AUTHORISATION OF THE ACTIVITIES OF CRYPTO-ASSET SERVICE PROVIDERS

Pursuant to Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services ('**Dáptv.**') and as provided for in Section 3 (1) of MNB Decree No. 36/2017 (XII. 27.) on the Rules for Electronic Communication in Certain Official Matters in Progress before the Magyar Nemzeti Bank, the legal representative of the enterprise and the applicant (client) obliged, pursuant to Section 58 (2) of Act CXXXIX Of 2013 on the Magyar Nemzeti Bank ('**MNB Act**'), to apply electronic communication, shall submit its application, notification or other petition by using the prescribed form available in the information system supporting the electronic administration of the MNB ('**ERA System**') and introduced for the procedure related to the submission in question, in the manner and with content specified therein, simultaneously uploading the attachments specified by the law and other documents required by the MNB. In the licensing procedures, the applications and notifications must be submitted by using the prescribed electronic form available in the E-administration/Licensing service on the ERA interface on the MNB's website, attaching the certified electronic copies of the appendices. The resolutions, requests for clarification, notices and other communications of the MNB are delivered to the financial organisations or their legal representatives by sending them to the delivery storage space.

A mandatory annex to the application, the Good Business Reputation Questionnaire is available, without registration or logging in, on the ERA interface (Public Services/Forms/Select Forms/Good Business Reputation Questionnaires/Personal Licences), as a pdf file to be filled in, saved and validated.
The filled in and electronically signed questionnaire can be attached to the prescribed electronic form as an annex. The questionnaire is available at: https://era.mnb.hu/ERA.WEB/PublicServices/Current?code=eraformanyomtatvany
The website of the MNB includes information materials on electronic administration and the submission of annexes to be attached in authorisation procedures (electronic documents) at:
https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/engedelyezes/e-ugyintezes

Further information related to certain aspects of the licensing procedures (e.g. ascertaining the good business reputation) is available at:
https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/engedelyezes/tajekoztatok

I. Introduction

Regulation (EU) 2023/1114 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('**MiCA**') entered into force on 29 June 2023, with its parts that apply to crypto-assets services applying **from 30 December 2024**. The MiCA applies to natural and legal persons and certain other undertakings that are engaged in issuing, offering to the public or admitting to trading, or providing services related to, crypto-assets in the EU. The MiCA makes the operation and activities of crypto-asset service providers subject to prior authorisation by the MNB.

I.1 Transition period

Pursuant to Article 143(3) MiCA, Member States may decide not to apply the transitional regime for crypto-asset service providers provided for in the first subparagraph or to reduce its duration where they consider that their national regulatory framework applicable before 30 December 2024 is less strict than this Regulation. In view of this, pursuant to Section 16 of Act VII of 2024 on the Crypto Assets Market ('**Crypto Act**'), a crypto-asset service provider already operating before 30 December 2024 must comply with the requirements of Regulation (EU) 2023/1114 of the European Parliament and of the Council **as of 1 July 2025 at the latest.**

I.2 Implementation of the MiCA in Hungary

As of 30 June 2024, the Crypto Act has placed the supervision of entities, persons and activities covered by the relevant legislation, including crypto-asset service providers, under the supervision of the MNB. Section 40(41) of the MNB Act specifically states that '*[i]n carrying out its tasks provided for in Paragraph t) of Subsection (1) of Section 39 the MNB shall provide for the implementation of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No. 1093/2010 and (EU) No. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.*'

II. Crypto-asset service providers and the activities they can perform

According to Article 3(1)(15) of the MiCA, 'crypto-asset service provider' means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59.

Pursuant to Article 59(1) MiCA, a person shall not provide crypto-asset services, within the Union, unless that person is: a legal person or other undertaking that has been authorised as crypto-asset service provider in accordance with Article 63 (point (a)); or a credit institution, central securities depository, investment firm, market operator, electronic money institution, UCITS management company, or an alternative investment fund manager that is allowed to provide crypto-asset services pursuant to Article 60 (point (b).Subject to Article 59(2) MiCA, crypto-asset service providers authorised in accordance with Article 63 shall have their registered office in a Member State where they carry out at least part of their crypto-asset services. They shall have their place of effective management in the Union and at least one of the directors shall be resident in the Union. Article 59(3) MiCA provides that, for the purposes of paragraph 1, point (a), other undertakings that are not legal persons shall only provide crypto-asset services if their legal form ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if they are subject to equivalent prudential supervision appropriate to their legal form.

