposits made by third parties into accounts held by customers who benefit from the exemption provided for in Article 38(3) are excluded from the provisions of the preceding paragraphs.
4. Financial entities also keep a computerised and centralised record of visits made to safes by their lessees or persons authorised to access the safe, which shall include, at least, the date and time of the visit's start and end, as well as the full name and type and number of the identification document of the lessee or authorised person who made the visit.
5. For the purposes of the preceding paragraph, the definitions of 'safes', 'lessees' and 'persons authorised to access the safe' in Banco de Portugal Instruction no. 27/2020, of 26 November, shall apply.
6. The centralised records referred to in this article shall be immediately updated whenever the financial entity accepts a cash deposit from a third party or allows a visit to the safe it provides, and the data contained in the record shall be permanently available to the entire organisational structure of the financial entities.

Article 15

Duty to identify collaborators

Collaborators of financial entities who carry out the duties of identification and due diligence in accordance with the Law and this Notice, including the collection, recording, and verification of the supporting documents presented, shall make clear notations in the internal records to clearly identify themselves and the date on which they performed these actions.

Article 16

Outsourcing

Amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

1. The outsourcing of processes, services, or activities related to the compliance by financial entities with the duties laid down in the Law and in this Notice shall comply with the provisions of this article.

2. Financial entities are solely responsible for complying with the provisions of the Law and this Notice, including those related to processes, services, or activities they outsource.

3. Processes, services, or activities whose outsourcing is likely to jeopardise the quality of the measures and procedures adopted to comply with the requirements of the Law and this Notice cannot be outsourced, including the following:

   a) The approval of the financial entity's policies, procedures, and controls, as well as their revision in accordance with the provisions of Article 12 of the Law and Article 6 of this Notice;

   b) The approval of the financial entity's risk management model and its revision in accordance with the provisions of Articles 14 and 15 of the Law and Article 6 of this Notice;

   c) The outlining of characterising elements or indicators for detecting unusual or potentially suspicious conduct, activities or transactions;

   d) The fulfilment of the reporting duty laid down in Articles 43 and 44 of the Law;

   e) Other processes, services, or activities identified by the financial entity or outlined by the Banco de Portugal in a Circular Letter.

4. Financial entities are prohibited from engaging service providers established in countries with legal frameworks that include prohibitions or restrictions preventing or limiting the financial entity's compliance with legal and regulatory standards related to the prevention of money laundering and terrorist financing, including the provision and circulation of information.

5. Before outsourcing any processes, services or activities, financial entities shall:

   a) Identify, for each process, service or activity to be outsourced, the essential aspects on which the fulfilment of the duties laid down in the Law and this Notice depends;

   b) Identify and assess the specific risks of money laundering and terrorist financing associated with outsourcing these processes, services, or activities, including the risks associated with:

i) The process, service or activity to be outsourced, paying particular attention to the risks that may arise from the use of new or developing technologies;

ii) Service providers;

iii) The potential interruption or failure in the execution of the process, service or activity to be outsourced.

c) Outline and implement control tools and procedures that are suitable for mitigating the specific risks identified and assessed in accordance with the preceding paragraph, namely through the provision of contingency plans, business continuity plans, and exit strategies;

d) *(Repealed)*;

Repealed by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

e) *(Repealed)*.

Repealed by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

6. The outsourcing of processes, services or activities must be subject to prior approval from the AML/CFT compliance officer and formalised through a written contract.

7. Whenever financial entities outsource processes, services or activities, they shall:

a) Have unrestricted and immediate access to all facilities where the outsourced processes, services or activities are provided, as well as to devices, systems, networks, data, documents, personnel, records or any other information relevant to the provision of the outsourced processes, services or activities;

b) Review, with a frequency appropriate to the identified risks, the relevance of the practices referred to in paragraph 5;

Added by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

c) Ensure that they have prior knowledge of the essential aspects identified under paragraph 5(a) of this Article, including any changes in the design, configuration, or execution of the outsourced processes, services, or activities, in a manner that allows the financial entity to maintain the ultimate decision-making power regarding the outsourcing relationship;

Renumbered by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

d) Ensure that outsourced processes, services, or activities are carried out with an appropriate level of material, human, and financial resources and, where applicable, by collaborators with training in the prevention of money laundering and terrorist financing, in accordance with the provisions of Article 55 of the Law and Article 53 of this Notice;

Renumbered by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

e) Ensure the existence of contingency and business continuity plans in the event of an unplanned interruption or failure in the execution of outsourced processes, services or activities;

Renumbered by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

f) Adopt the necessary measures and mechanisms to ensure the confidentiality, security, robustness and protection of data and systems, in accordance with the Law and this Notice;

Renumbered by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

g) Document in writing the analyses carried out under this article, incorporating them into the documents or records referred to in Article 14(3)(c) of the Law.

Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

Article 17

Reporting irregularities

1. For the purposes of Article 20(7) of the Law, financial entities shall prepare an annual report containing, at least:

   a) A description of the specific, independent and anonymous channels that internally ensure the appropriate receipt, handling and filing of reports of irregularities related to potential violations of the Law, this Notice and internally established policies, procedures and controls regarding the prevention of money laundering and terrorist financing;

   b) A brief summary of the received reports and their processing.

2. Financial entities shall inform Banco de Portugal about their compliance with the obligations set out in the preceding paragraph, as set out in the Report on the Prevention of Money Laundering and Terrorist Financing, as specified in Article 83 of this Notice.

Article 18

Restrictive measures

1. To comply with the provisions of Article 21 of the Law and Article 10(3) of Law no. 97/2017, financial entities shall adopt the necessary means and mechanisms to ensure, as executing entities, compliance with the duties set out in Law no. 97/2017.

2. For the purposes of the preceding paragraph, financial entities shall have permanent, fast and secure mechanisms in place that ensure the immediate, full, and effective implementation of restrictive measures and allow, at least:

   a) The detection of any individuals or entities identified in restrictive measures;

b) The blocking or suspension of transactions or groups of transactions, when the financial entity is required to comply with freezing obligations arising from financial sanctions as referred to in Article 16 of Law no. 97/2017;

c) The existence of reliable, secure and effective communication channels and procedures that ensure the proper fulfilment of the reporting and information duties set out in Article 23 of Law 97/2017, and ensure close cooperation with the Directorate-General for Foreign Policy of the Ministry of Foreign Affairs and the Office for Economic Policy and International Affairs of the Ministry of Finance, in accordance with the provisions of Article 22 of Law 97/2017.

3. Financial entities monitor, through periodic and independent assessments, the proper functioning of the means and mechanisms implemented to ensure compliance with restrictive measures.

4. The provisions of Article 20 of the Law and Article 17 of this Notice apply to irregularities related to potential violations of Law no. 97/2017.

5. It is the responsibility of the AML/CFT compliance officer to:

a) Ensure immediate and comprehensive awareness and ongoing updates of lists of individuals and entities issued or updated under restrictive measures;

b) Continuously monitor the adequacy, sufficiency and timeliness of the means and mechanisms designed to ensure compliance with restrictive measures;

c) Comply with the obligations of prior notification, reporting and requesting prior authorisation for the execution of fund transfers, in accordance with the provisions of Article 14(2) and Article 15(1) of Law no. 97/2017;

d) Immediately implement freezing measures in accordance with the provisions of Article 16(4) of Law no. 97/2017, and record them in the cases specified in Article 16(5);

e) Fulfil the reporting and information duties laid down in Article 23 of Law no. 97/2017;

f) Fulfil the reporting duty laid down in Article 24 of Law no. 97/2017;

g) Act as the point of contact with the Directorate-General for Foreign Policy of the Ministry of Foreign Affairs and the Office for Economic Policy and International Affairs s of the Ministry of Finance, ensuring compliance with the cooperation duty laid down in Article 22 of Law no. 97/2017.

6. Compliance with the duties set out in points (c) to (f) of the preceding paragraph is outlined in a written document or record and subject to the retention duty as specified in Article 51 of the Law and Article 50 of this Notice.

7. Whenever financial entities decide not to implement restrictive measures, they shall record this in a written document or record, in accordance with the provisions of the preceding paragraph:

   a) The reasons for the decision not to implement the measures;

   b) A reference to any informal contacts that may have been established with the competent national authorities in the decision-making process, indicating the respective dates and means of communication used.

Article 19

Agents and distributors of financial entities subject to supervision by the Banco de Portugal in accordance with the RJSPME

1. Financial entities that, in accordance with the RJSPME, operate through agents or distributors and are subject to supervision by the Banco de Portugal, adhere to the provisions of the Law, this Notice, and other relevant regulations regarding the activities carried out by such agents or distributors, whether within or outside the national territory.

2. Financial entities adopt and implement the necessary procedures to ensure compatibility between the provisions of the preceding paragraph and the obligations set out in Article 22(5) of the Law concerning agents or distributors operating outside the national territory.

3. To comply with the provisions of the preceding paragraphs, financial entities:

   a) Carry out the necessary due diligence to verify the integrity and good commercial and financial reputation of agents or distributors;

   b) Provide agents or distributors with specific training in the prevention of money laundering and terrorist financing, including at least information about:

      i) The applicable legal framework;

      ii) The policies, procedures and controls related to the prevention of money laundering and terrorist financing outlined and implemented by the financial entity;

      iii) The risks, types, and methods associated with funds or other assets originating from or related to criminal activities or terrorist financing;

iv) The vulnerabilities of the business areas developed, as well as the products, services, and operations offered by the entity, along with the distribution channels for these products and services and the means of communication used with customers.

c) Continuously monitor, with unrestricted access to the necessary information, the compliance of agents or distributors with the applicable standards and procedures;

d) Establish a regular programme of visits to the facilities of agents or distributors to directly assess the extent of their compliance with obligations, followed by the preparation of assessment reports.

4. Compliance with the obligations set out in the preceding paragraph is outlined in a written document or record and subject to the retention duty as specified in Article 51 of the Law and Article 50 of this Notice.

CHAPTER II
Duty of identification and due diligence

SECTION I
Identification and standard due diligence

Article 20
Identifying information of customers and representatives

1. To comply with Article 24(1)(a)(viii) of the Law, when a natural person is unemployed or retired, financial entities also collect information about their last occupation.

2. Whenever they collect and record identifying information concerning sole proprietors, financial entities obtain the identifying information referred to in Article 24(1)(a) of the Law, as well as the following:

   a) Legal person identification number or, where it does not exist, an equivalent number issued by a foreign competent authority, without prejudice to the provisions of the following paragraph;

   b) Name;

   c) Head office;

   d) Object.

3. In cases where sole proprietors do not have a national or foreign legal person identification number, financial entities collect and record the natural person tax identification number used.

Article 21

Supporting documents related to identifying information of customers and representatives

1. Whenever the supporting documents used do not include, in the case of natural persons, any of the identifying information listed in Article 24(1)(a)(vii) to (xi) of the Law, and, in the case of legal persons or collective interests without legal personality, any of the identifying information listed in Article 24(1)(b)(v) to (viii) of the Law, financial entities may, depending on the specifically identified risk, turn to:
   a) Sources of information considered reliable, credible, and sufficient;
   b) A written statement, in hard-copy or electronic format, from the customer or their representative.
2. To comply with the provisions of Article 24(1)(b)(v) and (vi) of the Law and the provisions of the preceding paragraph, financial entities collect and record the following identifying information related to shareholders holding 5% or more of the capital and voting rights, as well as members of the governing body or equivalent body, and other relevant senior executives with management powers:
   a) In the case of natural persons:
      i) Full name;
      ii) Date of birth;
      iii) Nationality as stated on the identification document;
      iv) Type, number, expiration date, and issuing authority of the identification document;
      v) Tax identification number or, when they do not have a tax identification number, the equivalent number issued by a competent foreign authority;
   b) In the case of legal persons or collective interests without legal personality:
      i) Name;
      ii) Object;
      iii) Full address of the head office;

iv) Legal person identification number or, where it does not exist, an equivalent number issued by a competent foreign authority.

3. To prove the information referred to in the preceding paragraph, a simple written statement issued by the legal person or collective interests without legal personality is admissible.

4. To comply with the provisions of Article 24(2) of the Law, financial entities collect a simple copy, in hard copy or electronic form, of the enabling document referred to therein.

5. When checking that the identifying information specified in Article 24(1)(a)(i), (ii), (iv), (v) and (vi) of the Law is carried out using the supporting documents provided for in Article 25(2) of the Law, and these do not allow access to an image of the handwritten signature, it is considered sufficient for the purpose of verifying the signature element that the supporting document used allows for the unambiguous identification of the data subject.

6. For the purposes of the provisions of Article 25(4)(c)(i) of the Law, the procedures specified in Annex I to this Notice are also acceptable as alternative methods of verifying identifying information, as specified therein.

Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

7. The supporting documents collected by financial entities in the context of previous identification processes can be used in subsequent processes, as long as they are kept up to date, in accordance with the provisions of Article 40 of the Law and Article 45 of this Notice.

Article 22

Beneficial owners

1. Financial entities collect the supporting documents and adopt measures that, based on the specifically identified risk, they consider suitable, appropriate, and sufficient to comply with the provisions of Article 32(2) of the Law.

2. Without prejudice to measures that financial entities autonomously adopt on their own initiative, the documentation or records formalising the identification and due diligence process must contain specific information fields aimed at identifying the beneficial owners on behalf of whom customers are acting or who ultimately control the customers when they are legal persons or collective interests without legal personality.

3. Verification of the identifying information of beneficial owners under the provisions of Article 32(3) of the Law can only take place when the following cumulative conditions are met:

a) The financial entity, prior to establishing the business relationship, documents in writing the circumstances that confirm the existence of a situation of proven reduced risk, including this verification in the record referred to in Article 29(4) of the Law;

b) The information obtained in compliance with Article 33(1) of the Law raises no doubts about its timeliness and accuracy;

c) The customer is established in a low-risk country or territory, to be assessed, in particular, in accordance with Annex II to the Law, which implements mechanisms for obtaining information about beneficial owners consistent with Article 32 of the Law.

4. Financial entities immediately verify the identity of the beneficial owner, under the terms set out in Article 32(2) or 32(4) of the Law, if they become aware of any circumstance that could jeopardise the verification of a situation of proven reduced risk.

5. The provisions in paragraph 3 do not preclude the obligation to broaden the knowledge of the beneficial owner, under the terms and for the purposes of Article 29(6) of the Law.

6. For the purposes of Article 32(4)(a) of the Law, and without prejudice to other situations that are classified as such by financial entities based on internally set criteria, situations indicative of potentially higher risk provided for in the Law, namely in Annex III thereto, are particularly taken into account for the classification of an increased risk level, as well as any others specified in this Notice.

7. The provisions of Article 32(4) of the Law also apply when:

a) The supporting evidence of the quality or identity of the beneficial owner raises doubts;

b) There are suspicions of money laundering or terrorist financing, or the characterising elements specified in Article 52(2) of the Law are present;

c) The process of identifying and verifying the identity of the beneficial owner is carried out through third-party entities, under the terms and for the purposes of Article 41 of the Law and Article 46 of this Notice.

