



## Requirements for crypto-asset service providers concerning disclosures on the prevention of money laundering and terrorist financing

### Purpose and objective of the guideline

The purpose of this document is to provide guidance to applicants for authorisation referred to in Article 62 of Regulation (EU) No 1093/2010 on markets in crypto assets, so-called MiCA, to prepare the application documents concerning the prevention of money laundering and terrorist financing in a way ensuring that the application can be processed as smoothly as possible. At the end of the guideline, reference is also made to the requirements for documents to be provided by companies providing crypto-asset services based on another authorisation, i.e. by virtue of notification.

In accordance with Article 62(2)(i) of MiCA, an applicant for authorisation as a crypto-asset service provider shall include in the application a description of the internal control mechanisms, policies and procedures to identify, assess and manage risks, including money laundering and terrorist financing risks.

The description shall demonstrate that the mechanisms, policies and procedures are adequate and proportionate to the nature, quality and extent of the applicant's activities and their inherent risk. Furthermore, the description shall indicate how the applicant has sought to ensure compliance with obligations provided in the Act on the prevention of money laundering and terrorist financing (444/2017, the AML Act).

In order for the applicant to be sufficiently prepared for producing the disclosures and documents required by regulation, the applicant should study, in particular, the following guidelines:

- FIN-FSA regulations and guidelines:
  - [Prevention of money laundering and terrorist financing \(2/2023\)](#)
  - [Customer due diligence related to compliance with sanctions regulation and national freezing orders \(4/2023\)](#)
- [Guidelines of the European Banking Authority \(EBA\):](#)
  - ML/TF Risk Factors Guidelines (EBA/GL/2021/02), and, in particular, Guidelines EBA/GL/2024/01 introducing sector-specific Guideline 21 for crypto-asset service providers (CASP) into the ML/TF Risk Factors Guidelines
  - Guidelines concerning compliance with the Regulation on information accompanying transfers of funds (EBA/GL/2024/01)
  - Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer (EBA/GL/2022/05) (AML compliance officer guidelines)
  - Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 (EBA/GL/2022/15)
  - Guidelines on outsourcing arrangements (EBA/GL/2019/02)
- [Financial Action Task Force \(FATF\): Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers](#)

The abovementioned **guidelines should be taken into account** in preparing the risk assessment as well as policies and procedures.



In addition, the EBA is in the process of preparing *Guidelines on internal policies, procedures and controls to comply with restrictive measures*. When complete, these guidelines will also apply to crypto-asset service providers.

### Information and documents to be provided with the application

The European Securities and Markets Authority (ESMA) has published draft standards specifying the contents of the application for authorisation and of the notification on the provision of crypto-asset services based on another authorisation<sup>1</sup>.

The requirements of Article 62 of MiCA are specified in Article 6 of the standard on the contents of the application for authorisation. Below is a list of the disclosures and/or documents to be provided, along with further guidelines on their contents.

#### 1. Risk assessments

- Risk assessment of money laundering and terrorist financing
  - See EBA's ML/TF Risk Factors Guidelines and FIN-FSA regulations and guidelines 2/2023, chapter 4
  - The risk assessment must include **separate assessments** of the money laundering risk and terrorist financing risk.
  - The risk assessment must provide the applicant's justified assessment of the **inherent risk** of the applicant's activity and **residual risk** both as a whole and separately with respect to the following factors:
    - Customers
    - Products and services provided
    - Distribution channels used
    - Geographical areas of operation
- Risk assessment related to sanctions and national freezing orders
  - See FIN-FSA regulations and guidelines 4/2023, chapter 5, and the EBA's draft guidelines concerning sanctions regulation
- Description of the process of preparing the abovementioned risk assessments, including the processes and schedules in which the risk assessment is updated.
- Declaration of parties responsible for preparing the risk assessment and updating it.

#### 2. Policies and procedures to prevent money laundering and terrorist financing.

- The policies and procedures must cover the following areas
  - Obligations concerning customer due diligence
  - Obligations due to the Regulation on information accompanying transfers of funds
  - Detection of suspicious transactions and compliance with the reporting obligation
  - Compliance with obligations due to sanctions regulation and freezing orders
- Elaborating guidelines:

---

<sup>1</sup> [Final Report on Draft technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation \(MiCA\) – first package](#)



- See FIN-FSA regulations and guidelines 2/2023, chapter 5, definitions of policies and procedures
  - The policies and procedures must be risk-based, and the connection between the risk assessment and the selected risk management methods must be indicated.
- 3. Information on the person in charge of ensuring compliance with anti-money laundering and counter-terrorist financing obligations and evidence of the person's experience and education.**
- For more detailed information, see FIN-FSA regulations and guidelines 2/2023, subchapter 5.2.2.2 (reference and text corrected 5.9.2024)
- 4. Description of annual actions and resources to ensure the sufficient expertise of the personnel in risks related to the prevention of money laundering and terrorist financing and crypto assets in particular.**
- 5. Information on the** frequency of the assessment of the adequacy and effectiveness policies, procedures and internal control mechanisms as well as the person or function responsible for such assessment.
- 6. Description of the independent channel referred to in chapter 7, section 8 of the AML Act or an application for the use of the FIN-FSA's reporting channel to notify suspected infringements in accordance with the instructions provided on the FIN-FSA's website.**
- More information on the independent channel and the application to be filed with the FIN-FSA on the FIN-FSA's website: [Link to the instructions.](#)

### **Disclosures to be provided in the notification procedure**

Under the MiCA Regulation, crypto-asset services may also be provided by financial entities that already have an authorisation granted by the FIN-FSA for other than the provision of crypto-asset services. With the exception of credit institutions, the range of permitted crypto-asset services is limited according to the type of authorisation. Financial entities, including credit institutions, must notify the FIN-FSA before providing services, however. The notification procedure for financial entities regarding for the provision of a crypto-asset service is set out in Article 60 of the MiCA Regulation.

In accordance with Article 60(7)(b) of MiCA, a description of prevention of money laundering and terrorist financing must be provided in the notification procedure corresponding to the one provided when applying for authorisation. The requirements are the same also in the ESMA standards on the application for authorisation and on the notification procedure.

With a view to the abovementioned, in the notification procedure, the notifier must submit disclosures similar to those submitted with an application for authorisation. However, in contrast to the application for authorisation, the disclosures must only be provided to the extent that changes have been made to the existing policies, procedures and risk management framework due to the provision of crypto-asset services. For example, as regards the risk assessment, it is possible to submit only an excerpt concerning crypto-asset services.