BANCO DE PORTUGAL
EUROSISTEMA

Banco de Portugal Notice no. 1/2023

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.

Law no. 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.

On 1 September 2021, Law no. 58/2020, of 31 August, came into force, transposing into national law the revision promoted by Directive (EU) 2018/843 of the European Parliament and of the Council of 23 October 2018 to the aforementioned Directive (EU) 2015/849, amending, among other laws, Law no. 83/2017, of 18 August.

As a result of these changes, the list of entities obliged to comply with the provisions of Law no. 83/2017, of 18 August, now includes entities that carry out, in Portugal, in the name or on behalf of a customer, at least one of the economic activities with virtual assets listed in Article 2(1)(mm) of that law.

Pursuant to Article 112-A of Law no. 83/2017, of 18 August, since the new regime came into force, those activities involving virtual assets can only be carried out by entities that have obtained prior registration with Banco de Portugal. To this end, Banco de Portugal Notice no. 3/2021 was published on 23 April 2021, regulating the rules on the process of registration with Banco de Portugal, applicable to entities that carry out activities with virtual assets.

Banco de Portugal is also the competent national authority for verifying compliance with ML/TF preventive duties by the entities exercising the aforementioned

Published in: Official Gazette, 2nd Series, Part E, no. 17, of 24-01-2023

activities with virtual assets, in accordance with Article 89(1)(j) of Law no. 83/2017.

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 and 55.

Banco de Portugal, as the competent authority in this matter, is responsible for approving the regulations applicable to entities that carry out activities with virtual assets (see, in particular, Article 94(2)(d) of Law no. 83/2017, of 18 August).

The relevance of this Notice therefore stems above all from the need to fulfil the multiple mandates addressed to the Banco de Portugal by the legislation referred to above and, at the same time, to adapt the legal requirements to the specific operating reality of entities that carry out activities with virtual assets, without prejudice to the technological neutrality that the sector-specific regulations issued must comply with.

This Notice also amends Banco de Portugal Notice no. 1/2022, of 6 June, in very limited areas that derive from the need to rectify very specific aspects or to conform the way financial entities should relate to entities that carry out activities with virtual assets.

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

Therefore, in the use of the powers conferred on 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, and by Article 27 of Law no. 97/2017, of 23 August, Banco de Portugal determines:

TITLE I
General provisions

Article 1
Object and scope

1. This Notice regulates, in the exercise of the powers conferred by Article 94 of Law no. 83/2017, of 18 August (hereinafter referred to as the 'Law'), particularly paragraph 2(d), the conditions of exercise, the procedures, instruments, mechanisms, application formalities, reporting obligations and other aspects necessary to ensure compliance with the duties to prevent money laundering and terrorist financing, as part of the activity of entities that carry out activities with virtual assets.

2. This Notice also regulates, in the exercise of the powers conferred by Article 27 of Law no. 97/2017, of 23 August (Law no. 97/2017), the means and mechanisms necessary for compliance with the duties laid down in that law by entities that carry out activities with virtual assets.

Article 2

Definitions

1. For the purposes of this Notice, the following definitions apply:

   a) 'Real-time monitoring' refers to the monitoring conducted before virtual assets are made available to the beneficiary or, if applicable, to another entity that carries out activities with virtual assets, beneficiary or intermediary;

   b) '*Ex post* monitoring' refers to the monitoring conducted after the virtual assets have been made available to the beneficiary or, if applicable, to another entity that carries out activities with virtual assets, beneficiary or intermediary;

   c) 'Hosted wallet' refers to a wallet hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature and that allows its holder (customer) to control, hold, store, move and receive virtual assets, including private cryptographic keys;

   d) 'Omnibus wallet', refers to a 'hosted wallet' or to a self-hosted address securitised or held by the entity itself which carries out activities with virtual assets and which it uses on behalf of its customers or counterparties;

   e) 'Customer' refers to any natural person, legal person, whether corporate or non-corporate, or centre of collective interests without legal personality, who comes into contact with an entity that carries out activities with virtual assets for the purpose of having a service provided or a product made available by it, through the establishment of a business relationship or the execution of an occasional transaction.

   f) 'Collaborator' refers to any natural person who, on behalf of or in the interest of the entity that carries out activities with virtual assets 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 (employee) or not (external collaborator);

   g) 'Relevant collaborator' refers to any employee or external collaborator of the entity that carries out activities with virtual assets, who fulfils at least one of the following conditions:

      i) Be a member of the management body of the entity that carries out activities with virtual assets;

      ii) Hold a position that involves direct, in-person or remote contact with the customers of the entity that carries out activities with virtual assets;

iii) Hold a position within the entity that carries out activities with virtual assets related to compliance with the regulatory framework regarding the prevention of money laundering and terrorist financing;

iv) Be qualified as such by the entity that carries out activities with virtual assets;

h) '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;

i) 'Self-hosted address' refers to an address or wallet that is not hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature, and that allows its owner or holder to independently store, move or receive virtual assets, including private cryptographic keys;

j) 'Distributed ledger address' refers to an alphanumeric code that identifies an address in a network that uses distributed ledger technology or a similar technology where virtual assets can be sent or received;

k) 'Entity that carries out activities with virtual assets' refers to an entity that carries out, within national territory, one or more of the activities with virtual assets listed in Article 2(1)(mm) of the Law, in accordance with Article 4(6) of the Law, and is registered with Banco de Portugal in accordance with Article 112-A of the Law;

l) 'Entity of an equivalent nature' refers to an entity with its head office abroad which, while not subject to the obligation to register with the Banco de Portugal under the terms of Article 112-A of the Law, carries out activities with virtual assets;

They are rectified by Statement of Rectification no. 371/2023, of 9 May.

m) 'Single transaction identifier' refers to a combination of letters, numbers or symbols determined by the entity that carries out activities with virtual assets, which allows the traceability of the transfer of virtual assets back to the originatorand beneficiary;

n) '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 higher risk of money laundering or terrorist financing, including 'high-risk third countries' within the meaning of Article 2(1)(bb) of the Law;

o) 'Means of remote communication' refers to any means of communication – telephone, electronic, telematic or otherwise –that allows the establishment of business relationships, the execution of occasional transactions or the performance of operations in general, without the simultaneous physical presence of the entity that carries out activities with virtual assets and its customer;

p) 'Pooled wallet' refers to a hosted wallet which is used by a customer to hold the virtual assets of their customers, who do not have the power to operate the wallet;

q) 'Representatives' refers to all individuals with decision-making powers in a business relationship or occasional transaction, including the authority to move virtual assets or fiat money, based on legal or voluntary representation instruments, 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 entity that carries out activities with virtual assets;

r) 'Durable medium' refers to any hard-copy 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;

s) 'Batch file transfers' refers to a set of several individual virtual asset transfers, aggregated for transmission purposes;

t) 'Videoconference' refers to a means of remote communication that enables the verification of identifying information of natural persons 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 and Law no. 97/2017 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. Entities that carry out activities with virtual assets ensure the existence of a regulatory compliance monitoring function concerning the prevention of money laundering and terrorist financing (regulatory compliance monitoring function), which guarantees:

   a) The outlining and effective implementation of policies, procedures and controls appropriate to the effective management of money laundering and terrorist financing risks to which the entity is or may be exposed;

   b) Compliance, by the entity that carries out activities with virtual assets, with the legal and regulatory rules on the prevention of money laundering and terrorist financing.