8. The provisions of Article 21(7) of this Notice also apply to the verification of the identity of beneficial owners.

Article 23

Purpose and nature of the business relationship

1. The information regarding the purpose and intended nature of the business relationship obtained in compliance with Article 27(a) of the Law is proven by the customer or the financial entity through the collection of supporting documents and the adoption of measures that, based on the specifically identified risk, it deems suitable, appropriate, and sufficient whenever at least one of the following situations occurs:

   a) Increased risk level associated with the business relationship;

   b) The supporting documents raise doubts as to their content or suitability, authenticity, timeliness, accuracy, or sufficiency.

2. For the purposes of the provisions set out in point a) of the preceding paragraph, and without prejudice to other situations that may be classified as such by financial entities according to internally established criteria, particular consideration is given to the classification of an increased risk level, at least, in situations indicative of potentially higher risk as provided for in the Law, especially in Annex III thereto, as well as any others specified in this Notice.

3. Financial entities verify the information regarding the purpose and intended nature of the business relationship, as provided in paragraph 1, concerning business relationships whose purpose and nature have not yet been verified, whenever the circumstances mentioned in that provision arise subsequent to the establishment of the business relationship.

4. Whenever financial entities ascertain that the transactions conducted during the course of the business relationship are inconsistent with the knowledge they possess regarding the purpose and nature of the business relationship or the risk profile of the customer, they adopt enhanced identification and due diligence measures appropriate to the increased risk level associated with the business relationship.

Article 24

Source and destination of funds

1. For the purposes of Article 27(b) of the Law and the assessment to be made by financial entities to the need to obtain information about the source or destination of funds handled as part of a business relationship or when carrying out an occasional transaction, particular consideration is given to, among other internally set aspects:

   a) Situations indicative of potentially higher risk provided for in the Law, namely in Annex III thereto, as well as any others specified in this Notice;

b) The characterising elements specified in Article 52(2) of the Law;

c) Indicators of suspicion of money laundering or terrorist financing identified by the Banco de Portugal.

2. Information on the source and destination of the funds is:

a) Provided with the level of detail appropriate to the specifically identified risk;

b) Verified through the collection of supporting documents and the adoption of measures that, based on the specifically identified risk, financial entities deem to be suitable, appropriate, and sufficient.

3. Whenever, during the course of the business relationship or subsequent occasional transactions, financial entities find that the transactions carried out prove to be inconsistent with the information previously obtained regarding the source or destination of funds or the customer's risk profile, they adopt enhanced identification and due diligence measures appropriate to the increased risk level associated with the business relationship or the transaction.

Article 25

Activity characterisation

1. To comply with the provisions of Article 27(c) of the Law, financial entities:

a) Before establishing a business relationship, collect information about the main characterising elements of their customers' actual activity, namely information about its nature, level of income, or turnover generated, as well as the countries or geographical areas associated with it;

b) During the continuous monitoring of the business relationship, expand their knowledge of the elements mentioned in the preceding paragraph, considering, for this purpose, among other internally outlined aspects:

i) The risk specifically identified during the course of the business relationship;

ii) The regularity or duration of the business relationship;

iii) Situations indicative of potentially higher risk provided for in the Law, namely in Annex III thereto, as well as any others specified in this Notice;

iv) The characterising elements specified in Article 52(2) of the Law;

v) Indicators of suspicion of money laundering or terrorist financing identified by the Banco de Portugal.

2. The information referred to in the preceding paragraph is verified through the collection of supporting documents and the adoption of measures that, based on the specifically identified risk, financial entities deem to be suitable, appropriate and sufficient.

3. Whenever financial entities ascertain that the transactions conducted during the course of the business relationship are inconsistent with the knowledge they possess regarding the customer's activities or risk profile, they adopt enhanced identification and due diligence measures appropriate to the increased risk level associated with the business relationship.

Article 26

Deferred verification of identifying information and limits on the movement of funds

1. For the purposes of Article 26(3) of the Law, financial entities only enter into a business relationship when, cumulatively, they are provided with:

   a) All the identifying information specified in Articles 24 and 32 of the Law, as well as in Article 20 of this Notice, applicable to the specific case;

   b) The supporting documents referred to in Article 24(1)(a)(i) to (vi) and Article 24(1)(b)(i) to (iv) and (vi) of the Law.

2. To comply with the provisions of Article 26(3)(d) of the Law, financial entities establish and adopt limits on the number and amount of permitted operations, as well as on the type of products, services, transactions, and distribution channels made available, without prejudice to the provisions of the following paragraphs.

3. For the purposes of Article 26 and Article 65, both of the Law, any changes of ownership are prohibited until the identity verification process is completed.

4. For the purposes of Article 65 of the Law, the identity of the customer and the beneficial owner is deemed to be verified when the information referred to in paragraph 1 is provided to the financial entity, and any debit transactions on the account or associated payment instruments are prohibited until the identity verification process is completed.

5. When the initial deposit into the account is made in cash or using another untraceable payment method that makes it impossible to identify the payer, financial entities do not allow any debit or credit transactions to take place after such initial deposit until the identity verification process is completed.

6. When it comes to establishing business relationships aimed at acquiring payment instruments dissociated from an account that allow fund transfers, financial entities do not allow any transactions made in cash or using another untraceable payment method that makes it impossible to identify the payer

to take place after such initial funding until the identity verification process is completed.

7. For the purposes of Article 26(4) of the Law, the provision of supporting evidence proving the identifying information must take place within a maximum period of 60 days from the date on which the identifying information was first collected and recorded.

8. Financial entities immediately terminate the business relationship if the identity verification process is not completed within the time frame specified in the preceding paragraph, in full compliance with the provisions of Article 50 of the Law and Article 49 of this Notice.

Article 27

Adequacy to the risk level

1. In compliance with the provisions of this Chapter, financial entities take into account the information sources specified in Article 8 of this Notice, especially the European Supervisory Authority Guidelines that establish simplified and enhanced identification and due diligence measures, as well as other factors to be considered when adopting the following procedures:

   a) Assessing, weighing and managing the risk of money laundering and terrorist financing associated with business relationships and occasional transactions;

   b) Outlining the scope of the measures to be adopted under the duty of identification and due diligence, based on the specifically identified risk.

2. Whenever, in accordance with Article 28 of the Law, the risk analysis conducted by financial entities regarding the business relationship or occasional transaction justifies an increased level of knowledge about the customer, their representative, or the beneficial owner, the entities:

   a) Request additional information or elements to the extent appropriate to the specifically identified risk;

   b) To the extent appropriate to the specifically identified risk, they also require a higher level of verification of the identifying information and details obtained, particularly concerning information whose verification does not depend on documentary evidence.

SECTION II

Simplified and enhanced measures

SUBSECTION I

General provisions

Article 28

Factors and types indicative of money laundering and terrorist financing risk

1. For the purposes of Article 35(3) of the Law, when analysing the risks of money laundering and terrorist financing that may lead to the adoption of simplified measures, financial entities consider:
   a) Regarding situations indicative of potentially lower risk listed in Annex II to the Law, the aspects listed in Annex II to this Notice;
   b) The factors and types indicative of potentially lower risk listed in Annex III to this Notice.
2. For the purposes of Article 36(5) of the Law, when analysing the risks of money laundering and terrorist financing that may lead to the adoption of enhanced measures, financial entities consider, in addition to the situations indicative of potentially higher risk listed in Annex III to the Law, the factors and types indicative of potentially higher risk listed in Annex IV to this Notice.
3. When analysing the risks of money laundering and terrorist financing in accordance with the Law and this Notice, financial entities also consider other situations, factors and types indicative of risk that are appropriate to their specific operating reality.
4. Without prejudice to the cases expressly provided for in the Law and in this Notice, the isolated presence of the factors and types indicative of risk referred to in the preceding paragraphs does not necessarily result in the automatic assignment of a high or low risk level to the business relationship or occasional transaction.
5. When weighting risk factors, financial entities ensure that:
   a) Economic or profit-related considerations do not influence the risk rating;
   b) The weighting does not lead to a situation where it is impossible for any business relationship or transaction to be classified as high risk;
   c) Automatic risk rating is subject to manual review;

d) The decision to manually review automatically assigned risk ratings is always substantiated and is the responsibility of the AML/CFT compliance officer or another collaborator of the financial entity who is not directly involved in the business relationship with the customer, under the supervision of the AML/CFT compliance officer.

6. The assessments, procedures, and measures outlined under this Section are documented in writing and integrated into the documents prepared by financial entities in compliance with Article 12(4) and Article 14(3)(c), both of the Law, in a manner that demonstrates their adequacy in detail, and are also subject to the duty of retention in accordance with the provisions of Article 51 of the Law and Article 50 of this Notice.

SUBSECTION II

Simplified Measures

Article 29

General provisions

1. For the purposes of Article 35 of the Law, financial entities document, in writing:

   a) Assessments and analyses that identify the existence of situations with proven low risk;

   b) The specific content of the simplified measures to be adopted for each of the situations referred to in the preceding paragraph.

2. Whenever simplified measures are applied, financial entities:

   a) Obtain sufficient identifying information to comply with the applicable identification and due diligence procedures, even if simplified;

   b) In addition to the monitoring provided for in Article 35(7) of the Law, and without prejudice to the provisions of Article 27(2) of this Notice, they adopt mechanisms that allow for the continuous verification of the maintenance of a proven low risk of money laundering and terrorist financing.

3. In addition to the provisions of Article 35(4) of the Law, the following are considered examples of simplified measures:

   a) The verification of the identification of the customer and the beneficial owner after the establishment of the business relationship, in accordance with Article 26 of this Notice, without demonstrating that this is necessary for the normal course of business;

   b) The mere collection of information that should not be included in the identification documents of natural persons, legal persons, or collective interests without legal personality;

c) The inference of the customer's activity or profession from the purpose or type of the business relationship established or the transaction carried out.

4. The provisions of this Subsection do not prevent financial entities from adopting simplified measures other than those provided for in the Law and in this Notice, provided that they are communicated to the Banco de Portugal, separately from any report, at least 30 days before their application, and the Banco de Portugal may adopt risk management measures that fall within the scope of its supervisory powers.

Article 30

Specific schemes

1. For the purposes of Article 35(6) of the Law, financial entities may adopt the simplified measures set out in Articles 31 to 33 of this Notice, provided that the specific assumptions set out therein are verified and the other applicable obligations set out in the Law and this Notice are complied with.

2. The extension of the services or products provided by the financial entity to the customer, beyond those covered by the simplified measures set out in Articles 31 to 33 of this Notice, does not require the establishment of a new business relationship, but it does call for the application of the identification and due diligence procedures required under the Law and this Notice, prior to the provision of new services or products.

Article 31

Credit operations

1. Without prejudice to the use of the supporting documents referred to in Article 25(2) and (4)(c) of the Law, in the contracting of credit operations using remote means of communication, for an amount equal to or less than € 50,000, financial entities may verify the identifying information referred to in Article 24(1)(a)(i) to (vi) of the Law, by collecting plain copies of the original identification documents, in hard copy or electronic format, provided that, cumulatively:

   a) The borrowed capital is transferred to an account held by the borrower, whenever the credit operation is dissociated from the immediate payment of a good or service;

   b) The borrower designates an account in their name for payments or repayments of the borrowed capital in a financial entity headquartered or with a branch in a Member State of the European Union or in a third country that offers identical guarantees of fund traceability, and provides proof of ownership through mechanisms to be outlined by the financial entity;

c) They take appropriate additional measures to fully verify the identifying information, in particular by consulting public databases or using certificates that allow the borrower to be uniquely identified;

d) The risk associated with those credit operations is not considered relevant by financial entities.

2. The mechanisms and additional measures provided for in points b) and c) of the preceding paragraph:

a) Are outlined by the financial entity's AML/CFT compliance officer, based on a prior and reasoned opinion from them demonstrating their suitability to the risk of the credit operations usually carried out by the financial entity;

b) Are documented in writing for each credit relationship.

3. For the purposes of paragraph 1(d), and without prejudice to other situations that are classified as such by financial entities based on internally established criteria, the situations indicating a potentially higher risk provided for in the Law, namely in Annex III thereto, as well as any others contained in this Notice, are given particular consideration for the classification of an increased risk level.

4. Under the terms of this article, whenever the borrower chooses to make payments or repayments through an account held by a person other than the borrower, the financial entity requests a justification for this choice.

5. Financial entities analyse and reassess the risk associated with the business relationships established under the terms of this article and consider the application of enhanced identification and due diligence measures whenever, during the course of the business relationship, they identify:

a) Situations where the funds made available are not used or are used for purposes other than those initially indicated;

b) Situations involving cash payments, the use of other untraceable payment methods, or payments made through an account held by a person other than the borrower without proper justification being provided.

Article 32

Payment initiation services and account information services

1. When contracting the payment initiation and account information services referred to in Article 4(g) and (h) of the RJSPME, financial entities collect and record the full name or denomination of the customer, their representatives, and beneficial owners, as well as the following identifying information:

a) In the case of natural persons:

i) Type, number, expiration date and issuing authority of the identification document; or

ii) Tax identification number or, when they do not have a tax identification number, the equivalent number issued by a competent foreign authority.

b) When they are legal persons, the legal person identification number or, where it does not exist, an equivalent number issued by a competent foreign authority.

2. The application of the provisions in the preceding paragraph can only take place when the following conditions are met:

a) When providing payment initiation services, the financial entity adopts mechanisms to ensure that payment operations are initiated with payment service providers headquartered or establishments in a Member State of the European Union or in a third country where there is a regulatory and supervisory framework compatible with the provisions of the Law and this Notice;

b) When providing account information services, the financial entity adopts mechanisms that allow:

i) Accessing data from at least one account held by the customer with payment service providers headquartered or established in a Member State of the European Union or in a third country where there is a regulatory and supervisory framework compatible with the provisions of the Law and this Notice; and

ii) Ensuring knowledge of the capacity in which the customer operates the accounts associated with them whenever a new account is added to the account information service.

Article 33

Electronic money

Financial entities may apply the scheme provided for in paragraph 1 of the preceding article to the provision of services related to the use of electronic money, whenever the following conditions are cumulatively met:

a) The services provided to the customer by the financial entity are limited to electronic money products that meet all the conditions specified in paragraph 2(1) of Annex II to this Notice;

b) The funds used to purchase or top up the electronic money product originate from an account domiciled with a financial entity headquartered or established in a Member State of the European Union or in a third country where there is a regulatory and supervisory framework compatible with the provisions of the Law and this Notice.

SUBSECTION III

Enhanced measures

Article 34

General provisions

1. In accordance with the provisions of Article 36(1) to (3) of the Law, financial entities adopt, in addition to those provided for in the Law, the enhanced measures set out in the following articles.
2. The provisions of the preceding paragraph do not preclude the adoption of other enhanced measures outlined by financial entities under the scheme provided for in Article 36(4) of the Law.
3. For the purposes of adopting enhanced measures, financial entities establish different levels of high risk that reflect their specific operating reality, including at least the aspects set out in Article 14(2)(a) of the Law, and review them in accordance with the provisions of Article 6 of this Notice.

