Banco de Portugal issues a Notice on the prevention of money laundering in the trading of digital assets

abreuadvogados.com

A. Background of the Notice

The entities that carry out any activity with virtual assets are regulated and supervised for the purposes of prevention of money laundering and terrorist financing (hereinafter "ML/TF"), and are required to comply with the preventive duties of ML/TF under Law No. 83/2017 of 18 August (hereinafter “AML/CFT” or “Law”), which transposes the Directives 2015/849/EU of the European Parliament and of the Council of May 20, 2015, and 2016/2258/EU of the Council of 6 of December 2016, as amended by Law No. 58/2020 of 31 August, which transposes Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018. In addition, Law No. 97/2017 of 23 August, which regulates the application and enforcement of restrictive measures approved by the United Nations or the European Union.

Thus, the Bank of Portugal, in the light of the powers conferred by the Law, regulates, through Notice No. 1/2023 of 24 January 2023 (the “Notice”), the aspects that are required to ensure compliance with the duties to prevent money laundering and terrorist financing in the context of the activities of entities that carry out any activity involving virtual assets.

In this sense, the Bank of Portugal aims to assist entities in fulfilling their ML/TF duties by defining, densifying and implementing the policies, procedures and controls required to comply with the duties set out in the AML-CFT.

Finally, this Notice has also amended Bank of Portugal Notice No. 1/2022 of June 6, only with regard to very limited elements arising from the need to rectify very specific aspects or to establish the way in which financial entities should relate to entities that carry out activities with virtual assets.

B. To whom does it apply?

The Notice is applicable to entities that carry out activities with virtual assets (hereinafter "Entities"), in Portugal, in the name or on behalf of a client, and for this purpose they should be registered with the Bank of Portugal, pursuant to article 112-A of Law No. 83/2017.

Entities that carry out activities with virtual assets are considered to be the entities that perform at least one of the following activities involving virtual assets:

(i) Exchange services between virtual assets and fiat currencies or between one or more virtual assets;
(ii) services whereby a virtual asset is moved from one address or wallet to another (virtual asset transfer); and
(iii) Services of safekeeping, or safekeeping and administration of virtual assets or of instruments that enable the control, ownership, storage or transfer of such assets, including private encrypted keys.

Hence, if an entity performs activities with virtual assets, but these are not included in the provisions of paragraph mm), it may be concluded that it will not be subject to the duties of ML/TF.

In light of Article 6(4) of Law No. 83/2017, the following persons or entities are considered to carry out activities with virtual assets in national territory:

a) Legal persons or entities equivalent to legal persons incorporated in Portugal to carry out activities with virtual assets;
b) Natural persons, legal persons and other entities domiciled in Portugal that conduct activities with virtual assets or that have an establishment located in Portuguese territory through which they conduct activities with virtual assets;
c) Other individuals or entities that, due to the exercise of activities with virtual assets, are required to file a declaration of commencement of activity with the Tax and Customs Authority.

In this sense, as has been reiterated by the supervisor's understanding, the registration with the Bank of Portugal implies the establishment of an effective operation based in Portuguese territory, and not the mere exercise of cross-border operations with the attraction of clients in Portugal from abroad.

C. From when?

The Notice will come into force on 15 July 2023, with the exception of the use of videoconferencing as an alternative procedure for proving the identification elements, under the terms set out in Annex I to the Notice, which will be applicable immediately.

D. What are the main obligations for Entities that conduct activities with virtual assets?

Entities that carry out activities with virtual assets are subject to several preventive duties, among which the following stand out:

- **Duty of Control**

The Entities shall ensure the implementation of a regulatory compliance control function with regard to the prevention of ML/TF, for which purpose they should appoint a AML compliance officer, who will guarantee:

- The definition and effective application of the policies and of the procedures and controls adequate for the effective management of the AML/CFT risks to which the Entity is or may be exposed;
- Compliance with legal and regulatory standards on the prevention of ML/TF.

The aforementioned functions shall be segregated from the activities they monitor and control, unless their number of employees is lower than 6 and the operating income in the last economic year is less than € 1,000,000.00.

Without prejudice to the appointment of a AML compliance officer, the Entity shall additionally assign the ML/TF prevention function to an executive member of the management body. This new requirement seems to extend the provisions of Article 13 of Law No. 83/2017, which gives supervisory entities the power to require the designation of a member of the management body as responsible for the implementation of the regulatory framework of duties in the area of AML/CFT, "whenever appropriate". With Notice No. 1/2023, Banco de Portugal extends this duty to all entities that carry out activities with virtual assets.

Any supervening change in the organisation of the Entities with repercussions on this matter shall be communicated in due time to the Bank of Portugal.