2. Entities that carry out activities with virtual assets shall ensure the segregation of the regulatory compliance monitoring function from the activities that that function monitors and controls, without prejudice to the provisions of the following paragraph.

3. The requirement set out in the previous paragraph does not apply to the regulatory compliance monitoring function, whenever the number of collaborators, excluding directors, is lower than 6 and operating income in the last financial year was less than €1,000,000.

4. Entities that carry out activities with virtual assets 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. Entities that carry out activities with virtual assets appoint an executive member of the management body for the purposes of Article 13(4) of the Law, who is responsible, namely, for:
   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. Entities that carry out activities with virtual assets ensure that the member of the management body appointed under the terms of the previous 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) Ensures that any situations of potential conflicts of interest are identified in advance, minimised and subject to careful and independent monitoring.

Article 5

AML/CFT compliance officer

1. For the purposes of Article 16 of the Law, entities that carry out activities with virtual assets appoint one person responsible for monitoring regulatory compliance (AML/CFT 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, and the policies, procedures and instrumental controls for their execution, which is made available to relevant collaborators of the entity that carries out activities with virtual assets;
   b) Supporting the preparation and execution of the assessments provided for in Article 17 of the Law and Article 10 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 provision of all communications from Banco de Portugal made under the Law, this Notice, and other regulatory provisions, to all relevant collaborators of the entity that carries out activities with virtual assets.
3. For the purposes of Article 16(3)(a) of the Law, entities that carry out activities with virtual assets ensure that the AML/CFT compliance officer:
   a) Performs those duties on an exclusive basis;
   b) Does not perform any other duties within the entity, without prejudice to the provisions of Article 16(3) of this Notice and Article 16(3)(e) of the Law.

Article 6

Supervening changes

Entities that carry out activities with virtual assets shall immediately notify Banco de Portugal, under the terms and through the channels set out in Article 51, of any changes that may occur:

a) Regarding the following identification details of the member of the management body appointed for the purposes of Article 13(4) of the Law and Article 4 of this Notice:
   i) Name;

ii) Corresponding departments;

iii) Telephone contact;

iv) Email address;

b) Regarding the following identification details of the AML/CFT compliance officer appointed for the purposes of Article 16 of the Law and Article 5 of this Notice:

i) Name;

ii) Position and its place in the hierarchical structure;

iii) Date of beginning of term of office;

iv) Direct telephone contact;

v) Email address;

vi) Place in the organisational structure;

vii) Roles undertaken.

Article 7

Risk identification

1. In compliance with Article 14(2)(a) of the Law, when identifying the specific money laundering and terrorist financing risks inherent to their specific operating reality, entities that carry out activities with virtual assets shall consider, among others, the following specific aspects:

a) Types of virtual assets to be made available and the main characteristics of each, including whether they are in any way liable to hide identity, as well as the protocols used and the susceptibility to being altered;

b) Issuer of each virtual asset made available;

c) Total value of the virtual assets made available;

d) Number and value of the virtual assets transacted;

e) Execution of virtual asset transfers from or to self-hosted addresses;

f) Products, services or transactions involving the use of cash or other untraceable means;

g) Nature and scope of each distribution channel used, including whether it is an open-loop or closed-loop circuit;

h) Whether and to what extent the distribution channels for products and services with virtual assets interact with, or are linked to, distribution channels for products and services in fiat money;

i) Use of other service providers to make products, services and transactions available.

2. When identifying concrete money laundering and terrorist financing risks, entities that carry out activities with virtual assets consider the indicative situations of potentially lower risk listed in Annex II to the Law, taking into account the aspects listed in Annex II to this Notice, the indicative situations of potentially higher risk listed in Annex III to the Law, and the factors and indicators of risk listed in Annexes III and IV to this Notice.

Article 8

Review of the internal control system and risk management practices

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 risk management practices referred to in Article 14(2)(d) and Article 15, both of the Law, shall be carried out at intervals of no more than 12 months.

Article 9

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 and in Article 7 of this Notice, entities that carry out activities with virtual assets shall make use of 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 used by entities that carry out activities with virtual assets 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, both of the Law, and the specific aspects set out in Article 7 of this Notice.
3. In order to comply with the provisions of this article, entities that carry out activities with virtual assets shall consider, where applicable, the following information sources:
   a) Information, guidelines or alerts issued or disseminated by Banco de Portugal;
   b) Information, guidelines or alerts from the Financial Intelligence Unit (FIU) or other judicial and police authorities;
   c) Information, guidelines or alerts issued by the Government, including the Anti-Money Laundering and Counter-Terrorist Financing Coordination Committee ;
   d) Information, guidelines or alerts issued by the European Supervisory Authorities, the Financial Action Task Force or the European Commission;
   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 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 entities that carry out activities with virtual assets, including information gathered during identification and due diligence procedures, as well as internally drawn up and updated lists and databases;

h) Information registered on a network that uses distributed ledger or similar technology;

i) Black lists of entities, addresses or wallets from sources considered reliable and credible.

4. In order to comply with the provisions of this article, entities that carry out activities with virtual assets shall also consider, among others, the following information sources:
   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 indexes or specific assessment reports on jurisdictions where entities that carry out virtual activities 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 entities that carry out activities with virtual assets or equivalent entities, insofar as legally permissible.

Article 10

Effectiveness assessment

1. For the purposes of Article 17 of the Law, entities that carry out activities with virtual assets 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, due diligence and retention procedures adopted, including those performed by third parties;

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 internal training policy of the entity that carries out activities with virtual assets, including the adequacy and scope of the training activities provided;

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

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

2. In order to fulfil the assessment provided for in the previous paragraph, entities that carry out activities with virtual assets shall ensure the existence or outsourcing of an audit function or a duly qualified third-party that ensures the independence of this assessment.

3. The assessments provided for in this article shall be carried out at intervals of no more than 12 months.

Article 11

Procedures and information systems in general

1. Entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets:
   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 entity that carries out activities with virtual assets 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.

d) Adopt network analysis tools that use distributed ledger or similar technology;

e) Adopt tools that allow them to screen addresses or wallets held by or associated with customers against black lists of entities, addresses or wallets referred to in Article 9(3)(i) of this Notice;

f) Adopt tools to detect the use of technologies that make it possible to hide the identity or location, namely by using mixers, tumblers, or anonymisers, or virtual private network (VPN) services;

g) Adopt Internet Protocol (IP) address tracking tools.