Article 35

Customers, representatives, and beneficial owners

1. For the purposes of Article 36(6)(a) of the Law, examples of specific measures to obtain additional information about customers, their representatives, or beneficial owners include the collection of information about:
   a) The source and legitimacy of the assets;
   b) The legitimacy of the funds involved in the business relationship or occasional transaction;
   c) Their reputation;
   d) Close family members and persons recognised as closely associated;
   e) Previous activities;
   f) The number, size and frequency of transactions expected to be carried out as part of the business relationship.
2. Whenever they carry out additional due diligence to verify the information obtained, as provided for in Article 36(6)(b) of the Law, financial entities use independent and credible sources of information, outlining their type and number based on the authenticity guarantees they offer and the specifically identified increased risks.
3. When verifying the source of assets, financial entities consider the use of the following supporting documents:
   a) Income statements and, where applicable, wealth control statements;
   b) Financial statements reports or legal certification of accounts;

c) Pay stubs;

d) Certificates from public records;

e) Document proving inheritance acquisition;

f) Publicly available information, including from the media, provided it comes from an independent and credible source.

4. In situations of increased risk where the customer, their representative or the beneficial owner have any connection to other jurisdictions, financial entities obtain at least information about:

a) The relationships with those jurisdictions;

b) The presence of associated persons who may influence their transactions;

c) In cases where they have their headquarters or domicile in another jurisdiction, the reason for wanting to establish a business relationship or carry out an occasional transaction outside their home jurisdiction.

5. In addition to reducing the time interval for updating information as provided for in Article 36(6)(e) of the Law, financial entities shall carry out a reanalysis of the risk and other elements associated with business relationships to which a higher risk rating has been assigned at least annually.

6. For the purposes of this article, the definitions of 'close family members' and 'persons recognised as closely associated' as provided for in Article 2(1)(w) and (dd) of the Law, respectively, are applicable, as the case may be, in reference to any customer, representative, or beneficial owner, even if they have not been identified as a 'politically exposed person' or 'holder of other political or public function.

Article 36

Product, service, transaction or distribution channel

1. Whenever they identify a situation of increased risk associated with a product, service, transaction or distribution channel, financial entities consider adopting the following measures:

a) Limiting the number or amount of permitted transactions;

b) Limiting the use to certain jurisdictions;

c) Limiting the use to certain types of customers;

d) Limiting or restricting cash transactions;

e) Requirement for conducting deposit, top-up, redemption or reimbursement transactions through traceable means, such as an account opened with a financial entity or another legally authorised entity that, not being located in a high-risk third country, demonstrably applies identification and due diligence measures compatible with those provided for in the Law and in this Notice;

f) Parameterisation of specific alerts in accordance with the risk assigned to the product, service or transaction, by outlining and applying rules to adjust the risk of the product, service or transaction when associated with high-risk customers.

2. Financial entities adopt enhanced measures whenever new products, services or distribution channels pose increased risks of money laundering or terrorist financing, including the involvement of top management in approving their marketing or use.

Article 37

Geographic location

Whenever they identify jurisdictions associated with a higher risk of money laundering or terrorist financing that are relevant to certain business relationships or occasional transactions, financial entities adopt the following measures:

a) Gathering additional information about the jurisdiction in question, in particular on the relevant regulatory framework and the existence of supervision compatible with the provisions of the Law and this Notice;

b) Enhancing the depth or frequency of monitoring procedures, as provided for in Article 36(6)(d) of the Law, particularly considering the source and destination of transactions.

Article 38

Cash deposits made by third parties

1. Without prejudice to the provisions of Article 23(1) of the Law, in the case of cash deposits made by third parties into accounts held by customers, financial entities verify the name of the depositor and the type, number, expiry date, and issuing authority of their identification document whenever the amount to be deposited is equal to or greater than €10,000.

2. In the cases provided for in the preceding paragraph, financial entities obtain information about the relationship between the third-party depositor and the beneficiary account holder, documenting or recording this information in writing and retaining it in accordance with the terms set out in Article 51 of the Law and Article 50 of this Notice.

3. In the case of cash deposits into accounts held by sole proprietors, individual limited liability establishments, or legal persons of a corporate nature, financial entities may waive the application of the procedures set out in paragraph 1 when the deposits are made into accounts held by a customer who, based on their internally established criteria, are classified as having a proven reduced risk.

4. For the purposes of this article, members of the governing bodies of the account holder, those who hold management positions, those who work as directors or managers, their employees, agents, and other individuals who provide services to them on a permanent, temporary, or occasional basis, including activities related to the transportation, custody, processing, and distribution of funds and assets as outlined in Article 3(1)(d) of Law no. 34/2013, of 16 May, are not considered third-party depositors or representatives.

Article 39

Jumbo accounts

Financial entities that use jumbo accounts guarantee the traceability of any transaction to or from that account in a manner that allows for the identification of the source and destination of the funds underlying each transaction, as needed.

Article 40

Pooled accounts

1. In addition to adopting all required identification and due diligence procedures, financial entities treat as beneficial owners the customers of the customer holding a pooled account, taking identification and identity verification measures in accordance with the specifically identified risk.

2. Whenever they identify a situation of increased risk associated with the use of pooled accounts, financial entities consider adopting the following measures:

   a) Obtaining additional information when fulfilling the supplementary procedures set out in Article 27 of the Law, as stipulated in Article 36(6)(a) of the same law;

   b) The involvement of higher hierarchical levels to authorise the establishment of the business relationship, as provided for in Article 36(6)(c) of the Law;

   c) Intensifying the depth and frequency of procedures for monitoring the business relationship or certain operations, sets of operations, or products provided, as provided for in Article 36(6)(d) of the Law;

d) Monitoring the follow-up of the business relationship, as provided for in Article 36(6)(f) of the Law.

Article 41

Private banking

1. Whenever they provide private banking services, financial entities adopt enhanced measures proportional to the existing risks.
2. For the purposes of the preceding article, financial entities adopt at least the following measures:
   a) Obtaining additional information when fulfilling the supplementary procedures set out in Article 27 of the Law, as stipulated in Article 36(6)(a) of the same law;
   b) The involvement of higher hierarchical levels to:
      i) Authorise the establishment of the business relationship, in accordance with Article 36(6)(c) of the Law;
      ii) Approve the risk assessment associated with the business relationship and subsequent revisions.
   c) Reduce the time interval for updating information, in accordance with Article 36(6)(e) of the Law;
   d) Monitor the follow-up of the business relationship, in accordance with Article 36(6)(f) of the Law;
   e) Re-analyse the risk and other elements associated with business relationships that are assigned a higher risk rating, on at least an annual basis.
3. Financial entities also consider adopting the following measures:
   a) The requirement that cash deposits and deposits of other valuables be made in person and over the counter;
   b) Intensifying the depth and frequency of monitoring procedures, as provided for in Article 36(6)(d) of the Law, namely by defining thresholds that trigger specific analyses;
   c) Real-time analysis and monitoring of transactions;
   d) Obtaining additional information about complex business structures, such as trust funds or private investment vehicles, ensuring that they are used for legitimate purposes and that the identity of their beneficial owners is known.

Article 42

Trade finance

1. Whenever they provide trade finance services, financial entities adopt enhanced measures proportional to the existing risks.
2. For the purposes of the preceding article, financial entities adopt at least the following measures:
   a) Obtaining, in accordance with Article 36(6)(a) of the Law, additional information about:
      i) Customers, their representatives, and beneficial owners;
      ii) Planned or executed transactions;
      iii) The counterparties to commercial transactions.
   b) The involvement of higher hierarchical levels to:
      i) Authorise the establishment of the business relationship, in accordance with Article 36(6)(c) of the Law;
      ii) Approve the risk assessment associated with the business relationship and subsequent revisions.
3. For the purposes of point a) of the preceding paragraph, specific examples of measures to obtain additional information include the collection of information about:
   a) The jurisdictions in which the customer operates;
   b) The existence of exchange controls or restrictions on the outflow of foreign currency in jurisdictions where the customer operates;
   c) The trade routes used, including jurisdictions of source, destination, and transit of the goods, as well as the ships, ports, airlines, shipping companies, and carriers used;
   d) The goods traded, especially dual-use goods or goods that are at odds with the declared economic activity;
   e) Buyers, suppliers, insurance companies, agents, and other third parties involved in the trade, as well as their geographic locations.
4. When verifying the information obtained in accordance with the preceding paragraphs, financial entities consider the use, among others, of the following supporting documents:
   a) Publicly available information, particularly from the International Maritime Bureau and free container tracking services provided by shipping companies;

b) Obtaining external opinions on whether the pricing of goods is commercially rational, especially for traded goods for which current and credible price information can be obtained;

c) Checking whether the weights and volumes of the goods to be shipped are compatible with the shipping method.

Article 43

Measures to be taken by the correspondent in the context of correspondent banking relationships

1. For the purposes of Article 70(1) of the Law, and in addition to the measures set out in that article, financial entities:

   a) In the context of providing payable-through accounts)**:**

      i) For the purposes of Article 70(1)(f)(i) of the Law, they ensure that the respondents verify the identity of the customers who have direct access to the accounts, as well as their representatives and beneficial owners, in identical terms as those provided for in the Law and in this Notice;

      ii) They identify and document in writing the specific risks associated with using the payable-through account, including demonstrating that the execution of transactions without direct access to the account is not sufficient to serve the purposes of the business relationship;

      iii) They outline, document in writing and implement specific and enhanced monitoring procedures for the business relationships in question, in a manner that allows, in particular, the management of the specifically identified risks and the identification of the holders of ultimate control over the account.

   b) In the context of the indirect use of the correspondence relationship by other entities providing financial services who intend to rely on the respondent to carry out transactions and access financial services through the correspondent (nested activity)):

      i) They obtain information and assess the risk related to the existence and operations carried out as part of correspondent relationships dependent on the respondent, taking into account, in particular, the size, geographic location, type of customers and services offered;

      ii) They ensure the completeness and transparency of messages and payment orders in a manner that allows for the verification of all parties involved in transactions on behalf of correspondent relationships dependent on the respondent;

      iii) They assess the respondent's controls to manage the risk associated with the nested activity;

iv) They implement mechanisms for the detection of undeclared nested activities and for the subsequent execution of the necessary follow-up measures to identify any elements characterising suspicion;

v) They document in writing the actions outlined in the preceding sub-paragraphs.

c) They periodically review the effectiveness of the policies, procedures, and internal controls outlined and adopted by the respondent to prevent money laundering and terrorist financing, adopting the frequency and verification techniques based on the specifically identified risk and ensuring, in any case, the completeness and transparency of messages and payment orders.

2. When assessing the specific risk associated with the correspondent relationship, including for the purposes of Article 70(6) of the Law, financial entities, without prejudice to the sources of information provided for in Article 8 of this Notice and the other aspects considered during the normal and enhanced identification and due diligence procedures, particularly consider the following factors:

a) The jurisdiction in which the respondent is located;

b) The group to which the respondent belongs, as well as the jurisdictions of the respective subsidiaries and branches;

c) The management and control structure of the respondent, including their beneficial owners;

d) The presence of politically exposed persons in the structures referred to in the preceding paragraph;

e) The reputation, main business areas, customer base, target market segments and jurisdictions in which the respondent operates;

f) The risks associated with the specific services to be provided to the respondent by the correspondent;

g) The likelihood of the practices outlined in points a) and b) of the preceding paragraph occurring, and in particular, the accessibility of information regarding any third parties who may use the services of the correspondent.

3. Financial entities apply, *mutatis mutandis*, the measures provided for in Article 70 of the Law and in this article as part of business relationships they establish with the entities referred to in Article 2(1)(l) of Banco de Portugal Notice no. [•]/2022, of [•] [•]»

Text amended by Notice no. 1/2023, published in the Official Gazette, Series II, Part E, no. 17, of 24-01-2023.

Article 44

Measures to be taken by the respondent in the context of correspondent banking relationships

1. For the purposes of Article 71(2)(a) of the Law, the following types of operations, at least, are considered to be of high risk:
   a) Fund transfer operations, as set out in Article 2(s) of the RJSPME;
   b) Other fund transfer transactions involving non-banking entities domiciled outside the national territory.
2. When identifying other high-risk situations in accordance with the provisions of Article 71 of the Law, financial entities especially consider the following factors:
   a) The jurisdictions involved in the payment chain;
   b) The complexity of the payment chain and the clearing systems used between the entities authorised to provide financial services within that chain;
   c) The nature, size and number of the parties involved in the payment chain, as well as the jurisdictions in which they operate;
   d) The technology used to transmit information and process transactions in the payment chain;
   e) The volume and amount of transactions conducted or to be conducted.
3. For the purposes of Article 71(1)(b) of the Law, financial entities ensure that, throughout the payment chain, entrusted funds are always traceable and identifiable in relation to other funds belonging to other entities or intended for purposes other than the processing of fund transfers.

SECTION III

Obligation to update

Article 45

Information update

1. The provisions of Article 40(1) of the Law also apply to the information and supporting documents obtained in compliance with this Notice, which are contained in a written document or record and are subject to the duty of retention as stipulated in Article 51 of the Law and Article 50 of this Notice.
2. In addition to the situations listed in Article 40(4) of the Law, financial entities also promptly carry out the necessary information update procedures as referred to in the preceding paragraph whenever they become aware of the occurrence of at least one of the following facts related to the customer, their representative, or the beneficial owner:

a) Change in the management body;

b) Change in the nature of the activity or business model;

c) Expiration of the validity period of identification documents.

3. In the contractual clauses governing their relationships with customers, financial entities expressly include the obligation for customers to notify them of any changes made to their identifying information or other information provided at the beginning or during the course of the business relationship.

SECTION IV

Contracting with other entities

Article 46

Execution of identification and due diligence procedures by third-party entities

1. In accordance with the provisions of Article 41(1) of the Law, financial entities may use a third-party entity to carry out identification and due diligence procedures, provided that the latter is:

a) One of the entities provided for in Article 3(1) of the Law;

b) An entity of a nature equivalent to the entities specified in the preceding paragraph, headquartered abroad;

c) A branch, established in national territory or abroad, of the entities specified in the preceding paragraphs;

d) One of the entities referred to in Article 3(3)(a) of the Law.

2. Without prejudice to the provisions of Article 41(4) of the Law, financial entities are also prohibited from using third-party entities established in countries with legal systems that provide for prohibitions or restrictions that prevent or limit the financial entity's compliance with legal and regulatory standards concerning the prevention of money laundering and terrorist financing, including the provision and circulation of information.

3. In addition to the provisions of Article 41(6) of the Law, whenever they turn to the execution of identification and due diligence procedures by third-party entities, financial entities ensure that:

a) Third-party entities have:

i) An adequate internal control system to prevent money laundering and terrorist financing;

ii) The necessary human, material and technical resources to carry out identification and due diligence procedures either in person or through remote communication methods, as appropriate.

b) The identification and due diligence procedures are conducted by employees of the third-party entity with appropriate training in the prevention of money laundering and terrorist financing, in accordance with the provisions of Article 55 of the Law and Article 53 of this Notice;

c) The internal records supporting the identification and due diligence procedures carried out by the third-party entity clearly identify the third-party entity, the employee who performed them and the date of their execution.