While Article 59 of the MiCA does not require a procedure (regularity) on a professional basis in the course of the crypto-asset service provider's occupation or business, the definition of a crypto-asset service provider in Article 3(1)(15) of the MiCA already includes this condition, and recital 21 of the MiCA states that '"any person that provides crypto-asset services on a professional basis in accordance with this Regulation should be deemed to be a 'crypto-asset service provider'". Therefore, if a person wishes to provide crypto-asset services on a professional basis in the course of his or her occupation or business, an activity licence is required.

The provision of crypto-asset services on a professional basis in the course of an occupation or business may be provided subject to authorisation by the MNB under Article 59 of the MiCA, provided that it does not fall within the scope of one or more of the exemptions in Article 2(2) of the MiCA (persons or entities not subject to the MICA) or the case of crypto-asset services provided at the exclusive initiative of the client under Article 61.

Article 3(1)(16) of MiCA lists the crypto-asset services that may be performed as follows:
(a) providing custody and administration of crypto-assets on behalf of clients;
(b) operation of a trading platform for crypto-assets;
(c) exchange of crypto-assets for funds;
(d) exchange of crypto-assets for other crypto-assets;
(e) execution of orders for crypto-assets on behalf of clients;
(f) placing of crypto-assets;
(g) reception and transmission of orders for crypto-assets on behalf of clients;
(h) providing advice on crypto-assets;
(i) providing portfolio management on crypto-assets;
(j) providing transfer services for crypto-assets on behalf of clients.

Pursuant to Article 70(4) of MiCA, crypto-asset service providers may themselves, or through a third party, provide payment services related to the crypto-asset service they offer provided that the crypto-asset service provider itself, or the third party, is authorised to provide those services under Directive (EU) 2015/2366.. However, the MiCA does not specify what is meant by payment services. Please note, however, that in many cases, institutions under Article 60 of MiCA are subject to the principle of a clean profile and business exclusivity, and therefore cannot provide payment services under the current legislation, because EU legislation is not harmonised as regards the content of payment services and the conditions for their provision.

Article 65 of the MiCA provides for the possibility for undertakings providing crypto-asset services authorised and supervised in accordance with the Regulation to exercise the freedom to provide services and the freedom of establishment in the territory of EEA States to carry out **cross-border activities** without having to obtain a specific

authorisation from the competent authority of the Member State where they intend to provide services (the so-called 'passport').

Under Article 59(7) MiCA, crypto-asset service providers shall be allowed to provide crypto-asset services throughout the Union, either through the right of establishment, including through a branch, or through the freedom to provide services. Crypto-asset service providers that provide crypto-asset services on a cross-border basis shall not be required to have a physical presence in the territory of a host Member State.

Accordingly, the MiCA distinguishes the following forms of activity to EEA States:

- direct cross-border provision of services (under the freedom to provide services): in this case, the crypto-asset service provider is not physically present in the Member State and provides services directly on a cross-border basis;
- establishment of a branch (within the framework of freedom of establishment)

If the crypto-asset service provider, after obtaining its licence, would also carry out its activities abroad in an EEA member state, as referred to above, in the course of the licensing procedure for the activity, it shall therefore be required to make a statement pursuant to the provisions of Article 65(1) of the MiCA: a list of the Member States in which the crypto-asset service provider intends to provide crypto-asset services (point (a)), the crypto-asset services that the crypto-asset service provider intends to provide on a cross-border basis (point (b)), the starting date of the intended provision of the crypto-asset services (point (c)), a list of all other activities provided by the crypto-asset service provider not covered by this Regulation (point (d)).