3. Entities that carry out activities with virtual assets 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 12

Specific procedures and information systems

1. For the purposes of the provisions of Article 19(2)(b) of the Law, entities that carry out activities with virtual assets shall consider the following sources of information, in addition to those provided for in Article 9 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, and also as part of the updating procedures provided for in Article 42 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 and Article 7 of this Notice;

   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 13

Procedures for differentiating occasional transactions from business relationships

1. Entities that carry out activities with virtual assets equip their internal control systems with the means and procedures to differentiate customers engaged in occasional transactions from 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, entities that carry out activities with virtual assets 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 14

Procedures and centralised records for occasional transactions

1. Entities that carry out activities with virtual assets equip their internal control systems with the means and procedures to enable them to verify the existence of seemingly linked transactions, as provided for in Article 23(1)(b) of the Law.
2. In defining the means and procedures referred to in the preceding paragraph, entities that carry out activities with virtual assets take into account the following indicative criteria for the existence of linked 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 entity that carries out activities with virtual assets, as provided for in Article 14 of the Law.
3. In order to assess the criterion set out in point a) of the previous paragraph, entities that carry out activities with virtual assets consider, along with other elements, the use or existence of addresses or wallets, hashes or common Internet Protocol (IP) addresses.
4. Without prejudice to the provisions of paragraph 2, entities that carry out activities with virtual assets 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 operation carried out by the customer or group of customers recognised as related to each other.
5. In order to ensure effective control of the limit set out in Article 23(1)(b)(ii) of the Law, entities that carry out activities with virtual assets implement a

computerised and centralised record of all occasional transactions carried out, regardless of their amount, in order to identify the splitting of operations.

6. Entities that carry out activities with virtual assets ensure that the record referred to in the previous 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 they carry out an occasional transaction;

   c) Is permanently available to the entire organisational structure.

Article 15

Duty to identify collaborators

Collaborators of entities that carry out activities with virtual assets 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

1. The outsourcing of processes, services or activities related to compliance, by entities that carry out activities with virtual assets, with the duties laid down in the Law and in this Notice shall comply with the provisions of this article, even when using service providers that are part of the same group.

2. Entities that carry out activities with virtual assets are solely responsible for complying with the provisions of the Law and this Notice, including those related to the 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 policies, procedures and controls of the entity that carries out activities with virtual assets, as well as their revision in accordance with the provisions of Article 12 of the Law and Article 8 of this Notice;

   b) The approval of the risk management model of the entity that carries out activities with virtual assets and its revision in accordance with the provisions of Articles 14 and 15 of the Law and Article 8 of this Notice;

   c) The outlining of characterising elements or indicators for detecting unusual or potentially suspicious conducts, 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 entity that carries out activities with virtual assets or outlined by Banco de Portugal in a Circular Letter.

4. Entities that carry out activities with virtual assets are prohibited from engaging service providers established in countries with legal frameworks that include prohibitions or restrictions preventing or limiting compliance by those entities 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, entities that carry out activities with virtual assets 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;
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 they outsource processes, services or activities, entities that carry out activities with virtual assets 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;
    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 entity that carries out activities with virtual assets to maintain the ultimate decision-making power regarding the outsourcing relationship;

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 employees with training in the prevention of money laundering and terrorist financing, in accordance with the provisions of Article 55 of the Law and Article 48 of this Notice;

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;

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;

g) Permanently monitor the quality, adequacy and effectiveness of the outsourced processes, services or activities, and ensure that any errors or weaknesses that may be identified are corrected in good time, failing which the outsourcing contractual relationship will be terminated;

h) 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.

Article 17

Reporting irregularities

1. For the purposes of Article 20(7) of the Law, entities that carry out activities with virtual assets must prepare an annual report by 28 February of each year which, in relation to the period between 1 January and 31 December of the previous year, shall contain 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. In accordance with Article 20(5) of the Law, the report referred to in the preceding paragraph shall be kept pursuant to Article 51 of the Law and Article 45 of this Notice and made permanently available to the Banco de Portugal.

Article 18

Restrictive measures

1. In order to comply with the provisions of Article 21 of the Law and Article 10(3) of Law no. 97/2017, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets shall have permanent, fast and secure mechanisms in place that ensure the immediate, full and effective enforcement of restrictive measures, and that allow at least for:

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

   b) The blocking or suspension of operations or sets of operations, when the entity that carries out activities with virtual assets 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 no. 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 no. 97/2017.

3. Entities that carry out activities with virtual assets 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 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 45 of this Notice.
7. Whenever entities that carry out activities with virtual assets 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

Group policies

Compliance with the duty to inform set out in Article 22(8)(b) of the Law is ensured by entities that carry out activities with virtual assets by sending the Banco de Portugal, under the terms and through the channels set out in Article 51 of this Notice, a specific communication that identifies:

a) The host country;
b) The impediments or limitations, found in the law of the host country, to compliance with the provisions of Article 22(4)(6)(7) of the Law;
c) The additional measures adopted under Article 22(8)(a) of the Law.

Rectified by Statement of Rectification no. 371/2023, of 9 May.

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, entities that carry out activities with virtual assets also collect information about their prior occupation.
2. Whenever they collect and record identifying information concerning sole proprietors, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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 management 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 support 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, entities that carry out activities with virtual assets collect a plain copy, in hard copy or electronic format, 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.

7. The supporting documents collected by entities that carry out activities with virtual assets 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 42 of this Notice.

Article 22

Beneficial owners

1. Entities that carry out activities with virtual assets 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 entities that carry out activities with virtual assets 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 entity that carries out activities with virtual assets, prior to establishing the business relationship, documents in writing the circumstances that confirm to 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. Entities that carry out activities with virtual assets immediately verify the identity of the beneficial owner, under the terms set out in Article 32(2) or (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 entities that carry out activities with virtual assets based on internally established 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 43 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. 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 entity that carries out activities with virtual assets 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 entities that carry out activities with virtual assets 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. Entities that carry out activities with virtual assets 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 entities that carry out activities with virtual assets ascertain that the operations 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 and virtual assets

1. For the purposes of Article 27(b) of the Law and the assessment to be made by entities that carry out activities with virtual assets to the need to obtain information about the source or destination of funds handled as part of a business relationship or when carrying out a occasional transaction, special consideration is given to, among other internally outlined 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, entities that carry out activities with virtual assets deem suitable, appropriate and sufficient.

3. Whenever, during the course of the business relationship or subsequent occasional transactions, entities that carry out activities with virtual assets find that the operations 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.