4. For the purposes of Article 42 of the Law, financial entities may use the third-party entities mentioned in paragraph 1 that are part of the same group.

Article 47

Credit intermediaries

1. Identification and due diligence procedures can be carried out through the credit intermediaries referred to in Article 3(j) of Decree-Law no. 81-C/2017 of 7 July, in its current wording.

2. The execution of identification and due diligence procedures by credit intermediaries is provided for in the contractual clauses governing the relationships between the financial entity and the credit intermediary.

3. Whenever they use credit intermediaries to carry out identification and due diligence procedures, financial entities ensure that:

a) Credit intermediaries carry out the identification and due diligence procedures that the financial entities themselves adhere to, in accordance with the provisions of the Law and this Notice;

b) The internal records supporting the identification and due diligence procedures carried out by credit intermediaries clearly identify the intermediary and, if applicable, the employee who performed them, as well as the date of their execution;

c) Credit intermediaries send, in hard copy or electronic form, the information obtained during the execution of identification and due diligence procedures as soon as possible, but before the funds are made available by the lender, without prejudice to paragraph 6.

4. For the purposes of paragraph 3(a), financial entities:

a) Transmit to credit intermediaries the internal identification and due diligence procedures that they adhere to, in accordance with the provisions of the Law and this Notice;

b) Provide credit intermediaries with specific information on the prevention of money laundering and terrorist financing.

5. Compliance with the obligations stipulated in the preceding paragraph is documented in written records and is subject to the duty of retention as provided for in Article 51 of the Law and Article 50 of this Notice.

6. When the conditions set out in Article 26(3) of the Law and Article 26 of this Notice are met, or when the simplified measures referred to in Article 35(4)(a) of the Law and Article 29(3)(a) of this Notice are applied, the information obtained during the execution of identification and due diligence procedures can be sent after the funds have been made available by the lender, but no later than 60 days after the date on which the identifying information was first collected and recorded.

7. The information sent by credit intermediaries in accordance with paragraph 3(c) is always analysed by financial entities to verify its sufficiency, suitability and aptitude, and it is up to the latter to complete the information collected by the credit intermediaries or conduct a new identification process in cases where the information is insufficient, inappropriate or when there are doubts about the supporting documents used, or when the associated risk justifies it.

8. In cases where a credit intermediary repeatedly fails to strictly comply with the provisions of paragraph 3(c), either regarding the timing of information transmission or its content, financial entities consider terminating the contractual relationship established with that intermediary, including the conclusions of such consideration in a written document or record.

9. Financial entities are solely responsible for the exact compliance with the identification and due diligence procedures carried out by credit intermediaries, as if they were performed directly by the financial entities themselves.

Article 48

Promoters and other intermediary relationships

1. The provisions of the preceding article apply, in accordance with and subject to the limitations of their respective activities, to obtaining information through the following individuals or entities:

   a) Promoters referred to in Banco de Portugal Instruction no. 11/2001, of 15 June;

   b) Non-financial companies that engage in manual exchange activities in an accessory and limited manner, as provided for in Notice no. 13/2003;

   c) Other individuals or entities that, under the legal or regulatory framework applicable to financial entities, provide some form of intermediation between them and their customers.

2. In the case of manual currency exchange transactions carried out through non-financial companies authorised for this purpose, compliance with the duty of identification and diligence is only required when the aggregation of transactions for a given customer reaches the limit specified in Article 23(1)(b)(i) of the Law, without prejudice to the need to comply with the other procedures set out in Article 13(8) of this Notice.

CHAPTER III
Other duties

Article 49
Duty of refusal

1. In the situations provided for in Article 50(2) and (3)(b) of the Law, financial entities, once the decision to terminate the business relationship has been made:
   a) Prohibit any movement of funds or other assets associated with the business relationship, including through any remote means of communication;
   b) Contact the customer within a maximum of 30 days, so that the customer can specify the account to which the funds should be returned or personally appear before the financial entity to effect the return in accordance with paragraphs 3 and 4;
   c) Hold the funds or other assets, keeping them unavailable until they can be returned.
2. If the customer, when contacting the financial entity, provides the missing information that led to the decision to terminate the business relationship, and there is no suspicion, the financial entity can re-establish the relationship by conducting all legally required identification and due diligence procedures, without prejudice to the provisions of Article 21(7) of this Notice.
3. Without prejudice to the provisions of the following paragraph, the refund of funds referred to in Article 50(6) of the Law is made by financial entities through one of the following means:
   a) Transfer to an account opened by the customer with a financial or other legally authorised entity that, not being located in a high-risk third country, demonstrably applies identification and due diligence measures compatible with those specified in the Law and this Notice, explicitly indicating the reason for the transfer in the accompanying message;
   b) A crossed and non-negotiable cheque drawn on the financial entity in favour of the customer, with an explicit mention of the reason for payment on the cheque;
   c) Another admissible means, with the possibility of refunding the funds in cash if the customer proves not to have an account with a financial or other legally authorised entity that meets the requirements specified in point a).

4. In the situations specified in Article 26(8) of this Notice, financial entities make the refund referred to in the preceding paragraph using the same means that were used for the initial delivery of funds if it was made in cash or another non-traceable payment method.
5. Any documentation provided upon the termination of the business relationship or the refund of the respective funds or other assets must include an explicit mention of the reason for the action.
6. Where the coordination referred to in Article 50(3)(d) of the Law takes place, financial entities consult the competent judicial and law enforcement authorities before proceeding with any refund of funds or other assets under this article.
7. Financial entities, when terminating a business relationship based on the existence, according to internally outlined criteria, of an increased risk of money laundering or terrorist financing that does not constitute a legal basis for exercising the duty of refusal, comply, *mutatis mutandis*, with the following provisions of:
   a) Article 50(3)(c) and (d) and (4) of the Law;
   b) Paragraphs 3 to 6 above, and in these cases, the mentions referred to in paragraph 5 are not included.

Article 50

Duty of retention

All documents, records, and analyses collected or prepared in the context of compliance with this Notice are subject to the duty of retention as stipulated in Article 51 of the Law.

Article 51

Duty of examination

1. In the situations specified in Article 52(4) of the Law, financial entities also include, as completely as possible, in the document or record referred to in that provision, the information listed in Article 44(1)(c)(i) to (iii) of the Law, along with the reasons that support the absence of specific suspicion factors.
2. The Banco de Portugal disseminates and updates, by means of a Circular Letter, an illustrative list of potential indicators of suspicion, listing behaviours, activities or transactions that may be related to funds or other assets that originate from criminal activities or are related to terrorist financing.

Article 52

Duty of non-disclosure

To comply with the duty of non-disclosure laid down in Article 54 of the Law, financial entities ensure that contacts with customers relating to the communications specified in paragraph 1 of said article are conducted, whenever appropriate and proportionate, in coordination with the AML/CFT compliance officer and, whenever necessary, with the competent judicial or law enforcement authorities.

Article 53

Duty of training

1. Financial entities outline and implement a training policy appropriate for the purposes set out in Article 55(1) and (2) of the Law, aimed at ensuring comprehensive, ongoing, and up-to-date knowledge about, among other aspects:
   a) The regulatory framework applicable to the prevention of money laundering and terrorist financing;
   b) The policies, procedures and controls related to the prevention of money laundering and terrorist financing outlined and implemented by the financial entity;
   c) Guidelines, recommendations and information issued by judicial authorities, law enforcement authorities, supervisory authorities or associations representing the sector;
   d) The risks, types and methods associated with funds or other assets originating from or related to criminal activities or terrorist financing;
   e) The vulnerabilities of the business areas developed, as well as the products, services and operations offered by the entity, along with the distribution channels for these products and services and the means of communication used with customers;
   f) Reputational risks and the administrative consequences resulting from failure to comply with the duties to prevent money laundering and terrorist financing;
   g) Specific professional responsibilities regarding the prevention of money laundering and terrorist financing and, in particular, the policies, procedures and controls associated with compliance with preventive duties.
2. For the purposes of Article 55(3) of the Law, the training provided to newly hired collaborators is appropriate to their experience and professional qualifications and covers, at least, the following aspects:

a) The basic principles and concepts of preventing money laundering and terrorist financing;

b) The fundamental principles of the financial entity's internal control system and the policies, procedures and controls instrumental to its implementation;

c) The main risks and elements characterising suspicion associated with each business area of the financial entity, in terms that enable collaborators to recognise, from the start of their functions, any behaviours, activities or transactions whose characteristics make them susceptible to being related to funds or other assets originating from criminal activities or related to terrorist financing.

3. The records referred to in Article 55(5) of the Law contain, at least, the following information on internal or external training activities that have been conducted:

a) Name;

b) Date of completion;

c) Training entity;

d) Duration (in hours);

e) Nature (internal or external training);

f) Environment (face-to-face or remote training);

g) Supporting educational materials;

h) Name and position of trainees (internal and external);

i) Final evaluation of trainees, when applicable.

CHAPTER IV
Own transactions

Article 54
Own transactions

1. For the purposes of Article 63 of the Law, financial entities fully comply with the duties to prevent money laundering and terrorist financing laid down in the Law and this Notice, concerning their own transactions and their respective counterparties.

2. Financial entities establish and implement procedures for the prevention of money laundering and terrorist financing with regard to their relationships with counterparties, ensuring, at least:

a) That they do not engage in acts that could result in their involvement in any money laundering or terrorist financing operations, adopting all appropriate measures to prevent such involvement, as provided for in Article 11(3) of the Law;

b) That they obtain the necessary information from the counterparty to adequately manage the risk of money laundering and terrorist financing, with the possibility of applying simplified customer due diligence measures with respect to their counterparties, in accordance with Article 35 of the Law and Article 29 of this Notice;

c) Compliance with the duties of examination, communication, abstention, collaboration and non-disclosure;

d) The adoption of additional measures to monitor the counterparty and transactions that are proportional to the specifically identified risk.

3. For the purposes of subparagraph b) of the preceding paragraph, situations indicative of potentially reduced risk include, among others that may be identified by financial entities or the Banco de Portugal, the following:

a) Relationships established with entities authorised to provide financial services headquartered or established in a Member State of the European Union or in a third country where there is a regulatory and supervisory framework compatible with the provisions of the Law and this Notice;

b) Transactions in markets with adequate guarantees of transparency regarding information about beneficial owners and the formal ownership of counterparties;

c) Transactions between entities that are part of the same group, provided there are no restrictions on the circulation of information and it can be obtained to respond to requests received by the competent authorities;

d) Operations established with counterparties unrelated to the provision of financial services, including outsourcing relationships provided for in Article 16 of this Notice.

4. Financial entities cease to adopt simplified measures as soon as they become aware of any element characterising suspicion or any other circumstance that may increase the risk of their counterparties or transactions, in which case they adopt all the required identification and due diligence procedures, whether normal or enhanced, depending on the specifically identified risk, in accordance with the Law and this Notice.

5. Whenever financial entities become aware that a natural or legal person intends to hold a qualifying holding in them, as set out in Article 2-A(ee) of the RGICSF, financial entities, prior to the capital injection:

a) Obtain verified information about the source of the funds;

b) Identify the beneficial owners of the proposed acquirers.

6. Compliance with the obligations stipulated in this article is documented in written records and is subject to the duty of retention as provided for in Article 51 of the Law and Article 50 of this Notice.

TITLE III

Integrated mutual agricultural credit system

CHAPTER I

Duty of control

Article 55

Establishing the common internal control system

1. The Caixas de Crédito Agrícola Mútuo (CCAMs) that are part of the Integrated Mutual Agricultural Credit System (SICAM) outline and adopt, in coordination with Caixa Central de Crédito Agrícola Mútuo (Caixa Central), a common internal control system for the prevention of money laundering and terrorist financing, in accordance with Article 67 and Article 12, both of the Law.

2. Caixa Central and the CCAMs ensure the proper and effective implementation of the common internal control system, ensuring:

   a) The effective management of the money laundering and terrorist financing risks to which each CCAM, individually, and the SICAM, in general, may be or may become exposed;

   b) Compliance by Caixa Central and the CCAMs with legal and regulatory standards on the prevention of money laundering and terrorist financing.

3. For the purposes of the preceding paragraph, Caixa Central and the CCAMs ensure, in particular:

   a) That the degree of intervention, attribution and distribution of responsibilities of Caixa Central and each CCAM are in compliance with the provisions of this Title;

   b) The effective implementation of the tools or information systems adopted in compliance with Articles 18 and 19, both of the Law;

   c) The existence of direct, secure and confidential communication channels between Caixa Central's AML/CFT compliance officer and the AML/CFT compliance officers of the CCAMs;

   d) The establishment of formal systems and processes for collecting, processing and archiving information to support analysis and decision-making by relevant internal structures, particularly in relation to customer and transaction monitoring and the

examination of potential suspicions, as well as the exercise of the duty of communication, in accordance with the different responsibilities of the CCAMs and Caixa Central as provided for in this Title.

4. Caixa Central establishes the information to be reported by the CCAMs to Caixa Central and how this information is reported and subsequently processed by Caixa Central.

5. Without prejudice to the provisions of the preceding paragraph, the CCAMs immediately report to Caixa Central any anomalies detected in the exercise of their responsibilities regarding the prevention of money laundering and terrorist financing.

6. Caixa Central, in compliance with Article 12(3) of the Law, reviews, with a frequency appropriate to the existing risks, not exceeding the period stipulated in Article 6 of this Notice, the adequacy of the policies, procedures, and controls outlined in this article.

7. For the purposes of the preceding paragraphs, and in compliance with Article 12(4) of the Law, Caixa Central is responsible for preparing the written document that outlines the set of policies, procedures, and controls for preventing money laundering and terrorist financing, and the degree of intervention, attributions, and responsibilities, both exclusive and common, of Caixa Central and each CCAM in compliance with these policies, procedures, and controls.

8. The provisions of this article do not prejudice the compliance by Caixa Central and the CCAMs with the other legal and regulatory provisions related to internal control to which they may be subject.

Article 56

Responsibility of the governing body

1. The governing body of Caixa Central is responsible for approving and ensuring the implementation of policies, procedures, and controls for the prevention of money laundering and terrorist financing, in compliance with the provisions of Article 13(1) and (2)(a) of the Law and this Title.

2. The governing body of Caixa Central is responsible for:

   a) Appointing the AML/CFT compliance officer of Caixa Central, as provided for in Article 16 of the Law, providing them with the necessary means and resources for their respective function, in compliance with the legally established requirements;

   b) Monitoring the activities of other members of the senior management of Caixa Geral, to the extent that they oversee business areas that are or may be exposed to money laundering and terrorist financing risks;

c) Establishing direct contacts with the management of the CCAMs, in order to be informed about the monitoring of the business areas developed by their structure, which are or may be exposed to money laundering and terrorist financing risks;

d) Periodically monitoring and evaluating the effectiveness of the policies, procedures, and controls outlined for the SICAM, ensuring that the appropriate measures are taken to correct any deficiencies detected;

e) Complying with Article 13(3) of the Law regarding exercise of the duties of examination and communication within the SICAM, promoting the re-analysis of the critical review referred to in Article 68(3) of this Notice, whenever the governing body of the CCAM involved decides to maintain the decision not to report.