- **Duty of Risk Management**

During the identification of the ML/TF risks, the specific aspects of risk management set out in Article 7 should be taken into account, with emphasis on the following:

- What types of virtual assets will be made available and their characteristics;
- Issuer of each virtual asset made available;
- Total value of the virtual assets made available;
- Execution of virtual asset transfers originating from or destined to self-hosted addresses;
- Nature and scope of each distribution channel used.

Furthermore, the Entities should consider the situations of potentially lower risk and also the situations of potentially higher risk, listed in Annexes II, III and IV of the Notice.

The risk management policies, procedures and controls should be up-to-date, prepared using suitable, credible and diversified sources of information, and monitored annually in an independent manner.

The following procedures and information systems in general should be adopted:

- Adoption of tools that consolidate the records relating to business relations, occasional transactions or operations;
- Adoption of tools that filter addresses or wallets held or associated with clients against "black lists" of entities, addresses or wallets;
- Adoption of tools to detect the use of technologies that allow the obfuscation of identity or location, including through the use of mixers, tumblers or anonymizers, or VPN services;
- Adoption of Internet Protocol (IP) address tracking tools.

- **Duty of Customer Identification and Due Diligence Requirements**

I. Standard Due Diligence Measures

Entities are required to comply with identification and due diligence procedures whenever **(i)** they establish business relationship or **(ii)** they carry out any transaction that exceeds the amount exceeds €1,000.00 (euro), regardless of whether the transaction is carried out through a single operation or several apparently related operations that constitute a transaction executed within the scope of virtual assets whenever.

Within the scope of the identification and due diligence duties, the Entities may apply standard, simplified and enhanced measures, depending on the level of ML/TF risk in consideration.

In this regard, the identifying details of the customers and their representatives should be obtained through the means of proof established in Article 21 of the Regulations. In this regard, Article 21(6) of the Notice provides the possibility of videoconferencing as an alternative procedure for verification of the identification details, under the terms foreseen in Annex I to the Notice.

They are also obliged, under the terms of Article 22 of the Notice, to gather evidence of identification of the beneficial owners on whose behalf the customers are acting or who ultimately control the customers.

In addition to these identification procedures, they shall further proceed to:

- Obtaining information on the purpose and nature of the business relationship (article 23 of the Notice);
- Obtaining information on the origin and destination of the funds and virtual assets (article 24 of the Notice);
- Maintaining a continuous monitoring of the business relationship (article 25 of the Notice).

It should also be noted that entities may only begin a business relationship when all the requirements of Article 26.1 of the Notice have been met, which correspond, in particular, to the identification of the parties and the respective supporting documents.

Finally, it is important to mention that the Entities may adapt the nature and extent of the identity verification and due diligence procedures, depending on the risks associated with the business relationship or occasional transaction, and whenever an increased level of knowledge of the customer, its representative or the beneficial owner is justified, the Entities shall request additional information or elements and a higher level of evidence thereof.

II. Enhanced Due Diligence Measures

With regard to enhanced measures, it is important to highlight the Article 32 of the Notice, which establishes the enhanced measures to be adopted in a situation of increased risk associated with a product, service, operation or distribution channel. Entities should adopt enhanced measures whenever products, services or operations are concerned which:

a) Are related in some particular instance to:
    i. Virtual assets that may offer an enhanced level or guarantee of anonymity ("anonymity enhanced coins" - AECs or "privacy coins");
    ii. Anonymisation services for transactions with virtual assets, including through the use of mixers, tumblers or anonymisers or virtual private network (VPN) services;
b) Involves the use of automated teller machines to exchange virtual assets and cash;
c) Involves the use or acceptance of payments in cash, anonymous e-money, including with the use of anonymous prepaid instruments.

If an Entity provides omnibus wallets in its activity, a matter not previously regulated autonomously, it will have to ensure the traceability of any transaction to or from that

wallet, in terms that allow the identification of the origin and destination of the virtual assets underlying each transaction, whenever necessary.

In the case of pooled wallets, it is clarified that Entities are required to treat the customers of the holder of a pooled wallet as beneficial owners at all times, adopting identification and identity verification measures that are proportional to the risk identified.

E. What are the applicable rules for virtual asset transfers?

The Notice defines a number of rules for the sending and receiving of virtual asset transfers, as well as for virtual asset transfers originating from or destined to self-hosted addresses.

Thus, when sending transfers, the entity that carries out activities with virtual assets will require its customers to provide the necessary information so that the transfer can be executed, namely, the identification of the parties, the address of the distributed registry (in case of use of a distributed registry network), the internal identification number of the customer portfolio or the unique transaction identifier, and in addition, in the case of the payer, the address, tax identification number and citizen card.

The abovementioned information does not have to be included in the transfer, provided that it is previously made available to the entity that carries out activities with virtual assets and that the latter has to ensure that the information provided is credible.

However, in the case of virtual asset transfers received on behalf of a customer, the Entities shall monitor the transfers and implement the necessary procedures to detect whether the necessary information required to process the transfer accompanies it, and before making the virtual assets available to the beneficiary, they should verify whether the documents certifying the sources of information are credible.