4. Entities that carry out activities with virtual assets obtain information on the source or destination of virtual assets handled within the scope of a business relationship or when carrying out a occasional, when the customer's risk profile or the characteristics of the operation so justify, and the provisions of this article shall apply, with the specificity provided for in the following paragraph.

5. For the purposes of the previous paragraph, when complying with paragraph 2(b), entities that carry out activities with virtual assets give particular consideration to the use of the following supporting documents:

   a) Information obtained from network analysis tools that use distributed ledger or similar technology;

   b) Transaction history associated with addresses or wallets held by the customer;

   c) Receipts or other forms of documentation of the initial acquisition or exchange of the virtual assets.

6. Without prejudice to compliance with the other obligations and duties laid down in the Law and in this Notice, when providing exchange services between virtual assets and fiat money, or between virtual assets, entities that carry out activities with virtual assets collect the supporting documents and adopt the measures that, depending on the specifically identified risk, ensure that:

   a) The customer is the holder of the account or of the payment instrument or of the electronic money of source or destination of the fiat money subject to the exchange operation;

   b) The customer is the owner or holder of the wallet of source or destination of the virtual assets subject to the exchange transaction.

Article 25

Activity characterisation

1. In order to comply with the provisions of Article 27(c) of the Law, entities that carry out activities with virtual assets:

   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, entities that carry out activities with virtual assets deem suitable, appropriate and sufficient.

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

Article 26

Deferred verification of identifying information and limits to the movement of fiat money and virtual assets

1. For the purposes of Article 26(3) of the Law, entities that carry out activities with virtual assets 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. Whenever they make use of the option conferred by Article 26(3) of the Law, entities that carry out activities with virtual assets do not allow, beyond the initial delivery of fiat money or virtual assets, the execution of any operations by or on behalf of the customer, nor do they carry out changes of ownership, until the identity verification process is completed.
3. 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.
4. Entities that carry out activities with virtual assets 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 44 of this Notice.

Article 27

Additional information and supporting documents

In accordance with Article 28 of the Law, whenever the risk analysis conducted by entities that carry out activities with virtual assets regarding the business relationship or occasional transaction justifies an increased level of knowledge about the customer, their representative or 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, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets 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 employee of the entity who is not directly involved in the business relationship with the customer, under their supervision.

SUBSECTION II

Simplified Measures

Article 29

Simplified Measures

1. For the purposes of Article 35 of the Law, entities that carry out activities with virtual assets 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, entities that carry out activities with virtual assets:
   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 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 entities that carry out activities with virtual assets 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 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.

SUBSECTION III

Enhanced measures

Article 30

General provisions

1. In accordance with the provisions of Article 36(1) to (3) of the Law, entities that carry out activities with virtual assets adopt, in addition to those provided for in the Law and in this Notice, 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 the entities that carry out activities with virtual assets under the scheme provided for in Article 36(4) of the Law.
3. For the purposes of adopting enhanced measures, entities that carry out activities with virtual assets outline different levels of high risk that reflect their specific operating reality, including at least the aspects set out in Article 14(2)(a) and Article 15, both of the Law, and in article 7 of this Notice, and review them in accordance with the provisions of Article 8 of this Notice.

Article 31

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 and virtual assets 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, entities that carry out activities with virtual assets

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, entities that carry out activities with virtual assets consider using 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, entities that carry out activities with virtual assets 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 a occasional transaction outside their home jurisdiction.
5. For the purposes of the previous paragraph, in order to ascertain the connection of the customer, their representative or the beneficial owner with other jurisdictions, entities that carry out activities with virtual assets consider, in particular, the use of Internet Protocol (IP) address tracking tools.
6. In addition to reducing the time interval for updating information as provided for in Article 36(6)(e) of the Law, entities that carry out activities with virtual assets 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.
7. 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 32

Product, service, transaction or distribution channel

1. Whenever they identify a situation of increased risk associated with a product, service, transaction or distribution channel, entities that carry out activities with virtual assets 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) Limiting or restricting transactions with certain types of virtual assets;
   f) Requirement to carry out transactions through traceable means, namely through an account opened with a financial or other legally authorised entity or through a wallet hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature 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 in this Notice;
   g) Parameterisation of 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. Entities that carry out activities with virtual assets 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.
3. In addition to other situations identified by entities that carry out activities with virtual assets, the provisions of this article are always applicable to products, services or operations that:
   a) In any way relate to:
      i) Virtual assets that can offer a higher level or guarantee of anonymity ('anonymity enhanced coins' - AECs or 'privacy coins');
      ii) Services for anonymising transactions with virtual assets, including through the use of mixers, tumblers or anonymizers, or virtual private network (VPN) services;
   b) Involve the use of ATMs to exchange virtual assets and cash;
   c) Involve the use or acceptance of cash payments, anonymous electronic money, including the use of anonymous prepaid instruments.

Article 33

Remote contracting

For the purposes of Article 38(2) of the Law, whenever entities that carry out activities with virtual assets identify an increased risk associated with the business relationship or occasional transaction, they consider adopting the following measures:

a) Obtaining additional information about customers, their representatives or beneficial owners, as provided for in Article 36(6)(a) of the Law and Article 31 of this Notice;

b) Carrying out additional due diligence to verify the information obtained, as provided for in Article 36(6)(b) of the Law and Article 31 of this Notice;

c) Requiring the carrying out of transactions through traceable means, namely through an account opened with a financial or other legally authorised entity or through a wallet hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature 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 in this Notice, as provided for in Article 36(6)(g) of the Law.

Article 34

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, entities carrying out activities with virtual assets 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 origin and destination of transactions.

Article 35

Omnibus wallet

Entities that carry out activities with virtual assets using omnibus wallets guarantee the traceability of any transaction to or from that wallet, in a manner that allows identifying the source and destination of the virtual assets underlying each transaction, as needed.

Article 36

Pooled wallets

1. In addition to adopting all required identification and due diligence procedures, entities that carry out activities with virtual assets treat as beneficial owners the customers of the customer

holding a pooled wallet, 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 wallets, entities that carry out activities with virtual assets 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, and in Article 31 of this Notice;

   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 37

Transfers of virtual assets sent

1. Entities that carry out activities with virtual assets shall comply with the provisions of this article with regard to transfers of virtual assets that, regardless of their value, they send on behalf of a customer (originator).