3. The governing body of each CCAM is responsible for:

a) Appointing the AML/CFT compliance officer of the CCAM, as provided for in Article 16 of the Law, providing them with the necessary means and resources for their respective function, in compliance with the legally established requirements;

b) Monitoring the activities of other members of the senior management of the CCAM they manage, to the extent that they oversee business areas that are or may be exposed to money laundering and terrorist financing risks;

c) Ensuring that the CCAM they manage provides the necessary cooperation to Caixa Central and acts in accordance with the procedures and controls outlined by the latter;

d) Refraining from any behaviour that may harm or diminish the guarantees of independence of the AML/CFT compliance officer of the CCAM they manage, especially as provided for in Article 13(3)(a) of the Law;

e) Preparing the critical review provided for in Article 68(3) of this Notice, concerning the exercise of the duty of examination by the CCAM they manage.

Article 57

Risk management

1. In compliance with Article 14 of the Law, Caixa Central identifies the specific risks of money laundering and terrorist financing inherent in the operational reality of the SICAM as a whole.

2. Caixa Central outlines and adopts the means and control procedures that are appropriate for mitigating the specific risks identified and assessed, adopting and promoting the adoption by the CCAMs of especially enhanced procedures when there is an increased risk of money laundering or terrorist financing.

3. Whenever Caixa Central identifies CCAMs exposed to specific risks other than those identified for the SICAM as a whole, it adopts and promotes the adoption, by the CCAMs in question, of the means and control procedures that are appropriate for mitigating such risks.
4. For the purposes of the preceding paragraphs, the CCAMs are responsible for:
   a) Identifying the specific risks of money laundering and terrorist financing inherent to their specific operating reality, including the risks mentioned in Article 14(2)(a) and Article 15, both of the Law;
   b) Reporting the results of the assessment to Caixa Central, within the deadlines and at the intervals established by the latter;
   c) Adopting the risk control and mitigation procedures outlined by Caixa Central.
5. To comply with points a) and b) of the preceding paragraph, Caixa Central outlines the risk identification forms that will be filled out and reported by the CCAMs.
6. Unless otherwise determined by the Banco de Portugal, and without prejudice to the provisions of paragraph 3, Caixa Central may exempt CCAMs from carrying out the individual risk assessments provided for in this article and ensure the risk assessment for the SICAM as a whole, if the specific risks inherent to the CCAMs' sector of activity are clearly identified and understood.
7. Pursuant to the provisions of Article 14(2)(d) of the Law, Caixa Central reviews, at intervals appropriate to the identified risks, not exceeding those provided for in Article 6 of this Notice, the currency of the risk management practices, so that they adequately reflect any changes that may have occurred in the specific operating reality of the SICAM as a whole and the CCAMs in particular, as well as the risks associated with this reality.

Article 58

AML/CFT compliance officer

1. Caixa Central and CCAMs ensure:
   a) The existence of direct, secure and confidential communication channels appropriate to the exercise of the functions of the AML/CFT compliance officers of the CCAMs and Caixa Central;
   b) Unrestricted and timely access by the AML/CFT compliance officer of Caixa Central to all relevant information from the CCAMs, in accordance with the common internal control system implemented.
2. The AML/CFT compliance officer of Caixa Geral is responsible for:

a) Participating in outlining and issue prior opinions on policies and controls aimed at preventing money laundering and terrorist financing in the SICAM, in accordance with the provisions of Article 16(2)(a) of the Law;

b) Monitoring, on an ongoing basis, the adequacy, sufficiency, and currency of the policies, procedures, and controls for the prevention of money laundering and terrorist financing for the SICAM, proposing necessary updates, in accordance with the provisions of Article 16(2)(b) of the Law;

c) Participating in the outlining, monitoring, and evaluation of the SICAM's internal training policy, in compliance with the provisions of Article 16(2)(c) of the Law;

d) Ensuring the centralisation of all information from the various business areas of the SICAM and all relevant information from the CCAMs, in compliance with Article 16(2)(d) of the Law;

e) Fulfilling, with regard to the SICAM, the role of interlocutor provided for in Article 16(2)(e) of the Law;

f) Ensuring the immediate provision to all relevant collaborators of the SICAM of the communications made by the Banco de Portugal under the Law and this Notice and other regulatory provisions.

3. The AML/CFT compliance officers of the CCAMs collaborate with Caixa Central, providing all requested information immediately.

Article 59

Effectiveness assessment

1. Caixa Central ensures compliance with Article 17 of the Law and Article 9 of this Notice, and is responsible for monitoring the quality, suitability, and effectiveness of the policies, procedures, and controls regarding the prevention of money laundering and terrorist financing established for the SICAM.

2. Whenever deficiencies are detected under the provisions of the preceding paragraph, Caixa Central adopts and promotes the adoption by the CCAMs, as soon as possible, of the corrective measures necessary to remedy the identified deficiencies.

3. For the purposes of the preceding paragraphs, the CCAMs are responsible for:

a) Implementing the corrective measures indicated to them by Caixa Central;

b) In the event that the identified deficiencies individually affect a specific CCAM, and whenever requested by Caixa Central, responding to any questions or issuing an opinion on such deficiencies.

Article 60

Technical, material and human resources

1. Caixa Central and the CCAMs ensure that they have the technical, material, and human means and resources necessary to ensure the proper functioning of the common internal control system, as well as to fulfil their legal and regulatory obligations regarding the prevention of money laundering and terrorist financing, in particular those arising from this Title and the written document referred to in Article 55(7) of this Notice.
2. Caixa Central includes in the assessment provided for in article 59 of this Notice an analysis, prepared in close coordination with the AML/CFT compliance officer, of the adequacy of the technical, material and human means and resources of the CCAMs.
3. Whenever Caixa Central detects any deficiencies in the analysis provided for in the preceding paragraph, it requests the CCAMs concerned to correct them.
4. The CCAMs correct the deficiencies in technical or human means or resources detected by Caixa Central, so as not to jeopardise the functioning of the common control system and the prevention of money laundering and terrorist financing.

Article 61

Preparation of reports and supervisory reporting

1. Caixa Central is responsible for submitting the report provided for in Article 83 of this Notice, containing aggregated information relating to the SICAM.
2. Unless otherwise determined by the Banco de Portugal, the CCAMs are not required to individually submit the report provided for in Article 83 of this Notice, without prejudice to their obligation to provide Caixa Central with all the necessary information for carrying out the reporting duty on behalf of the SICAM.

Article 62

Reporting irregularities

Taking into account the specificities of the SICAM's common internal control system, Caixa Central is responsible for outlining and implementing specific channels for reporting the irregularities provided for in Article 20 of the Law, ensuring that such irregularities are reported to the supervisory body of the CCAM in question and to Caixa Central's supervisory body.

Article 63

Restrictive measures

1. Caixa Central is responsible for outlining the necessary means and mechanisms, taking into account the specificities of the SICAM's common internal control system, to ensure compliance with the provisions of Article 21 of the Law and Article 18 of this Notice by the SICAM.
2. The CCAMs are responsible for implementing all the means and mechanisms outlined by Caixa Central under the provisions of the preceding paragraph.

CHAPTER II

Other duties

Article 64

Duty of identification and due diligence

1. The CCAMs are responsible for complying with the duty of identification and due diligence.
2. When establishing and monitoring a business relationship, conducting occasional transactions and operations in general, as well as updating information and supporting documents previously obtained, the CCAMs carry out the procedures and apply the tools and information systems, under the terms established by Caixa Central.
3. Caixa Central is responsible for:
    a) Promoting the completeness and updating of the information collected by the CCAMs whenever it becomes aware, through information collected by itself or by a CCAM other than the one that performed the initial identification and due diligence procedures, of additional identifying information;
    b) Promoting the completeness of the information collected by the CCAMs or ensuring that a new identification is made whenever it detects any insufficiency in the information or means of proof used, or when the associated risk justifies it;
    c) Outlining and ensuring the consistent implementation by CCAMs of the procedures adopted under Articles 27 and 28 of the Law, and Articles 23, 24, 25, and 27 of this Notice;
    d) Outlining for the SICAM as a whole the situations that may warrant the application of simplified or enhanced measures for identification and due diligence, as well as the specific content of admissible measures, under the terms of Articles 35 and 36 of the Law, and Articles 29 and 34 of this Notice;
    e) Ensuring that the information collected during the identification and due diligence procedures is recorded and centralised in the implemented information systems, so as to ensure proper management of the risks to which the SICAM is exposed;

f) Ensuring that the SICAM has access to the information mentioned in the preceding paragraph, namely through the implemented information systems, to the extent that such access is relevant for the CCAMs to comply with their specific obligations.

4. Caixa Central ensures that the procedures and information systems implemented in the SICAM are loaded and parameterised with information collected by Caixa Central and each CCAM, in order to, in particular:

   a) Keep updated lists of politically exposed persons, close family members, persons recognised as being closely associated, holders of other political or public positions, persons subject to restrictive measures, persons identified in determinations by sectoral authorities, or other qualifying aspects of customers that may be relevant in the prevention of money laundering and terrorist financing;

   b) Ensure their uniform implementation by the CCAMs during the execution of identification and due diligence procedures.

5. Caixa Central outlines the update procedures to be applied to the SICAM in accordance with the provisions of Article 40 of the Law and Article 45 of this Notice, ensuring:

   a) That the information provided for in Article 40(1) of the Law can be updated at any CCAM;

   b) That the SICAM has access to the information collected during the update procedures, namely through the implemented information systems, to the extent that such access is relevant for the CCAMs to comply with their specific obligations.

6. The procedures referred to in compliance with the preceding paragraph are detailed in the written document referred to in Article 55(7) of this Notice.

7. Based on their individual assessment of the risk of money laundering or terrorist financing, the CCAMs may apply additional enhanced measures and notify Caixa Central's AML/CFT compliance officer of this decision.

8. Whenever, as a result of the communication provided for in the preceding paragraph, Caixa Central's AML/CFT compliance officer identifies risks that affect more than one CCAM or the SICAM as a whole, they establish the adoption of additional measures and their respective prerequisites in the CCAMs concerned or in the SICAM as a whole, as the case may be.

Article 65

Reporting duty

1. Caixa Central is responsible, with respect to the SICAM as whole, for reporting suspicious operations as provided for in Articles 43 and 44 of the Law, immediately informing the CCAMs involved of the decision to report.
2. The preceding paragraph covers the reporting of operations whose suspicion arises from direct monitoring by Caixa Central, as well as operations identified by the CCAMs and reported to Caixa Central in accordance with the provisions of this title.
3. Caixa Central gathers and collates all available information from the CCAMs and the SICAM, which is required under Articles 43 and 44 of the Law, and immediately forwards the relevant information to the competent authorities.
4. Caixa Central is responsible for complying with the duty of retention laid down in Article 43(3) of the Law.

Article 66

Duty of abstention

1. Caixa Central and the CCAMs, as part of their respective duties, are responsible for complying with the duty of abstention laid down in Article 47 of the Law.
2. In compliance with the provisions of Article 47(2) of the Law, in case of abstention from carrying out an operation or a set of operations, Caixa Central must notify the competent authorities of the operation in accordance with the provisions of the preceding article.
3. The exercise of the duty of abstention by the CCAMs does not require prior assessment by Caixa Central, although, whenever it does not hinder the efficient exercise of the duty, the AML/CFT compliance officer may be consulted beforehand.
4. Without prejudice to paragraph 6, Caixa Central is responsible for the queries and communications with the FIU and the Central Department for Investigation and Penal Action of the Attorney General's Office (DCIAP) provided for in Article 47(3) and (5) of the Law and for complying with the provisions of paragraph 6 of the same article.
5. For the purposes of the preceding paragraph, Caixa Central gathers and collates all the relevant information available from the CCAMs and the SICAM.
6. Whenever a CCAM deems that abstention is not possible, in accordance with Article 47(3) of the Law, it immediately informs Caixa Central of this fact, together with the reasons referred to in Article 47(6)(a) of the Law.
7. Whenever the execution of the operations mentioned in Article 47(5) of the Law depends on the actions of a CCAM, Caixa Central informs that CCAM of the expiration of the deadline or the DCIAP's decision.

8. Caixa Central is responsible for complying with the duty of retention laid down in Article 47(7) of the Law.

Article 67

Duty of refusal

1. Caixa Central and the CCAMs, as part of their respective duties, are responsible for complying with the duty of refusal laid down in Article 50 of the Law and Article 49 of this Notice.
2. The exercise of the duty of refusal by the CCAMs does not require prior assessment by Caixa Central, although whenever it does not hinder the efficient exercise of the duty or whenever it is necessary to liaise with the competent authorities, Caixa Central's AML/CFT compliance officer may be consulted beforehand.
3. Whenever, in the exercise of the duty of refusal, Caixa Central's regulatory compliance office has not been consulted, the CCAMs immediately notify Caixa Central of the exercise of the duty, including, for this purpose, the conclusions set out in Article 50(4)(a) and (b) of the Law.
4. For the purposes of Article 50(3)(d) of the Law, Caixa Central liaises with the competent judicial or law enforcement authorities.
5. Without prejudice to the provisions of the preceding paragraphs, and taking into account the provisions of Article 50(3) of the Law, as well as their duties and responsibilities in the common internal control system, Caixa Central may instruct the CCAMs to:
   a) Refrain from initiating business relationships, conducting occasional transactions or carrying out other operations;
   b) Terminate a business relationship whenever the specifically identified risk of money laundering and terrorist financing cannot be managed in any other way.
6. Whenever the analysis of the exercise of the duty of refusal leads to a report to the competent authorities, this is done in accordance with article 65 of this Notice.
7. Caixa Central is responsible for complying with the duty of retention laid down in Article 50(5) of the Law.

Article 68

Duty of examination

1. Caixa Central is ultimately responsible for complying with the duty of examination laid down in Article 52 of the Law and Article 51 of this Notice.

2. Whenever a CCAM detects the presence of characterising elements regarding a particular conduct, activity or operation, it immediately informs Caixa Central's AML/CFT compliance officer, providing all available information along with a preliminary report prepared by the CCAM's AML/CFT compliance officer, which contains an assessment of the existence of suspicions of money laundering or terrorist financing and concludes whether or not to report suspicious operations.
3. If the conclusion of the preliminary analysis provided for in the preceding paragraph is not to report, the critical review referred to in Article 13(3)(b) of the Law, prepared by the governing body of the CCAM involved, is added.
4. Any additional information requested by Caixa Central from the CCAMs as part of the exercise of the duty of examination is obtained and provided immediately.
5. Caixa Central takes the necessary measures to ensure the completeness of the duty of examination and informs the CCAMs involved of the outcome thereof.

Article 69

Duty of collaboration

1. Whenever, under the terms and for the purposes of Article 53 of the Law, the competent authorities address requests to the CCAMs regarding information that is centralised by Caixa Central, under the terms of this Title, Caixa Central may either respond directly to these requests or collect the requested information and prepare the corresponding response, which should be promptly sent by the requested CCAM while maintaining the full content of the information sent to it.
2. Whenever the requests for information mentioned in the preceding paragraph are answered directly by the CCAMs, they inform Caixa Central of the response sent.
3. Whenever, under the terms of paragraph 1, Caixa Central responds directly to the competent authorities, it informs the CCAM concerned of the response sent.
4. Without prejudice to the provisions of the following paragraph, communications from the Banco de Portugal addressed to entities integrated into the SICAM are sent to Caixa Central and replied to by the latter.
5. The provisions of the preceding paragraph do not preclude the possibility of the Banco de Portugal addressing communications directly to the CCAM in question whenever it deems it appropriate.