In the event that the information is not credible or is missing, the Entity will have to reject the transfer or request the missing information so that it can make the virtual assets available to the beneficiary.

The failure of the Entity to provide the necessary information within the scope of the transfers carried out, on a regular basis, will result in an obligation to report to the Bank of Portugal.

In the case of transfers of virtual assets to or from self-hosted addresses, all the information disclosure and transfer monitoring rules referred to above shall be complied with, in addition to the adoption of enhanced measures depending on the risk of the operation.

F. **Are there increased duties for covered entities in business relationships with foreign entities carrying out activities with virtual assets?**

Yes. Domestic entities that carry out activities with virtual assets are bound to apply a set of enhanced measures in business relationships with equivalent entities that have their registered office located abroad.

Therefore, besides the normal identification procedures, sufficient information on the corresponding foreign entities should be collected in order to ascertain the following

i) Nature of the activity and risks;
ii) Evaluation of reputation and quality;
iii) Critical evaluation of the policies and procedures for money laundering and financing of terrorism;
iv) Top management approval before any business relationship is entered into;
v) Preparation of a written document identifying the responsibilities of the parties.

To determine the risk associated with the business relationship, the Notice determines a set of analysis criteria, such as the base jurisdiction of the entities, the verification of registration and authorisation of the foreign entity for the execution of activities with virtual assets and the management and control structure of the same, including the beneficial owners.

Other criteria will also be used to determine the risk associated with the business relationship, including the jurisdiction of the entity, the management and control structure (including beneficial ownership), the presence of politically exposed persons in the structure, reputation, customer base, target market segment and the jurisdictions in which the correspondents of the entity operate.

The establishment of any business relationship with these entities will always depend on the prior opinion of the person responsible for regulatory control, and operations carried out within the scope of the business relationship are subject to closer monitoring.

G. What are the rules for subcontracting?

The subcontracting of processes, services or activities is the entire responsibility of the Entity that carries out activities with virtual assets, being limited by the Notice to certain operational activities (refer to Article 16 of the Notice).

Hence, the subcontracting of third parties will not be possible in the following activities:

i) The approval of the policies, controls and review procedures;
ii) The approval of the risk management model;
iii) The definition of characterising elements or indicators for detecting unusual or potentially suspicious conduct, activities or operations.

These limitations will also apply to entities that are part of the same group.

The subcontracting process will depend on the prior opinion of the AML compliance officer and the writing of the contract between the subcontracting Entity and its subcontractor.

H. Is it possible to subcontract a third party entity to carry out the identification and due diligence procedures?

Yes. The identification and due diligence procedures may be carried out by a third party entity, provided that it is:

i) A financial entity;
ii) An entity of equivalent nature to foreign-based financial entities;
iii) A branch of the financial entities, established in the national territory or abroad;
iv) An entity that carries out activities with virtual assets or an entity of an equivalent nature.

However, it is forbidden to subcontract entities that are established in countries that impede or prohibit compliance with the legal standards on prevention of money laundering and financing of terrorism, including the provision and circulation of information.

I. Are there other duties for entities that operate with virtual assets?

Yes. Entities that carries out activities with virtual assets are subject to a set of additional duties related to AML/CFT, as determined by Law No. 83/2017 and now densified by the Notice:

- Duty of refusal;
- Duty to preserve;
- Duty of examination;
- Duty of non-disclosure;
- Training duty.

In addition, the duty to prepare an annual report containing a description of the specific, independent and anonymous channels which internally ensure the receipt, processing and filing of reports of irregularities (refer to Article 17 of the Notice).

J. How can we help?

Abreu Advogados has an extensive experience in monitoring registration processes with the Bank of Portugal for entities that carries out activities with virtual assets. In this context, we have advised on the definition of policies and procedures relating to all

types of risks, including operational risk, as well as on matters of prevention of money laundering and terrorist financing and compliance.

Furthermore, we have experience in outsourcing risk management and modelling information security policies adapted to the most demanding international standards, such as ISO 27001.

We have a multidisciplinary team that combines Financial Law and TMT skills and is specialised in emerging technologies, which can provide assistance in the implementation of solutions compatible with the present Notice that translate into an added value for the clients' business.

Thinking about tomorrow? Let's talk today.

Diogo Pereira Duarte – Partner
diogo.p.duarte@abreuadvogados.com

Isabel Pinheiro Torres – Associated Partner
isabel.p.torres@abreuadvogados.com

Rafael Silva Teopisto – Associate Lawyer
isabel.p.torres@abreuadvogados.com

Ana Mafalda Cordeiro – Trainee Lawyer
mafalda.cordeiro@abreuadvogados.com

João Diogo Barbosa – Trainee Lawyer
joao.d.barbosa@abreuadvogados.com