2. Entities that carry out activities with virtual assets ensure that the transfers of virtual assets they send are accompanied by the following information:

   a) Regarding theoriginator:

      i) Full name;

      ii) In the case of transfers of virtual assets registered on a network using distributed ledger technology or a similar technology, the distributed ledger address or addresses and, if there is one and is used to process the transfer, the internal identification number of the customer's wallet;

      iii) In the case of transfers of virtual assets not registered in a network using distributed ledger technology or similar, the internal identification number of the wallet or, if there is none, the single transaction identifier (hash).

      iv) Full residential address, official identification document number and customer identification number or, alternatively, date and place of birth;

   b) Regarding the beneficiary:

      i) Full name;

      ii) In the case of transfers of virtual assets registered on a network using distributed ledger technology or similar technology, the

distributed ledger address or addresses and, if there is one and it is used to process the transfer, the internal identification number of the wallet with the entity that carries out activities with virtual assets or the entity of an equivalent nature receiving the transfer on behalf of the beneficiary;

iii) In the case of transfers of virtual assets not registered in a network using distributed ledger technology or similar technology, the internal identification number of the wallet with the entity that carries out activities with virtual assets or the entity of an equivalent nature receiving the transfer on behalf of the beneficiary or, if there is none, the single transaction identifier (hash).

3. The information contained in the previous paragraph does not have to be directly coupled or included in the transfer of virtual assets, as long as it is submitted, through secure channels, prior to or at the same time as the execution of the transfer.

4. Before carrying out the transfer of virtual assets, the entity that carries out activities with virtual assets shall verify the accuracy of the information on the originator referred to in paragraph 1(a), on the basis of documents or information obtained from sources of information considered reliable, credible and sufficient;

5. The verification referred to in the previous paragraph is considered to have been carried out if:

   a) The identity of the originator has been verified or updated in accordance with subsections I to IV of section III of Chapter IV of the Law and Chapter II of this Notice;

   b) The information obtained has been retained in accordance with Article 51 of the Law and Article 45 of this Notice.

6. Without prejudice to the provisions of Article 50 of the Law and Article 44 of this Notice, entities that carry out activities with virtual assets refuse to initiate or execute any transfer of virtual assets before ensuring full compliance with this article.

7. In the case of transfers of virtual assets in batches from a single originator, the provisions of this article shall not apply to individual transfers grouped in that batch, provided that, cumulatively:

   a) The respective file contains the information referred to in paragraph 2;

   They are rectified by Statement of Rectification no. 371/2023, of 9 May.

   b) The information referred to in the previous point has been verified in accordance with paragraphs 4 and 5; and

   c) Individual transfers contain the information referred to in paragraph 2(a)(iii) and 2(b)(iii).

   They are rectified by Statement of Rectification no. 371/2023, of 9 May.

Article 38

Transfers of virtual assets received

1. Entities that carry out activities with virtual assets shall comply with the provisions of this article with regard to transfers of virtual assets that, regardless of their value, they receive on behalf of a customer (beneficiary).
2. Entities that carry out activities with virtual assets apply effective procedures, including, where appropriate, real-time or *ex post* monitoring of transfers, to detect whether the originator and beneficiary information referred to in paragraph 2(a) and (b) of the preceding Article is included in or accompanies the transfer of virtual assets or the transfer of virtual assets in batches.
3. Before making virtual assets available to the beneficiary, entities that carry out activities with virtual assets verify the accuracy of the information on the beneficiary referred to in paragraph 2(b) of the preceding article, on the basis of documents or information obtained from sources of information considered reliable, credible and sufficient.
4. The verification referred to in the previous paragraph is considered to have been carried out if:
   a) The identity of the beneficiary has been verified or updated in accordance with subsections I to IV of section III of Chapter IV of the Law and Chapter II of this Notice;
   b) The information obtained has been retained in accordance with Article 51 of the Law and Article 45 of this Notice.
5. Entities that carry out activities with virtual assets implement effective risk-based procedures, in accordance with the Law and this Notice, to determine when to execute, reject or suspend a transfer of virtual assets that is not accompanied by the required complete information on the originator or beneficiary referred to in paragraph 2 of the previous article, and to take appropriate follow-up measures.
6. When applying the risk-based procedures referred to in the previous paragraph, entities that carry out activities with virtual assets take into account the procedures adopted in compliance with the provisions of Article 28 of the Law and Article 27 of this Notice.
7. At the time of receiving transfers of virtual assets, should they become aware that the information on the originator or beneficiary referred to in paragraph 2(a) and paragraph 2(b), respectively, of the previous article is missing or incomplete, the entities that carry out activities with virtual assets, depending on the specifically identified risk and without undue delay:
   a) Reject the transfer or return the transferred virtual assets to the distributed ledger address; or
   b) Ask the entity that carries out activities with virtual assets or an entity of an equivalent nature for the missing information required about the originator or the beneficiary before making the virtual assets available to the beneficiary.

8. Without prejudice to the following paragraph, entities that carry out activities with virtual assets regard the omission or incompleteness of the required information on the originator or beneficiary as a factor to be taken into account:

   a) To apply enhanced identification and due diligence measures to the business relationship, occasional transaction or operation, in accordance with the Law and this Notice;

   b) Within the framework of the duty of examination provided for in Article 52 of the Law and Article 46 of this Notice, to ascertain the possible suspicious nature of the transfer of virtual assets, or of any related operation, for the purpose of complying with the reporting duty provided for in Articles 43 and 44 of the Law.

9. In complying with this Article, where they identify entities that carry out activities with virtual assets or entities of an equivalent nature that repeatedly fail to provide, or provide incompletely, the required information on the originator or beneficiary, entities that carry out activities with virtual assets take appropriate measures to address the deficiencies detected.

10. For the purposes of the previous paragraph, the following are examples of measures to be adopted by entities that carry out activities with virtual assets:

    a) At an early stage, set an additional deadline for the provision of the required information on the originator or beneficiary or issue a notice indicating the measures that will be taken if the entity that carries out activities with virtual assets or an entity of an equivalent nature continues to fail to provide the requested information;

    b) Reject any future transfers of virtual assets to or from the entity that carries out activities with virtual assets or an entity of an equivalent nature;

    c) Restrict or terminate the business relationship with the entity that carries out activities with virtual assets or an entity of an equivalent nature, in cases where the risk associated with it cannot be managed through other means or procedures, including through the application of the enhanced due diligence identification measures provided for in Article 41.

    They are rectified by Statement of Rectification no. 371/2023, of 9 May.

11. In the cases provided for in paragraphs 9 and 10, entities that carry out activities with virtual assets shall notify the Banco de Portugal, through the channels referred to in Article 51, within a maximum period of three months:

    a) The identification of the entity that carries out activities with virtual assets or an entity of an equivalent nature that repeatedly fails to provide, or provides incompletely, the required information on the originator or beneficiary, indicating, among other elements, the country where it is authorised or registered;

    b) The nature of the omission or incompleteness, including:

       i) The frequency of transfers of virtual assets with omissions or incomplete information;

       ii) The period of time during which the omissions or incompleteness occurred;

iii) The possible reasons invoked by the entity that carries out activities with virtual assets or an entity of an equivalent nature to justify the repeated omission or incompleteness of the required information.

c) A description of the measures adopted under the preceding paragraph.