Article 70

Duty of training

1. Caixa Central is responsible for complying with the duty of training laid down in Article 55 of the Law and Article 53 of this Notice.

2. The CCAMs are responsible for ensuring the participation and presence of their collaborators in the specific and regular actions ensured by Caixa Central under the provisions of this article, in particular newly hired collaborators whose duties are directly relevant to the prevention of money laundering and terrorist financing.

Article 71

Coordinating competencies and sharing information

1. Regarding situations that are not specifically regulated in this Title, it is the responsibility:
   a) Of Caixa Central and the CCAMs, as part of their respective duties, to comply with the obligations aimed at preventing money laundering and terrorist financing laid down in the Law, this Notice, and other relevant regulations, namely as part of the duties of retention and non-disclosure;
   b) Of Caixa Central to outline the necessary means and mechanisms, taking into account the specificities of the SICAM's common internal control system, to ensure the proper compliance by Caixa Central and the CCAMs with these obligations.
2. In assessing non-compliance with the responsibilities assigned to Caixa Central under this Title, the compliance of the CCAMs with the provisions of Article 67(2) of the Law, this Notice, and other relevant regulations will always be taken into account.
3. Caixa Central ensures the coordination of the SICAM as a whole, sharing the information provided by one CCAM with another CCAM or with the SICAM as a whole whenever this proves necessary for the prevention of money laundering and terrorist financing.
4. For the purposes of the preceding paragraph, AML/CFT compliance officers of the CCAMs report to Caixa Central's AML/CFT compliance officer any information relevant for the prevention of money laundering and terrorist financing, namely information about customers, conducts, activities or transactions.
5. All information exchanged between the entities integrated into the SICAM, if this duty does not already result from another applicable rule, is documented in writing and retained in accordance with general terms.

Article 72

Specific duty of Caixa Central

When the establishment of the business relationship or the execution of a occasional transaction is carried out directly with Caixa Central, in person or through remote means of

communication, Caixa Central complies, *mutatis mutandis*, with the obligations outlined for the CCAMs in this Title.

TITLE IV

Activities carried out in Portugal by financial entities headquartered abroad

Article 73

Agents and distributors

1. The payment institutions and electronic money institutions referred to in Article 3(2)(b) and (c) of the Law, with regard to activities carried out in national territory, comply with the provisions of the Law, this Notice, and other relevant regulations.
2. For the purposes of Article 72(2)(a) of the Law, and without prejudice to the provisions of paragraphs 3 and 4 of this Article, the institutions referred to in paragraph 1:
   a) Appoint a member of the governing body responsible for ensuring compliance with the regulatory framework in force in Portugal with regard to the prevention of money laundering and terrorist financing, as provided for in Article 4 of this Notice;
   b) Appoint a AML/CFT compliance officer who carries out, exclusively or, where available, in coordination with the central contact point referred to in paragraph 5, the duties provided for in Article 16 of the Law, Article 5 of this Notice, and the other relevant regulatory provisions.
3. The persons appointed in accordance with the preceding paragraph are particularly bound by their duty of cooperation with the Banco de Portugal, ensuring their permanent availability and providing themselves with the necessary means of communication to comply with requests addressed to them.
4. For the purposes of Article 72(2)(c) of the Law, the specific training of agents and distributors includes, at least, the aspects listed in Article 19(3)(b) of this Notice.
5. The central contact point appointed in accordance with Article 72(2)(d) of the Law is provided by a person or entity that has, in national territory, an adequate physical and permanent structure to carry out its functions, equipped with the necessary means to prevent the improper disclosure of any information regarding either the activities and operations carried out by the network of agents or distributors, or any suspicions that certain funds or other assets originate from criminal activities or are related to terrorist financing.

6. When the institutions referred to in paragraph 1 operate in national territory simultaneously through a branch and a network of agents or distributors, the functions of the central contact point must be carried out by that branch.

7. The provisions of this article apply to entities considered equivalent to payment institutions referred to in Article 3(4) of the Law, when they operate in national territory through agents.

Article 74

Free provision of services

1. Financial entities headquartered in another Member State send an annual report to the Banco de Portugal on their activities under the freedom to provide services in national territory, with information on the performance of their activities in national territory, including, at least, the information referred to in Article 73(1)(b) of the Law.

2. The report referred to in the preceding paragraph is submitted to the Banco de Portugal by 28 February of each year, covering the period between 1 January and 31 December of the previous year, and will follow the form to be established by an Instruction, which will also specify the terms for submitting the report.

3. The Banco de Portugal may exempt financial entities from submitting the report mentioned in the preceding paragraphs whenever, in compliance with other legal or regulatory provisions, the information provided for in paragraph 1 has already been sent to this supervisory authority.

4. In order to assess the situations provided for in Article 73(2) of the Law, the Banco de Portugal takes into account any other information it is aware of.

5. When the situations provided for in Article 73(2) of the Law occur, the Banco de Portugal may:

   a) Request additional information from financial entities, particularly about the procedures and controls they have implemented to mitigate specifically identified risks;

   b) Subject financial entities to compliance with duties that are suitable for mitigating specifically identified risks, by means of a notification describing the content of the measures to be taken and the deadline for their compliance;

   c) Adopt supervisory measures, among those provided for in Section II of Chapter VII of the Law and in Article 82 of this Notice, which are suitable for verifying compliance with the measures enacted under the preceding paragraph.

6. When the situations provided for in Article 73(2) of the Law concern financial entities that operate simultaneously in national territory through branches, agents or distributors,

such entities comply with the provisions of the Law, this Notice, and other relevant regulations regarding all activities carried out in national territory, and it is the responsibility of the branches established in the territory to ensure that all necessary measures are adopted to this end.

7. The Banco de Portugal notifies the competent authorities of the Member State of the European Union in which the financial entities referred to in Article 73 of the Law and this Notice are headquartered:

   a) The failure to report or the incomplete reporting by the financial entity of the information to be reported under paragraph 1;

   b) The risk situations identified under Article 73(2) of the Law;

   c) The adoption of the measures provided for in paragraphs 5 and 6.

TITLE V

Payment service providers

Article 75

Establishment of obligations under Regulation (EU) 2015/847

1. Payment service providers declare, for each transfer of funds they execute, whether they act as the payment service provider of the payer, the payment service provider of the payee, or the intermediary payment service provider.

2. In cases where fund transfers constitute a direct debit within the meaning of Article 3(9)(b) of Regulation (EU) 2015/847, the payment service provider of the payer sends, as part of the direct debit collection, the required information about the payer and the payee to the payment service provider of the payer, in accordance with Articles 4 and 5 of Regulation (EU) 2015/847 and Article 147 of the Law.

Article 76

Exemptions and derogations

1. Payment service providers adopt appropriate policies, procedures and controls, including the implementation of information systems, to ensure compliance with the conditions necessary for the application of the exemptions and derogations provided for in Regulation (EU) 2015/847, in accordance with the following paragraphs.

2. For the purposes of the exemption provided for in Article 2(3) of Regulation (EU) 2015/847, payment service providers ensure that:

a) The fund transfer to be exempted is intended for the payment of goods or services, whenever the card, instrument or device can be used for fund transfers between individuals and for payments for goods or services;

b) The fund transfer is accompanied by the number of the card, instrument or digital device, and it allows the transaction to be traced back to the payer.

3. For the purposes of the derogation provided for in Article 5(1) of Regulation (EU) 2015/847, payment service providers ensure that all payment service providers involved in the payment chain are established in the European Economic Area.

4. In order to ensure effective control of the €1,000 limit provided for in Articles 5, 6, and 7 of Regulation (EU) 2015/847, payment service providers comply with the provisions of Article 13 of this Notice for all fund transfers.

Article 77

Policies and procedures

1. Payment service providers outline and ensure the effective implementation of policies, procedures and controls that are suitable for complying with Regulation (EU) 2015/847.

2. For the purposes of Article 148 of the Law, when applying the procedures referred to in the preceding paragraph, payment service providers take into account the procedures adopted in compliance with Article 28 of the Law.

3. For the purposes of the preceding paragraph, when assessing the risk of money laundering and terrorist financing to which they are exposed, payment service providers also consider:

a) The number of payment service providers that repeatedly fail to provide the required information about the payer or payee, in accordance with Articles 8(2) and 12(2) of Regulation (EU) 2015/847 and Article 80 of this Notice;

b) The complexity of the payment chains they are involved in as a result of their business model;

c) The volume and value of processed transactions.

4. Payment service providers ensure that the policies, procedures and controls referred to in this article:

a) Clearly outline:

i) The criteria they use to determine whether or not their services and payment instruments fall within the scope of Regulation (EU) 2015/847;

ii) Which of their services and payment instruments fall within the scope of Regulation (EU) 2015/847 and which are excluded from that scope;

iii) Which fund transfers are monitored in real time and which are monitored on an *ex post* basis, and the reasons for such differentiation, in accordance with Article 78(8) of this Notice;

iv) The obligations of collaborators and the procedures to be followed by them when they detect that the information required under Regulation (EU) 2015/847 is missing, incomplete, or has not been filled in with admissible characters or data in accordance with the conventions of the messaging or payment and settlement system used, pursuant to Article 79 of this Notice;

v) What information related to fund transfers is recorded, and how and where it should be recorded.

b) They are approved by the governing body of the payment service provider;

c) They are available to all relevant collaborators, including the people responsible for processing fund transfers;

d) They are reviewed at appropriate intervals, improved as necessary, and updated in accordance with Article 17 of the Law and Article 9 of this Notice.

5. For the purposes of point c) of the preceding paragraph, payment service providers ensure that all relevant collaborators are adequately trained as provided for in Article 55 of the Law and Article 53 of this Notice.

Article 78

Detection of missing information about the payer or the payee

1. The payment service provider of the payee and the intermediary payment service provider ensure that the verification of the admissible characters or data referred to in Articles 7(1) and 11(1) of Regulation (EU) 2015/847 is carried out in real time.
2. Without prejudice to the provisions of the preceding paragraph, the verification referred to in Articles 7(1) and 11(1), both of Regulation (EU) 2015/847, are deemed to have been complied with whenever the payment service provider of the payee and the intermediary payment service provider, respectively, consider, and can demonstrate to the Banco de Portugal, that:

a) They understand the validation rules of the messaging or payment and settlement system used;

b) The conventions of the messaging or payment and settlement system used allow:

i) Filling in all the necessary fields to obtain the information required by Regulation (EU) 2015/847;

ii) Automatically preventing the sending or receiving of fund transfers after detecting inadmissible characters or data;

iii) Flagging rejected fund transfers for analysis and manual processing.

3. For the purposes of point (b)(i) of the preceding paragraph, the payment service provider of the payee and the intermediary payment service provider may consider the International Bank Account Number (IBAN) or, if the fund transfer is carried out through a payment card, the card number, provided that the number used allows the fund transfer to be traced back to the payer or the payee.

4. If their messaging or payment and settlement system does not comply with paragraph 2(b), the payment service provider of the payee or the intermediary payment service provider implements control measures to remedy the identified deficiencies.

5. For the purposes of Articles 7(2) and 11(2), both of Regulation (EU) 2015/847, it is considered that the procedures applied by the payment service provider of the payee and the intermediary payment service provider, respectively, are effective in detecting the omission of the required information about the payer or payee, if they allow:

a) Detecting meaningless information;

b) Combining real-time and *ex-post* monitoring;

c) Alerting to high-risk indicators.

6. The payment service provider of the payee and the intermediary payment service provider treat meaningless information as missing information, even if such information has been filled in with admissible characters or data in accordance with the conventions of the messaging or payment and settlement system.

7. For the purposes of paragraph 5(a), whenever they use a list of terms commonly devoid of meaning, payment service providers review the terms on that list at appropriate intervals to ensure their relevance.

8. The real-time monitoring or *ex post* monitoring of fund transfers, including the level and frequency thereof, is determined by the payment service provider of the payee and the intermediary payment service provider according to a risk-based approach.

9. For the purposes of the preceding paragraph, the payment service provider of the payee and the intermediary payment service provider outline which high-risk indicators, among those identified in accordance with paragraph 11, individually or jointly, always trigger real-time monitoring and which ones trigger *ex-post monitoring*.

10. Without prejudice to the preceding paragraph, the payment service provider of the payee and the intermediary payment service provider carry out *ex post* checks on a randomly selected sample of all fund transfers.

11. In addition to other indicators identified by the payment service providers, the high-risk indicators referred to in the preceding paragraphs may include:

    a) Fund transfers that exceed a specific value threshold defined by the payment service providers based, at least, on the average value of transactions they typically process and the value that, considering their respective business models, constitutes an unusually high transaction;

    b) Fund transfers where the payment service provider of the payer or the payment service provider of the payee is established in a high-risk third country or in another country or territory with increased risk;

    c) A record of non-compliance regarding the prevention of money laundering and terrorist financing of the payment service provider of the payer or the intermediary payment service provider, considering the previous payment service provider in the payment chain;

    d) Fund transfers from a payment service provider that has repeatedly and without justification omitted information on the payer, in accordance with Article 80 of this Notice, or from a payment service provider that has repeatedly and without justification omitted information about the payer or the payee, even if it has not done so repeatedly;

    e) Fund transfers in which the name of the payer or the payee is missing or incomplete.

Article 79

Managing fund transfers where information is missing, incomplete or contains inadmissible characters or data

1. For the purposes of Articles 8(1) and 12(1), both of Regulation (EU) 2015/847, and without prejudice to Article 148 of the Law, the payment service provider of the payee and the intermediary payment service provider implement effective risk-based procedures to determine when to reject, suspend, or execute a fund transfer when real-time monitoring reveals that information about the payer or the payee is missing, incomplete, or has not been completed using admissible characters or data in accordance with the conventions of the messaging or payment and settlement system used.

2. In order to determine whether to reject, suspend, or execute a fund transfer in accordance with the preceding paragraph, the payment service provider of the payee and the intermediary payment service provider consider the risk of money laundering or terrorist financing associated with the transaction, and in particular whether:

   a) The type of information that is missing or incomplete raises concerns about money laundering or terrorist financing;

   b) One or more high-risk indicators, among those identified under the terms of Article 78(11) of this Notice, have been detected, indicating that the transaction presents an increased risk of money laundering or terrorist financing, or raises suspicions that the funds originate from criminal activities or are related to terrorist financing.

3. If the payment service provider of the payee or the intermediary payment service provider decides to reject a fund transfer under the terms of paragraph 2, they do not have to request the missing information, but communicate the reason for the rejection to the previous payment service provider in the payment chain.

4. If the payment service provider of the payee or the intermediary payment service provider decides to suspend a fund transfer under the terms of paragraph 2, they notify the previous payment service provider in the payment chain and request that they provide the missing information about the payer or payee, or that they provide that information using admissible characters or data in accordance with the conventions of the messaging or payment and settlement system used, as applicable.