III. Licensing conditions for crypto-asset providers

III.1 The application

Information to be provided in an Authorisation Form according to Article 62(2) of the MICA and the Draft RTS (Draft Regulatory Technical Standards supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in an application for authorisation as crypto-asset service provider ('**Draft RTS on authorization**'))[1]:

The applicant crypto-asset service provider

- company name, trading name, legal form
- registered office
- identification number (company registration number)
- LEI code
- the date of incorporation or registration and the Member State of registration
- contact details
- website address
- if the crypto-asset service provider intends to operate a crypto-asset trading platform, the address, telephone number and email address of the platform, the trading name of the platform
- a declaration of completeness pursuant to Section 59 (2) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank (MNB Act) (the applicant has provided the MNB with all relevant facts and data required for the issuance of the licence)

III.2 Capital requirements for crypto-asset service providers

Article 67(1) of MiCA requires a crypto-asset service provider to have, at all times, prudential safeguards in place, equal to an amount of at least the higher of the following:

- the amount of permanent minimum capital requirements indicated in Annex IV, depending on the type of the crypto-asset services provided (point (a));
- one quarter of the fixed overheads of the preceding year, reviewed annually (point (b)).

[1] https://www.esma.europa.eu/press-news/esma-news/esma-finalises-first-rules-crypto-asset-service-providersThe RTS concerned are attached as Annex 5 to the final report, which is available at the link.

The amount of permanent minimum capital requirements indicated in Annex IV, depending on the type of the crypto-asset services provided:

Crypto-asset service providers	Type of crypto-asset services	Minimum capital requirements under Article 67(1)(a)
Class 1	Crypto-asset service provider authorised for the following crypto-asset services: – execution of orders on behalf of clients; – placing of crypto-assets; – providing transfer services for crypto-assets on behalf of clients; – reception and transmission of orders for crypto-assets on behalf of clients; – providing advice on crypto-assets; and/or – providing portfolio management on crypto-assets.	EUR 50,000
Class 2	Crypto-asset service provider authorised for any crypto-asset services under class 1 and: – providing custody and administration of crypto-assets on behalf of clients; – exchange of crypto-assets for funds; and/or – exchange of crypto-assets for other crypto-asset.	EUR 125,000
Class 3	Crypto-asset service provider authorised for any crypto-asset services under class 2 and: – operation of a trading platform for crypto-assets.	EUR 150,000

For the purposes of paragraph 1, point (b), crypto-asset service providers shall calculate their fixed overheads for the preceding year, using figures resulting from the applicable accounting framework, by subtracting the following items from the total expenses after distribution of profits to shareholders or members in their most recently audited annual financial statements or, where audited statements are not available, in annual financial statements validated by national supervisors:
(a) staff bonuses and other remuneration, to the extent that those bonuses and that remuneration depend on a net profit of the crypto-asset service providers in the relevant year;
(b) employees', directors' and partners' shares in profits;
(c) other appropriations of profits and other variable remuneration, to the extent that they are fully discretionary;
(d) non-recurring expenses from non-ordinary activities.

Crypto-asset service providers that have not been in business for one year from the date on which they began providing services shall use, for the calculation referred to in paragraph 1, point (b), the projected fixed overheads included in their projections for the first 12 months of service provision, as submitted with their application for authorisation.

Under Article 67(4) MiCA, prudential safeguards shall take any of the following forms or a combination thereof:

- own funds, consisting of Common Equity Tier 1 items and instruments referred to in Articles 26 to 30 of Regulation (EU) No 575/2013 after the deductions in full, pursuant to Article 36 of that Regulation, without the application of threshold exemptions pursuant to Articles 46 and 48 of that Regulation (point (a));
- an insurance policy covering the territories of the European Union where crypto-asset services are provided or a comparable guarantee. (point (b)).

Where the crypto-asset service provider holds an insurance policy referred to in Article 67(4)(b) MiCA, the insurance policy shall be disclosed to the public on the crypto-asset service provider's website and shall have at least the following characteristics: it has an initial term of not less than one year (point (a)), the notice period for its cancellation is at least 90 days (point (b)), it is taken out from an undertaking authorised to provide insurance, in accordance with Union or national law (point (c)), it is provided by a third-party entity (point (d)).