12. The reporting obligation set out in the preceding paragraph applies without prejudice to the obligation to report suspicious transactions, in accordance with Articles 43 and 44 of the Law.

Article 39

Transfers of virtual assets from or to self-hosted addresses

1. Regarding transfers of virtual asset from or to self-hosted addresses, entities that carry out activities with virtual assets:

   a) Obtain and retain the information on the originator and the beneficiary referred to in Article 37(2)(a) and (b) respectively, in such a way as to ensure that the transfer of virtual assets can be individually identified;

   b) Adopt enhanced identification and due diligence measures appropriate to the increased risk level associated with the transaction.

2. Without prejudice to the adoption of other measures that are appropriate to mitigate the risks identified, regarding transfers of virtual assets that they send or receive on behalf of a customer (originator or beneficiary, respectively) for an amount higher than €1,000, entities that carry out activities with virtual assets adopt measures that, depending on the specifically identified risk, ensure that the self-hosted address is held by the customer, whenever they declare that they are the originator or beneficiary, as the case may be, of the transaction.

Article 40

Intermediated transfer of virtual assets

1. Entities that carry out activities with virtual assets comply with the provisions of this article with regard to transfers of virtual assets that, regardless of their value, they receive and send on behalf of another entity that carries out activities with virtual assets or an entity of an equivalent nature.

2. Entities that carry out activities with virtual assets shall ensure that all information received about the originator and the beneficiary referred to in Article 37(2)(a) and (b), respectively, that is included in, or accompanies, a transfer of virtual assets is:

   a) Transmitted with the transfer, and the provisions of Article 37(3) shall apply;

   b) Retained in accordance with the provisions of Article 51 of the Law and Article 45 of this Notice; and

   c) Made available at the request of the Banco de Portugal.

3. Entities that carry out activities with virtual assets shall also comply with the provisions of Article 38(5) to (12), *mutatis mutandis*, regarding the transfers of virtual assets referred to in this article.

Rectified by Statement of Rectification no. 371/2023, of 9 May.

Article 41

Business relationships with entities of an equivalent nature or with financial entities

1. Entities that carry out activities with virtual assets ('correspondent') apply the following enhanced measures to the business relationships they establish with entities of an equivalent nature or with financial or other entities of an equivalent nature based abroad ('respondents') to provide one or more of the services with virtual assets provided for in Article 2(1)(mm) of the Law:

   a) Carry out the normal identification and due diligence procedures provided for in the Law and in this Notice, including the identification, assessment and review of money laundering and terrorist financing risks specifically associated with the business relationship;

   b) Collect enough information about the respondents in order to:

      i) Understand the nature of their activity and the money laundering and terrorist financing risks associated with it;

      ii) Assess, on the basis of public information, its reputation and the quality of its supervision, including any history of investigative or sanctioning procedures in relation to money laundering or terrorist financing;

   c) Critically assess the policies, procedures and internal controls outlined and adopted by the respondents with a view to preventing money laundering and terrorist financing;

   d) Obtain the approval of top management before establishing new business relationships;

   e) Set out in a written document the responsibilities of the parties involved in the business relationship;

   f) In order to provide a portfolio that respondents' customers can access directly, they ensure that the respondents:

      i) Verify the identity of customers with direct access to the portfolio, their representatives and beneficial owners, under the same terms provided for by the Law and this Notice;

      ii) Continuously monitor the business relationships established;

      iii) Whenever requested, they are able to provide information on the fulfilment of the duty of identification and due diligence.

2. In assessing the specific risk associated with the business relationship referred to in paragraph 1(a), the correspondents, without prejudice to the sources of information referred to in Article 9 of

this Notice and the other elements assessed in compliance with the normal and enhanced procedures of identification and due diligence, give particular consideration to the following factors:

a) Whether the respondent is an entity authorised or registered to carry out activities with virtual assets;

b) The jurisdiction in which the respondents are located;

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

d) The management and control structure of the respondents, including the respective beneficial owners;

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

f) The reputation, main business areas, customer base, target market segments and jurisdictions in which the respondents operate;

g) The risks associated with the specific services to be provided to respondents by the correspondents;

h) The likelihood of the practices outlined in point f) of the preceding paragraph occurring and, in particular, the accessibility of information regarding any third parties that may use the services of the correspondents.

3. The establishment of business relationships in accordance with this article are always subject to the prior opinion of the AML/CFT compliance officer resulting from all the due diligences implemented under paragraph 1(a) to (c).

4. The information collected under the provisions of paragraph 1(a) to (c) are updated according to the degree of risk associated with the business relationships established, and the provisions of Article 40 of the Law and Article 42 of this Notice apply *mutatis mutandis*.

5. Without prejudice to existing obligations to comply with financial sanctions arising from a United Nations Security Council resolution or European Union regulation, as well as other additional countermeasures, the correspondents permanently and intensively monitor the transactions carried out as part of business relationships, in terms that allow them to assess:

a) The consistency of those transactions with the risks identified and with the purpose and nature of the services contracted under the business relationship;

b) The existence of any operations that must be reported in accordance with Article 43 of the Law;

6. In compliance with the provisions of the preceding paragraphs, when correspondents detect the existence of characterising elements that should motivate the exercise of the duty of examination provided for in Article 52 of the Law and Article 46 of this Notice:

a) They ask respondents for any additional information relevant to exercising that duty;

b) In the event of total or partial failure by respondents to provide information, they apply the measures provided for in Article 50 of the Law and Article 44 of this Notice, without prejudice to adopting other appropriate measures to manage the specific risk identified when termination of the relationship is not required, including, if necessary, limiting the operations carried out or the products offered as part of the relationship.

SECTION III

Obligation to update

Article 42

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 45 of this Notice.
2. In addition to the situations listed in Article 40(4) of the Law, entities that carry out activities with virtual assets 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. Entities that carry out activities with virtual assets expressly include in the contractual clauses governing their relationships with customers 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 43

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

1. In accordance with the provisions of Article 41(1) of the Law, entities that carry out activities with virtual assets may rely on third-party entity to perform the identification and due diligence procedures, provided that the latter is:
   a) One of the financial 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) An entity that carries out activities with virtual assets or an entity of an equivalent nature.

2. Without prejudice to the provisions of Article 41(4) of the Law, entities that carry out activities with virtual assets are also prohibited from relying on third-party entities established in countries with legal systems that provide for prohibitions or restrictions that prevent or limit the compliance of entities that carry out activities with virtual assets 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 resort to the execution of identification and due diligence procedures by third-party entities, entities that carry out activities with virtual assets 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 perform 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 48 of this Notice;

   c) The internal records supporting the identification and due diligence procedures performed 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, entities that carry out activities with virtual assets may use the third-party entities mentioned in paragraph 1 that are part of the same group.