5. The payment service provider of the payee or the intermediary payment service provider gives the previous payment service provider in the payment chain a reasonable deadline for providing the information requested in accordance with the preceding paragraph,

which, unless it concerns payment chains of greater complexity, may not exceed three business days for fund transfers made within the European Economic Area or five business days for fund transfers made outside the European Economic Area.

6. If the requested information is not provided within the deadline set in accordance with the preceding paragraph, the payment service provider of the payee or the intermediary payment service provider considers:

   a) Sending an alert to the previous payment service provider in the payment chain, requesting them to provide the missing information;

   b) Setting an additional deadline for providing the missing information;

   c) Informing the previous payment service provider in the payment chain that, if they do not provide the missing information within the set deadline, they may be subject to an internal procedure for high-risk cases, as provided for in Articles 8(2) and 12(2) of Regulation (EU) 2015/847 and Article 80 of this Notice.

7. If the information requested under the preceding paragraphs is not provided within the set deadline, including any extensions, the payment service provider of the payee or the intermediary payment service provider, in compliance with their policies, procedures and controls, decide whether to:

   a) Reject or execute the transfer;

   b) Consider whether or not the failure to provide the required information to the previous payment service provider in the payment chain is considered suspicious for the purposes of Articles 9 and 13, both of Regulation (EU) 2015/847, and Article 150 of the Law;

   c) The previous payment service provider in the payment chain must be subject to an internal risk monitoring procedure and treated as a payment service provider with repeated non-compliance, as provided for in Articles 8(2) and 12(2) of Regulation (EU) 2015/847 and Article 80 of this Notice.

8. If the payment service provider of the payee or the intermediary payment service provider decides to execute a fund transfer in accordance with paragraph 2, or only later detects that the required information is missing, incomplete or has not been filled in using admissible characters or data, they request the previous payment service provider in the payment chain to provide the missing information about the payer or the payee, or to provide that information using admissible characters or data after the transfer has been executed.

9. The request for information referred to in the preceding paragraph is subject to the provisions of paragraphs 5, 6, and 7.

10. The payment service provider of the payee and the intermediary payment service provider document and record all actions as outlined in the preceding paragraphs and provide a rationale for taking or not taking measures aimed at managing fund transfers where information is missing, incomplete or contains inadmissible characters or data, in accordance with the provisions of this article.

Article 80

Repeated non-compliance and measures

1. For the purposes of Articles 8(2) and 12(2) of Regulation (EU) 2015/847, the payment service providers of the payee and intermediary payment service providers adopt policies, procedures, and controls that enable the identification of payment service providers that repeatedly fail to provide information about the payer or the payee.
2. The procedures provided for in the preceding paragraph include, *inter alia*, the recording by the payment service provider of the payee or the intermediary payment service provider of all fund transfers in which information was missing.
3. The decision to treat a payment service provider as repeatedly failing to provide information on the payer or the payee under Article 8(2) and Article 12(2), both of Regulation (EU) 2015/847, is based on both quantitative and qualitative criteria, including at least:
    a) The percentage of transfers in which information is missing, sent by the payment service provider within a certain period of time;
    b) The percentage of follow-up requests that were left unanswered by the payment service provider or did not receive an adequate response within a certain period of time;
    c) The level of cooperation of the payment service provider in previous requests for missing information;
    d) The type of missing information.
4. The measures to be taken by the payment service provider of the payee and by the intermediary payment service provider under Articles 8(2) and 12(2) of Regulation (EU) 2015/847 concerning a payment service provider that repeatedly fails to provide the required information about the payer or the payee must be appropriate to the deficiencies detected and, without prejudice to others, may include one or more of the following measures:

a) Setting an additional deadline for providing the required information about the payer or the payee;

b) Issuing a warning specifying the measures that will be taken if the payment service provider continues to not provide the requested information;

c) Conducting real-time monitoring of all operations received from that payment service provider, as provided for in Article 78(8) of this Notice;

d) Rejecting any future fund transfers that the payment service provider may execute;

e) Restricting or terminating the business relationship with the payment service provider, in accordance with the provisions of the following paragraph.

5. Before deciding to terminate a business relationship, especially when the previous payment service provider in the payment chain is a third-country respondent, the payment service provider of the payee and the intermediary payment service provider assess whether or not they can manage the risk through other means or procedures, including the application of the enhanced identification and due diligence measures provided for in Article 70 of the Law and Article 43 of this Notice.

6. The payment service provider of the payee or the intermediary payment service provider communicates, without undue delay, and in accordance with Article 149 of the Law, the decision to treat a payment service provider as repeatedly failing to provide the required information about the payer or the payee.

7. The communication referred to in the preceding paragraph is made within a maximum period of three months after identifying the payment service provider with repeated non-compliance and includes, in accordance with the form to be established by the Banco de Portugal:

   a) The identification of the payment service provider that repeatedly fails to provide the required information, indicating, *inter alia*, the country in which it is authorised;

   b) The nature of the offence, including:

      i) The frequency of fund transfers with missing information;

      ii) The period of time during which the offences took place;

      iii) Any reasons provided by the payment service provider to justify the repeated omission of the required information;

   c) A description of the measures taken under this article.

8. The communication obligation set out in the preceding paragraphs applies without prejudice to the obligation to report suspicious transactions in accordance with Articles 9 and 13, both of Regulation (EU) 2015/847, and Article 150 of the Law.

9. The provisions of this article apply in cases where payment service providers provide incomplete information about the payer or the payee.

Article 81

Additional obligations of intermediary payment service providers

1. Intermediary payment service providers ensure that their policies, procedures and controls ensure that all information received about the payer or the payee accompanying the fund transfer is kept with that transfer.

2. To comply with Article 10 of Regulation (EU) 2015/847, intermediary payment service providers use messaging and payment systems that allow for the transfer of all information about the payer or the payee, regardless of whether such information is required by Regulation (EU) 2015/847.

3. For the purposes of the preceding paragraph, intermediary payment service providers ensure that their systems are capable of converting information into a different format, without errors or omissions, whenever necessary.

TITLE VI

Supervision

Article 82

Supervision by the Banco de Portugal

1. In accordance with Article 95(3) of the Law, for the purpose of verifying compliance with the duties and obligations provided for in the Law, this Notice, and other regulations aimed at preventing money laundering and terrorist financing, the Banco de Portugal also has the powers conferred by the RGICSF and the RJSPME.

2. For the purposes of the preceding paragraph, the Banco de Portugal may, in particular:

   a) Request financial entities to submit reports or opinions related to the prevention of money laundering and terrorist financing, carried out by a duly authorised entity accepted by the Banco de Portugal for this purpose;

   b) Require that special audits be carried out by an independent entity, designated by the Banco de Portugal and at the expense of the financial entity, as part of the prevention of money laundering and terrorist financing, as well as the subsequent submission of the corresponding reports.

3. For the purposes of article 96(a) of the Law, the Banco de Portugal has access to any premises or facilities used by third parties, including those of service providers, third-party entities, credit intermediaries, promoters, and other intermediaries, as provided for in Articles 16 and 46 to 48 of this Notice.
4. For the purposes of Article 96(b) of the Law, the Banco de Portugal has access to any tool or information system used by financial entities.

Article 83

Report on the prevention of money laundering and terrorist financing

1. Every year, financial entities submit a specific report on their internal control system and other information to be outlined by Instruction for the prevention of money laundering and terrorist financing.
2. The report referred to in the preceding paragraph is submitted to the Banco de Portugal by 28 February of each year, covering the period between 1 January and 31 December of the previous year, and will follow the form to be outlined by an Instruction, which will also specify the terms for submitting the report.
3. The report includes information about:
    a) Institutional information and relevant contacts of the financial entities;
    b) Policies, procedures and controls for preventing money laundering and terrorist financing;
    c) Risk management;
    d) Use of new technologies, products, and services with a potential impact on the prevention of money laundering and terrorist financing;
    e) Monitoring compliance with the regulatory framework;
    f) Monitoring compliance with the obligations related to reporting irregularities provided for in Article 17(1) of this Notice;
    g) Internal audit;
    h) External audit;
    i) General and specific information systems and procedures;
    j) Deficiencies detected by the financial entity in the prevention of money laundering and terrorist financing;
    k) Specific information about types of operations;

l) Information about specific types of financial entities, including procedures adopted as part of the SICAM;

m) Specific procedures to comply with Regulation (EU) 2015/847 and deficiencies detected in its implementation;

n) Corrective measures taken to address deficiencies identified by the financial entity and identified as a result of supervisory actions carried out by the Banco de Portugal;

o) Relevant quantitative information;

p) Self-assessment questionnaire of the financial entity, including its perception of the adequacy and degree of regulatory compliance of the procedures adopted in accordance with the Law, this Notice and other relevant regulations;

q) Other relevant information for the exercise of the supervisory powers of the Banco de Portugal in the field of the prevention of money laundering and terrorist financing.

4. In addition to the information referred to in the preceding paragraph, financial entities also communicate:

   a) The overall opinion of the governing body on the adequacy and effectiveness of the respective internal control system, specifically in the context of the prevention of money laundering and terrorist financing;

   b) Information about any detection, by the supervisory body of the financial entity, of high-risk deficiencies in their internal control system for the prevention of money laundering and terrorist financing during the reference period;

   c) Opinion of the supervisory body of the financial entity, clearly, comprehensively, and substantively expressing its view – in a positive manner – on the quality of their internal control system for the prevention of money laundering and terrorist financing.

5. Financial entities continuously update the information referred to in paragraph 3(a), in accordance with the terms to be outlined by Instruction.

TITLE VII

Supplementary provisions

Article 84

Portuguese language

1. Financial entities prepare and maintain a permanently updated Portuguese version of their procedure manuals or any other relevant internal documents or records concerning the prevention of money laundering and terrorist financing, as well as the opinions, examinations, analyses and informational reports referred to in the Law or this Notice.
2. When the evidentiary documents referred to in Article 51 of the Law and Article 50 of this Notice are not written in Portuguese, financial entities are obliged to:
   a) Be equipped with the means and resources necessary to fully understand them;
   b) Ensure that they are immediately and reliably translated, whenever requested to do so by the Banco de Portugal or other competent authorities as provided in the Law.

Article 85

Equivalent amount in foreign currency

Any reference in this Notice to amounts expressed in euros shall also be deemed to be made for an equivalent amount expressed in any other foreign currency.

Article 86

Communication channels

1. Unless otherwise provided by a rule or determination of the Banco de Portugal, communications made by financial entities to the Banco de Portugal under the terms and for the purposes of the Law, this Notice and other relevant regulations, including any requests for information or clarification related to compliance with the provisions of those regulations, are carried out through the BPnet services available in the 'Prevention of MLTF' Area of the BPnet System, a restricted-access computer platform regulated by Instruction 21/2020, of 15 July.
2. Financial entities adhere to the rules for subscribing to and using the BPnet services referred to in the preceding paragraph, as outlined by the Banco de Portugal in a Circular Letter.

3. Communications sent by the Banco de Portugal to financial entities via the BPnet services referred to in paragraph 1 shall be deemed to be notifications, including for the purposes of Article 112 of the Administrative Procedure Code.

TITLE VIII

Additional, transitional and final provisions

Article 87

References

All references made by other regulations or Circular Letters to regulations repealed pursuant to the following article shall henceforth be deemed to have been made to this Notice.

Article 88

Repealing rule

It repeals:

a) Banco de Portugal Notice no. 2/2018, of 26 September;

b) Banco de Portugal Instruction no. 2/2021, of 26 February.

Article 89

Entry into force

This Notice shall enter into force within 60 days of its publication.

24 May 2022. - The Governor, *Mário Centeno*.

Annex I to the Notice

(referred to in Article 21(6) of this Notice)

Using videoconference as an alternative procedure for verifying identifying information

Article 1

Videoconference

1. Financial entities may verify the identifying information referred to in article 24(1)(a)(i) to (vii) of the Law using videoconference, as provided for in this Annex.
2. The use of videoconference does not prejudice:
   a) The use of other means of verification provided for in Article 25 of the Law, namely those listed in paragraph 2;
   b) The verification of identifying information provided for in Article 24(1)(a)(viii) to (xi) of the Law, under the terms of Article 21(1) of this Notice;
   c) The application of the provisions of Article 35 of the Law and Articles 29 et seq. of this Notice.
3. The use of videoconference does not exempt financial entities from complying with the obligations arising from the duty of identification and due diligence, as well as other duties arising from the Law and this Notice, including but not limited to:
   a) Prior to establishing the business relationship:
      i) Assessing or detecting the status of 'politically exposed person', 'close family member', 'person recognised as being closely associated', or 'holder of another political or public position', as provided for in Article 19 of the Law and Article 11 of this Notice;
      ii) Ensuring compliance with restrictive measures adopted by the United Nations Security Council or adopted by the European Union, in accordance with Article 21 of the Law and Article 18 of this Notice.
   b) Whenever, in accordance with Article 28 of the Law and Article 27(2) of this Notice, the risk analysis carried out on a case-by-case basis by financial entities in relation to the business relationship justifies a higher level of customer knowledge:
      i) Requesting additional information to the extent appropriate to the specifically identified risk;
      ii) Requiring, to the extent appropriate to the specifically identified risk, a higher level of verification of the identifying information obtained.

Article 2

Prerequisites

1. Before adopting videoconference as a procedure for verifying identifying information, financial entities:

   a) Conduct a risk analysis that specifically identifies the money laundering and terrorist financing risks associated with the procedure in question;

   b) Perform effectiveness and security tests of the procedure;

   c) Obtain a prior opinion from the AML/CFT compliance officer, which specifically assesses the adequacy of the mechanisms designed to mitigate the risks identified in the analysis provided for in point a).

2. For the purposes of the risk analysis referred to in point a) of the preceding paragraph, financial entities determine, in particular, the types of identification documents accepted as part of this procedure and prepare a set of requirements and measures to ensure the adequate mitigation of any risks posed by the characteristics of certain types of identification documents.

3. The effectiveness and security tests referred to in paragraph 1(b) are not only conducted prior to and concurrently with the introduction of this procedure, but also periodically, in order to ensure its correct and proper functioning, particularly to address emerging fraud trends.

4. The analyses, tests, and opinions carried out for the purposes of the preceding paragraph are documented in written records and are subject to the duty of retention as provided for in Article 51 of the Law and Article 50 of this Notice.

Article 3

Safeguards

1. Whenever they use videoconference as a procedure for verifying identifying information, financial entities:

   a) Require that the initial fund delivery be made through a traceable means that allow the payer to be identified, originating from an account opened with a financial or other legally authorised entity which, not being located in a high-risk third country, demonstrably applies identification and due diligence measures compatible with those provided for in the Law and this Notice;

   b) Collect a plain copy of the original identification documents and other documents used to verify identifying information, in hard copy or electronic format.

2. Financial entities apply enhanced identification and due diligence measures proportional to the specifically identified risk whenever the initial delivery of funds, as provided for in point a)

of the preceding paragraph, originates from an account held by a person other than the customer, without credible justification being provided.

