

## AML-CFT Regulations: AMF clarifications regarding the main measures to be implemented by digital assets service providers<sup>1</sup>

### Provisions regarding anti-money laundering and combating the financing of terrorism

Digital assets service providers registered and/or licensed shall comply with several provisions regarding anti-money laundering and combating the financing of terrorism (articles L. 561-2 and seq. of the Monetary and Financial Code). To enable them to better understand the main obligations they shall comply with, the AMF specifies that, in assessing registration<sup>2</sup>/license applications, it will be especially attentive to the following points:

- The **implementation of a risk classification** determining the risk profile of each investor and the level of the vigilance measures to comply with.
- The **classification of the relationship** established with the client as business relationship or occasional relationship, in accordance with the duration of the relationship:
  - **The business relationship** is characterised by the entry into a contract that sets out the performance of several successive transactions or creating obligations on a continuous basis, or, in the absence of a contract, by the regularity of the intervention of the client.
  - **The occasional client** only performs one transaction or several transactions that are closely connected.
- The **implementation of vigilance measures** allowing the identification and the verification of the client identity and, if any, of the beneficial owner(s)<sup>3</sup>.
- In the above mentioned cases, the vigilance measures should be as follows:
  - **the identification of the client**, consisting in collecting the following identity items:
    - for an individual: name and first name, date and place of birth;
    - for a legal entity: legal form, name, registration number and address of the registered office and the address of the actual place of effective management of the activity, if different from the address of the registered office.

---

<sup>1</sup> This document constitutes a summary of the regime applicable and does not provide a full list of the measures to be implemented by the digital assets service providers. They should refer to the whole set of texts relating to anti-money laundering and terrorism financing that are applicable to them.

<sup>2</sup> It is worth to mention that, in the case of registration, the approval of the ACPR is required.

<sup>3</sup> Person who ultimately owns, directly or indirectly, the client or for whom the transaction is performed or the activity is provided.

- The verification of identity**, consisting in collecting any written document with probative force, *i.e.*:
  - for a physical person: an effective official identity document which includes a photograph; and
  - for a legal entity: any act or extract of official register dating less than three months or an extract of the *Journal Officiel*, ascertaining the name, legal form, address of the registered office and the identity of shareholders and executive officers, as well as legal representatives.
  
- In the case where the client is not physically present for being identified, **the implementation of at least one means of electronic identification** certified or attested by the *Agence nationale de la sécurité des systèmes d'information* (ANSSI) as defined in article R. 561-5-1,1°,a) of the Monetary and Financial Code, or **the implementation of at least two complementary measures** among those set out in article R. 561-20 of the Monetary and Financial Code, such as:
  - **collecting of a copy of a complementary document of;** and
  - **the realization of the first payment of the operations** from or to an account opened with a person mentioned in articles 1° to 6° bis of article L. 561-2 of the Monetary and Financial Code established in a Member State of the European Union or a State which is a party to the European Economic Area or in a third-country imposing equivalent obligations regarding anti-money laundering and terrorism financing.
  
- Before the entry into a business relationship or for an occasional client, **the collection of information relating to the purpose and the nature of the relationship and any other relevant information**, if necessary, according to the risks. The information is updated during all the business relationship. The information likely to be relevant is the following:
  - (i) the origin and destination of the funds, (ii) the economic justification declared by the client, (iii) the professional activities currently performed by the client, (iv) the income or any element allowing to assess the other resources of the client, (v) any element allowing to assess the assets of the clients, (vi) the mandates and powers and (vii) any element allowing to assess the financial situation for legal entities.
  
- The **implementation of strengthened vigilance measures**:
  - when a product or a transaction contains a high risk of money laundering and terrorism financing; and
  - for any transaction particularly complex or of an amount unusually high which do not appear to have an economical justification or legal purpose.

In this case, the digital assets service provider must question the client regarding the origin and destination of the funds, as well as the purpose of the transaction and the identity of the person who benefits from it.

- Regardless of the amount of the transaction, the implementation within the digital assets service provider of an **organisation, procedures, internal control and appointment of a person responsible** for the compliance with obligations regarding anti-money laundering and terrorism financing taking into account the size and nature of its activities.

- Compliance with assets freeze measures:**
  - In case of holding or receipt of funds or economical resources (digital assets) for the account of a client; and
  - The prohibition to make available, directly or indirectly, or to use funds or economical resources (digital assets) to the benefit of persons whose funds and economical resources are subject to a freezing measure.
- Digital assets service providers may give to external providers the performance, in their name and for their account, all or part of those diligences. In such a case, the digital assets service providers remain **responsible** for complying with their obligations.
- It is reminded that the digital assets service providers are, besides, subject to **obligations of declaration to TRACFIN**, set out in articles L. 561-15 and seq. of the Monetary and Financial Code and must appoint a TRACFIN correspondent to this end.
- The organisation of the AML-CFT scheme is adapted to the size**, nature of the digital assets activities and services provided, as well as risks identified by the digital assets service provider.