CHAPTER III
Other duties

Article 44
Duty of refusal

1. In the situations provided for in Article 50(2) and (3)(b) of the Law, entities that carry out activities with virtual assets, once the decision to terminate the business relationship has been made:

   a) Prohibit any transactions 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 support to which the virtual assets or fiat money should be returned or

personally appear before the entity that carries out activities with virtual assets to perform the return in accordance with paragraphs 3 and 4;

c) Hold the virtual assets or fiat money, keeping them unavailable until they can be returned.

2. When contacting the entity that carries out activities with virtual assets, if the customer provides the missing information that led to the decision to terminate the business relationship, and there is no suspicion, the entity that carries out activities with virtual assets can restore 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 the virtual assets or fiat money referred to in Article 50(6) of the Law is made by entities that carry out activities with virtual assets through one of the following means:

   a) Regarding fiat money:

      i) 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;

      ii) Crossed and non-negotiable cheque in favour of the customer, drawn on the financial entity or another legally authorised entity in which the entity that carries out activities with virtual assets has an open account, with an explicit mention of the reason for payment on the cheque;

   b) Regarding virtual assets, by transfer to:

      i) Hosted wallet of the customer hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature 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 in this Notice, including the reason for the transfer among the elements to be communicated about the originator in accordance with and for the purposes of Article 37(2)(a);

      Rectified by Statement of Rectification no. 371/2023, of 9 May.

      ii) Self-hosted address demonstrably under the effective control of the customer, provided that the customer is not the holder of hosted wallets that comply with the requirements referred to in the preceding point.

4. In the situations provided for in Article 26(4) of this Notice, entities that carry out activities with virtual assets make the refund referred to in the preceding paragraph:

   a) In the case of fiat money, through the means provided for in point a) of the preceding paragraph;

   b) In the case of virtual assets, through the means used for the initial transfer, in accordance with point b) of the preceding paragraph.

5. Any documentation provided upon the termination of the business relationship or the refund of the respective virtual assets or fiat money 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, entities that carry out activities with virtual assets consult the competent judicial and law enforcement authorities before proceeding with any refund of the virtual assets or fiat money under this article.
7. When terminating a business relationship based on the existence, according to internally set criteria, of an increased risk of money laundering or terrorist financing that does not constitute a legal basis for exercising the duty of refusal, entities that carry out activities with virtual assets comply, *mutatis mutandis*, with the 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 45

Duty of retention

1. 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.
2. Information recorded in a public, permanent and accessible manner on a network that uses distributed ledger technology or a similar technology does not remove the need for entities that carry out activities with virtual assets to retain and file that information in accordance with Article 51 of the Law and with this article.

Article 46

Duty of examination

1. In the situations specified in Article 52(4) of the Law, entities that carry out activities with virtual assets 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. By means of a Circular Letter, the Banco de Portugal disseminates and updates an illustrative list of potential indicators of suspicion, listing behaviours, activities or transactions that may be related to criminal activities or with money laundering or terrorist financing.

Article 47

Duty of non-disclosure

To comply with the duty of non-disclosure laid down in Article 54 of the Law, entities that carry out activities with virtual assets 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 48

Duty of training

1. Entities that carry out activities with virtual assets define 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 or monitoring authorities, or associations representing the sector;
   d) The risks, types, and methods associated with funds, virtual assets 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 that carries out activities with virtual assets, along with the distribution channels for these products and services and the means of communication used with customers.
   f) Network analysis tools that use distributed ledger technology or similar technology associated with the virtual assets and operations made available, as well as their traceability guarantees;
   g) Reputational risks and the administrative consequences resulting from failure to comply with the duties to prevent money laundering and terrorist financing;
   h) 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 basic principles of the internal control system of the entity that carries out activities with virtual assets, 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 entity that carries out activities with virtual assets, 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.

TITLE III
Supplementary provisions

Article 49
Portuguese language

1. Entities that carry out activities with virtual assets prepare and maintain a permanently updated Portuguese version of their procedure manuals or any other relevant internal documents or records on the prevention of money laundering and terrorist financing, as well as the opinions, examinations, analyses and information reports referred to in the Law or in this Notice.

2. When the evidentiary documents referred to in Article 51 of the Law and Article 45 of this Notice are not written in Portuguese, entities that carry out activities with virtual assets are obliged to:

Rectified by Statement of Rectification no. 371/2023, of 9 May.

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 50

Equivalent amount in foreign currency or virtual asset

Any reference in this Notice to amounts expressed in euros shall also be deemed made for an equivalent amount expressed in any other foreign currency or in the price of the currency of the virtual assets, at the exchange rate of the end of the previous day, as applicable.

Article 51

Communication channels

1. Entities that carry out activities with virtual assets participate in the BPnet System, in accordance with Instruction no. 21/2020 of 15 July.
2. Unless otherwise provided for by a rule or determination of the Banco de Portugal, communications made by entities that carry out activities with virtual assets 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.
3. Entities that carry out activities with virtual assets 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.
4. Communications sent by the Banco de Portugal to entities that carry out activities with virtual assets 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 IV

Transitional and final provisions

Article 52

Transitional rule

1. In order to comply with the duty to update the information on business relationships already established on the date of entry into force of this Notice, entities that carry out activities with virtual assets:
   a) Immediately carry out the updating procedures referred to in Article 40 of the Law and Article 42 of this Notice, in cases where it is shown that the period internally established by the entity that carries out activities with virtual assets for each category of risk associated with customers, counting from the date of the start of the business relationship or from the date of the last information update, has elapsed;
   b) Ensure the updating procedures as it is shown that the period internally set by the entity that carries out activities with virtual assets for each category of risk associated with customers, counting from the date of the start of the business relationship or from the date of the last information update, has elapsed;

2. The provisions of the preceding paragraph are without prejudice to the immediate updating obligations laid down in Article 40(4) of the Law and other applicable legal and regulatory provisions.

Article 53

Amendment to Banco de Portugal Notice no. 1/2022

1. Article 8 of Banco de Portugal Notice no. 1/2022 of 6 June is replaced by the following:

«Article 8 [...]

1. [...]
2. [...]
3. [...]
   a) Information, guidelines or alerts issued or disseminated by the Banco de Portugal;
   b) Information, guidelines or alerts from the FIU or other judicial and police authorities;
   c) […]
   d) Information, guidelines or alerts issued by the European Banking Authority, the Financial Action Task Force or the European Commission;

e) […]

   f) […]
   g) […]
4. [...]"