3. Whenever the identification documents presented or accessed raise doubts about their content, suitability, authenticity, currency, accuracy or sufficiency, financial entities:

   a) Do not accept the alternative means or procedures used, which do not have any probative effect;

   b) Make the communication provided for in Article 43 of the Law, subject to the verification of the respective prerequisites;

   c) Act, whenever possible, in coordination with the competent judicial or law enforcement authorities, consulting them beforehand whenever they have sufficient grounds to believe that not accepting the alternative means or procedures used may prejudice an investigation.

Article 4

Requirements associated with identified persons

1. The procedure for verifying identifying information through videoconference is only applicable to natural persons who hold a public document that meets the requirements of Article 25(1) of the Law.

2. The financial entity requests the provision of a contact that allows compliance with the requirements set forth in Article 7(3) and (4) of this Annex.

Article 5

Requirements regarding human and material resources

1. The videoconference is conducted by duly trained collaborators with appropriate training in the prevention of money laundering and terrorist financing, in accordance with the provisions of Article 55 of the Law and Article 53 of this Notice, as well as in matters related to fraud and forgery of identification documents.

2. Collaborators who verify identifying information through videoconference shall make a clear notation in the internal support records that identifies them and the date on which such verification was carried out, in accordance with the provisions of Article 15 of this Notice.

3. The financial entity holds the videoconference in a separate physical space that allows, among other things, for proper recording and the quality of the videoconference.

4. All the information collected during the videoconference, including its recording, is subject to a duty of retention, under the terms of Article 51 of the Law and Article 50 of this Notice.

Article 6

Technical requirements

Financial entities ensure that the technical means used are appropriate to guarantee that the videoconference:

a) Is conducted in real time and without interruptions or pauses;

b) Has adequate audio and visual quality to allow clear identification of the security features and characteristics of the identification document, as well as the subsequent verification of the identification data collected and verified;

c) Is recorded with the indication of the respective date and time, with the consent of the person involved;

d) Runs for a period of time sufficient to ensure full compliance with the procedures described in Article 7(2) of this Annex.

Article 7

Requirements to be observed during videoconference

1. During the videoconference, the financial entity captures a front and back image of the identification document mentioned in Article 4(1) of this Annex, indicating the date and time of capture and with sufficient quality for all the identifying information on the document to be perceptible, including the customer's photograph and signature.

2. In order to allow verification that the identification document presented does not give rise to doubts as to its content, suitability, authenticity, currency, accuracy or sufficiency, the videoconference includes:

   a) Checking security features of the identification document used, from different categories, if applicable;

   b) Checking other features of the identification document in comparison with the respective specimen, namely the card layout, the number, size and spacing of characters, and the typeface;

   c) Checking the condition of the identification document, ensuring, in particular, that it is not damaged, has not been tampered with, and does not contain any altered or erased features;

   d) Checking the truthfulness of the features on the identification document in relation to the customer, confirming, in particular, the resemblance to the document's photograph and the plausibility and knowledge of the date of birth;

   e) Asking the individual to tilt the document horizontally and/or vertically in front of the camera;

   f) Asking the individual to show the various sides and edges of the document in front of the camera;

g) Some questions regarding the identifying information to be verified, which should vary from session to session.

3. During the videoconference, a one-time password (OTP) with a limited duration and specially generated for this purpose, is sent to the individual, ensuring the full traceability of the identification procedure and the videoconference takes place in real time and without pauses.

4. The identification verification procedure is only considered complete once the individual enters the one-time password mentioned in the preceding paragraph and the system confirms it.

If the technical conditions necessary for properly conducting the identification verification process are not met, namely in the case of poor image quality, poor lighting or sound conditions, or interruptions in the video transmission, the videoconference will be interrupted and considered ineffective.

Annex II to the Notice

[referred to in Article 28(1)(a) of this Notice]

Aspects to be considered when assessing situations indicating reduced risk as provided for in the Law

Reduced risk situations identified in Annex II to the Law	Aspects to be taken into account by financial entities
1 - Risk factors inherent to the customer	
a) Companies with shares admitted to trading on a regulated market and, due to the rules of that market, the Law , or other binding instruments, subject to information duties that ensure adequate transparency regarding the respective beneficial owners;	1. Companies with shares admitted to trading on a regulated market, subject to information disclosure requirements consistent with European Union law or subject to equivalent international standards that ensure sufficient transparency of information regarding their beneficial owners and share ownership, may benefit from the adoption of simplified measures. 2. In order to identify regulated markets that ensure adequate transparency, financial entities also take into account, whenever available, the information provided by the supervisory authorities of their respective sectors regarding their operating rules. 3. Financial entities may adopt identical simplification measures for branches and subsidiaries subject to the exclusive control of companies with shares admitted to trading, as determined in accordance with the preceding points, provided they can documentarily prove the verification of said exclusive control.
b) Public administration or public companies;	The following may benefit from the adoption of simplified measures: 1. The Portuguese Government, the autonomous regions, local authorities, legal persons governed by public law of any nature integrated into the central, regional or local administration, as well as independent administrative entities. 2. Companies in the public business sector subject to exclusive control by the Government. 3. Other public authorities and bodies subject to transparent accounting and internal governance practices and subject to scrutiny.

c) Customers residing in geographical areas with lower risk, determined in accordance with paragraph 3 of Annex II to the Law.	1. When outlining situations of proven reduced risk associated with customers registered, established or residing in geographical areas with lower risk, financial entities, in addition to verifying the type of customer, always assess the risk associated with the specific territory of lower risk, in accordance with Annex II to the Law and the provisions of this Annex. 2. The following types of customers are presumed to have a proven reduced risk: a) Entities referred to in Article 3(1) of the Law, with the exception of payment institutions, electronic money institutions, and insurance intermediaries; b) Entities of a nature equivalent to those referred to in the preceding paragraph; c) Branches of the entities referred to in the preceding paragraphs, provided they comply with the procedures outlined by their parent company; d) Entities referred to in Article 3(3) of the Law.
2 - Risk factors inherent to the product, service, transaction or distribution channel	
a) Savings products similar in nature to life insurance contracts and pension funds with reduced annual premiums or contributions;	Premiums or contributions whose annual amount does not exceed €1,000 or whose single amount does not exceed €2,500 are presumed to be reduced.
b) Limited and clearly outlined financial products or services aimed at increasing the level of financial inclusion for certain types of customers;	1. The following are presumed to be limited and clearly outlined financial products or services: a) A basic banking service account, under the terms and conditions set out in Decree-Law no. 27-C/2000, of 10 March, in its current wording; b) Microcredit; c) Current accounts for students; d) Accounts and other basic payment products with limitations on the number and amount of transactions or on the type of payment services and instruments made available, provided they do not include: i) International transfers; ii) Credit products with a value exceeding €2,000. 2. When identifying situations of proven reduced risk associated with the use of limited and clearly outlined financial products or services, financial entities

	ensure that accounts with fund transactions exceeding two national minimum wages per month are monitored with the frequency applied to accounts subject to normal due diligence. 3. In addition to verifying the type of product, financial entities always assess the risk associated with the customer.
c) Products in which the risks of money laundering and terrorist financing are controlled by other factors, such as imposing top-up limits or transparency of ownership, and may include certain types of electronic money.	1. Electronic money products that meet the following conditions cumulatively are presumed to have proven reduced risk: a) The payment instrument cannot be topped up, or has a maximum monthly limit of €150 for payment transactions that can only be used within the national territory; b) The maximum amount stored electronically does not exceed €150; c) The payment instrument is used exclusively for purchasing goods or services; d) The payment instrument is not topped up using anonymous electronic money or another untraceable payment method; e) The monetary value represented by electronic money cannot be reimbursed in cash; f) Payment transactions initiated over the Internet or by remote means of communication may not exceed €50. 2. The provisions of the preceding paragraph do not preclude financial entities from identifying other situations of reduced risk associated with the use of electronic money, under the terms of Article 35(3)(b) of the Law and Article 28(3) of this Notice.
3 - Risk factors inherent to geographic location – registration, establishment or residence in:	

a) Third-party countries that have effective systems in place to prevent and combat money laundering and terrorist financing; b) Countries or jurisdictions identified by credible sources as having a low level of corruption or other criminal activities; c) Third countries that are subject, based on reliable sources such as mutual evaluation reports, detailed assessment or monitoring reports, to obligations to prevent and combat money laundering and terrorist financing that are consistent with the revised FATF recommendations and that effectively implement these obligations.	In their specific assessment of geographical risk, financial entities verify the existence of a regulatory and supervisory framework compatible with the provisions of the Law and this Notice.

Annex III to the Notice

[referred to in Article 28(1)(b) of this Notice]

Other potentially reduced risk situations

This Annex aims to provide financial entities with an illustrative list of indicative factors and types of potentially reduced money laundering or terrorist financing risks that should be considered by financial entities when analysing situations that may warrant the adoption of simplified measures, in addition to the provisions of Annex II to the Law and Annex II to this Notice.

However, financial entities may also consider other indicative factors and types of potentially reduced risk that are appropriate to their specific operating reality.

1. Risk factors inherent to customers:
    a) Customers with a simple control and ownership structure that allows information about their beneficial owners to be known easily and in a timely manner;
    b) Customers subject to information disclosure requirements consistent with European Union law or subject to equivalent international standards that ensure sufficient transparency of information regarding the respective beneficial owners, in addition to those mentioned in paragraph 1(a) of Annex II to the Law and paragraph 1(a) of Annex II to this Notice;
    c) Customers with low-value assets and investments.

2. Risk factors inherent to the product, service, transaction or distribution channel:
    a) Non-complex financial products with low profitability or return;
    b) Products with limited use or specific, pre-determined purposes, such as:
        i) Fixed-term savings products with low savings thresholds;
        ii) Products whose benefits can only be realised in the long term or for a specific reason, such as retirement or the purchase of a primary and permanent residence;
        iii) Products made available to specific categories of customers who meet predefined circumstances, such as social benefit recipients, parents representing their children, or minors until they reach legal age;
        iv) Recurring transfers, including direct debits, of the same amount and to the same beneficiary, with apparent economic rationality,

including payment of essential basic services, salary payments, and contributions to pension funds;

v) Products that do not allow cash top-ups or refunds;

vi) Products that can only be used within the national territory;

vii) Products that can only be used to purchase goods or services, particularly when the card holder can only make purchases from a limited number of merchants or points of sale, and the financial entity has sufficient knowledge of the activities conducted by the merchants;

viii) Low-value credit products, including those contingent on the purchase of a good or service.

c) Pooled accounts held by customers who meet the requirements set out in paragraph 1(c) of Annex II to the Law, as determined in accordance with the provisions of paragraph 1(c) of Annex II to this Notice, and who demonstrate that they are able to immediately provide information and documents concerning their own customers, in compliance with identification and due diligence measures compatible with those provided for in the Law and this Notice;

d) Payment initiation services;

e) Account information services.

Annex IV to the Notice

(referred to in Article 28(2) of this Notice)

Other potentially higher-risk situations

This Annex aims to provide financial institutions with an illustrative list of indicative factors and types of potentially higher money laundering or terrorist financing risks that are considered by financial entities when analysing situations that may warrant the adoption of enhanced measures, in addition to the provisions of Annex III to the Law.

However, financial entities should also consider other indicative factors and types of potentially higher risk that are appropriate to their specific operating reality. For the purposes of this Annex, the term 'customer' should be understood as generally referring not only to the concept set out in Article 2(1)(c) of this Notice, but also to the representatives of the customer, including individuals authorised to operate accounts held by customers of financial entities, as well as their beneficial owners.

1. Risk factors inherent to customers:

    a) Customers that are non-profit organisations and have been identified, pursuant to Article 145(3)(a) of the Law, as representing an increased risk of money laundering or terrorist financing;

    b) Customers residing or operating in jurisdictions associated with a higher risk of money laundering or terrorist financing, as determined in accordance with paragraph 3 of Annex III to the Law and paragraph 4 of this Annex;

    c) Customers with nationality or known connections to jurisdictions associated with a higher risk of terrorist financing or support for terrorist activities or acts;

    d) Customers with known connections to foreign terrorist fighters;

    e) Customers engaged in economic activities involving dual-use goods;

    f) Customers engaged in economic activities in sectors prone to tax evasion or considered by reliable and credible sources to have a high risk of money laundering and terrorist financing (e.g., real estate, gambling, transportation, auctions, among others);

    g) Customers engaged in economic activities in sectors often associated with high levels of corruption;

    h) Customers that use intermediaries or agents with broad powers of representation for the purposes of initiating or managing the business relationship, particularly when these intermediaries or agents

are headquartered or domiciled in jurisdictions associated with a higher risk of money laundering or terrorist financing;

i) Customers that are newly established legal entities with no known or suitable business profile for the declared activity;

j) Customers that are asset holding vehicles or asset management vehicles;

k) Customers that have been subject to administrative or judicial measures or sanctions for violating the regulatory framework related to money laundering or terrorist financing.

2. Risk factors inherent to the product, service, transaction or distribution channel:

a) Products or services associated with virtual assets;

b) Products, services, operations, or distribution channels characterised by an excessive degree of complexity or segmentation;

c) Cash and high-value operations, especially using high-denomination banknotes;

d) Occasional high-value transactions, considering what is expected for the product, service, transaction or distribution channel used;

e) Products without an established geographic use, even when it is not necessary for the execution of their purposes;

f) Loans secured by assets located in jurisdictions that hinder or prevent the acquisition of information regarding the identity and legitimacy of the parties involved (and their respective beneficial owners) in providing the collateral;

g) Fund circuits with a large number of intermediaries operating in different jurisdictions;

h) Electronic money products without limitations on:

i) Number or amount of payments, top-ups, or refunds allowed;

ii) Monetary value stored electronically.

i) Operations financed using anonymous electronic money, including the use of electronic money products benefiting from the exemption provided for in Article 12 of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015;

j) Electronic money products or other prepaid instruments that allow the transfer of funds between different users;

k) The creation or use of asset holding vehicles and asset management vehicles.

3. Risk factors inherent in correspondent relationships:

   a) Correspondent relationships in which the respondent – or the financial group to which it belongs – has been subject to measures or sanctions relevant to the prevention of money laundering and terrorist financing;

   b) Situations in which the respondent conducts a significant part of its business in activities or sectors frequently associated with money laundering or terrorist financing;

   c) Correspondent relationships with entities that hold an offshore banking licence.

4. Risk factors inherent to geographic location:

   a) Jurisdictions identified by reliable and credible sources as having ineffective judicial systems or deficiencies in the investigation of crimes associated with money laundering or terrorist financing;

   b) Jurisdictions that do not implement reliable and accessible records (or other equivalent mechanisms) of beneficial owners;

   c) Jurisdictions that have not implemented the Common Reporting Standard developed by the Organisation for Economic Co-operation and Development (OECD) on the automatic exchange of information);

   d) Jurisdictions known for offering simplified or non-existent relevant administrative procedures or clearly more favourable privileged tax schemes;

   e) Jurisdictions with legal frameworks that establish prohibitions or restrictions that prevent or limit compliance by the financial entity with the legal and regulatory standards governing its activity, including in terms of the provision and circulation of information.