2. Article 16 of Banco de Portugal Notice no. 1/2022 of 6 June is replaced by the following:

«Article 16

Outsourcing

1. [...]
2. [...]
3. [...]
4. [...]
5. [...]
   a) […]
   b) […]
   c) […]
   d) *(repealed);*
   e) *(repealed).*
6. [...]
7. [...]
   a) […]
   b) Review, with a frequency appropriate to the identified risks, the relevance of the practices referred to in paragraph 5;

c) *[former point b)];*
d) *[former point c)];*
e) *[former point d)];*
f) *[former point e)];*
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.

3. Article 21 of Banco de Portugal Notice no. 1/2022 of 6 June is replaced by the following:

«Article 21
[…]

1. [...]
2. [...]
3. [...]
4. [...]
5. [...]
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.
7. […]»

4. Article 43 of Banco de Portugal Notice no. 1/2022 of 6 June is replaced by the following:

«Article 43
[...]

1. [...]
2. [...]
3. Entities that carry out activities with virtual assets apply, *mutatis mutandis*, the measures provided for in Article 70 of the Law and in this article within the scope of business relationships they establish with the entities referred to in Article 2(1)(l) of Banco de Portugal Notice no. [•]/2022, of [•] [•]».

Article 54
Entry into force

1. This Notice shall enter into force on 15 July 2023, without prejudice to the provisions of the following paragraph.
2. For the purposes of the provisions of Article 25(4)(c)(i) of the Law, entities with virtual assets may use videoconference as an alternative procedure for verifying identifying information as of the publication of this Notice, complying for this purpose with the requirements set out in Annex I to this Notice.

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. Entities that carry out activities with virtual assets may verify the identifying information referred to in Article 24(1)(a)(i) to (vii) of the Law using videoconference, as specified 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 Article 29 of this Notice.
3. The use of videoconference does not exempt entities that carry out activities with virtual assets from complying with the obligations arising from the duty of identification and due diligence, as well as the other duties arising from the Law and this Notice:
   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 12 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 of this Notice, the risk analysis carried out on a case-by-case basis by entities that carry out activities with virtual assets regarding 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. Prior to the adoption of videoconference as a procedure for verifying identifying elements, entities that carry out activities with virtual assets:

   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, entities that carry out activities with virtual assets 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 45 of this Notice.

Article 3

Safeguards

1. Whenever entities that carry out activities with virtual assets use videoconference as a procedure for verifying identifying information:

   a) Require the initial delivery of fiat money or virtual assets to be carried out through traceable means which allow identifying the originator, through an account opened with a financial or other legally authorised entity or through a wallet hosted with an entity that carries out activities with virtual assets or an entity of an equivalent nature 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 in 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. Entities that carry out activities with virtual assets apply enhanced identification and due diligence measures proportional to the risk identified, whenever the initial delivery of fiat money or virtual assets, as provided for in point a) of the previous paragraph, originates from an account or wallet, respectively, 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, entities that carry out activities with virtual assets:

   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 entity that carries out activities with virtual assets 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 ensured 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 48 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 entity that carries out activities with virtual assets 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, in accordance with Article 51 of the Law and Article 45 of this Notice.

Article 6

Technical requirements

Entities that carry out activities with virtual assets 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 entity that carries out activities with virtual assets 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.
5. 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 rectified by Statement of Rectification no. 371/2023, of 9 May.

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 entities that carry out activities with virtual assets
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, entities that carry out activities with virtual assets also take into account, whenever available, the information provided by the supervisory authorities of their respective sectors regarding their operating rules. 3. Entities that carry out activities with virtual assets 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 prove with documents 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, entities that carry out activities with virtual assets, 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.
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-party 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, entities that carry out activities with virtual assets 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 entities that carry out activities with virtual assets with an illustrative list of indicative factors and types of potentially reduced money laundering or terrorist financing risks that should be considered 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, entities that carry out activities with virtual assets may also consider other factors and indicators of potentially lower 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) Products with limited use or specific, pre-determined purposes, such as:
        i) Products with limits on transactions, specifically in relation to the amount of virtual assets transacted;
        ii) Recurring transfers, of the same amount and to the same beneficiary, with apparent economic rationality;
        iii) Products that can only be used within the national territory;
        iv) 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 entity that carries out activities with virtual assets has sufficient knowledge of the activities conducted by the merchants;
    b) Pooled wallets 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;

Form 99999910/T – 01/14

Annex IV to the Notice

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

Other potentially higher-risk situations

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

However, entities that carry out activities with virtual assets must also consider other factors and indicators of potentially higher risk that are appropriate to their specific operating reality. For the purposes of this Annex, the term 'customer' shall be understood as referring, as a rule, not only to the concept set out in Article 2(1)(e) of this Notice, but also to their representatives and 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 3 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;

l) Customers who hold wallets hosted with entities of an equivalent nature that are not registered or licensed with a competent authority;

m) Customers with self-hosted addresses);

n) Customers whose assets or virtual assets portfolio derive to a large extent from investments in virtual assets, resulting from participation in public initial coin offerings, free launches of virtual assets (airdrops), collective reserves of virtual assets for the purpose of providing liquidity (liquidity pools) or other similar situations;

o) Customers that participate in mining operations or mining pools of virtual assets, especially when these operations:

   i) Occur in jurisdictions with an increased risk of terrorist financing;

   ii) Are related to virtual assets that present potentially increased risks of terrorist financing.

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

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

   b) Exchange transactions involving cash and high values, especially using high-denomination banknotes;

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

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

   e) Operations with virtual assets in which the use of tools or practices that make it difficult to identify the chain of transfers, the source or destination of certain virtual assets is detected, such as mixers, tumblers, peer-to-peer (P2P) platforms or virtual private network (VPN) services;

   f) Products, services or operations with virtual assets that facilitate anonymous or pseudo-anonymous transactions, particularly if they inhibit the ability to identify the beneficiary, such as so-called anonymity enhanced coins or privacy coins;

   g) Operations with virtual assets from or to self-hosted addresses);

   h) Operations involving entities of an equivalent nature that are not registered or licensed with a competent authority;

   i) Operations involving entities of an equivalent nature established in jurisdictions that do not have effective systems for preventing and combating money laundering and terrorist financing, without prejudice to the provisions of the Law with regard to high-risk third countries;

3. Risk factors inherent to geographic location:

   a) Jurisdictions that do not have a regulatory and supervisory framework for the prevention of money laundering and terrorist financing applicable to activities with virtual assets;

   b) 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;

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

   d) Jurisdictions that have not implemented the Common Reporting Standard developed by the Organisation for Economic Cooperation and Development (OECD) on the automatic exchange of information");

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

   f) Jurisdictions with legal frameworks that establish prohibitions or restrictions that prevent or limit compliance by the entity that carries out activities with virtual assets with the legal and regulatory standards governing its activity, including in terms of the provision and circulation of information.