The insurance policy shall include coverage against the risk of all of the following:
(a) loss of documents;
(b) misrepresentations or misleading statements made;
(c) acts, errors or omissions resulting in a breach of:
i. legal and regulatory obligations;

ii. the obligation to act honestly, fairly and professionally towards clients;
iii. obligations of confidentiality;
(d) failure to establish, implement and maintain appropriate procedures to prevent conflicts of interest;
(e) losses arising from business disruption or system failures;
(f) where applicable to the business model, gross negligence in the safeguarding of clients' crypto-assets and funds;
(g) liability of the crypto-asset service providers towards clients pursuant to Article 75(8).

Pursuant to Article 67 (4) (a) of the MiCA if the applicant chooses own funds as prudential safeguard, the legal origin of the capital has to be proved.

Pursuant to Article 3 of the Draft RTS on authorization, the applicant is required to provide the following for the purposes of demonstrating compliance with Article 67 of the MiCA:

- a declaration that:
  - the amount of the prudential safeguards that the applicant has in place at the time of the application for authorisation and the description of the assumptions used for its determination;
  - the amount of the prudential safeguards covered by own funds referred to in Article 67(4), point (a), where applicable;
  - the amount of the applicant's prudential safeguards covered by an insurance policy referred to in Article 67(4), point (b), where applicable.
- forecast calculations
  - forecast calculation of the applicant's prudential safeguards for the first three business years;
  - planning assumptions including stress scenarios for the above forecast as well as explanations of the figures;
  - expected number and type of clients, volume of orders and transactions and expected maximum amount of crypto-assets under custody;
- for companies that are already active, the financial statements of the last three years approved, where audited, by the external auditor;
- a description of the applicant's prudential safeguards planning and monitoring policies and procedures;
- proof that the applicant meets the prudential safeguards in accordance with Article 67 MiCA, including:
  - in relation to own funds: a document on how the applicant has calculated the amount in accordance with Article 67 MiCA; for companies that are already active and whose financial statements are not audited, a certification by the national supervisor of the amount of own funds of the applicant; for undertakings in the process of being incorporated, a statement issued by a bank certifying that the funds are deposited in the applicant's bank account;
  - in relation to own funds: proof of the legal origin of the financial resources according to the information in Article 8 of the Draft RTS on the acquisition of qualifying holdings pursuant to Article 8(e) of the Draft RTS on authorization (III.6.)
  - in relation to the insurance policy: the legal name, the date and Member State of incorporation or foundation, the address of the head office and, if different, of the registered office and contact details of the undertaking authorised to provide the insurance policy or comparable guarantee; a copy of the subscribed insurance policy incorporating all the elements necessary to comply with Article 67(5) and (6) MiCA, where available, or a copy of the insurance agreement incorporating all the elements necessary to comply with Article 67(5) and (6) MiCA signed by an undertaking authorised to provide insurance in accordance with Union law or national law.

III.3 Organisational requirements for the crypto-asset service provider

- the **articles of association** of the applicant crypto-asset service provider (Article 62(2)(c) MiCA)
- Organigram of the holding structure and organisational structure of the crypto-asset service provider according to Article 8 of the Draft RTS on authorization
- a detailed description of the applicant crypto-asset service provider's **governance arrangements** (Article 62(2)(f) MiCA) Article 4 of the Draft RTS on authorization details the requirements for the governance arrangements.
- a **programme of operations**, setting out the types of crypto-asset services that the applicant crypto-asset service provider intends to provide, including where and how those services are to be marketed, indicating the content elements set out in Article 2 of the Draft RTS on authorization (Article 62(2)(d) MiCA)

- a description of the applicant crypto-asset service provider's **internal control mechanisms**, policies and procedures to identify, assess and manage **risks**, including money laundering and terrorist financing risks, and **business continuity plan**, which should be designed to take into account the requirements of Articles 4 and 5 of the Draft RTS on authorization (Article 62(2)(i) MiCA)
- a description of the procedure **for the segregation of clients' crypto-assets and funds**, subject to the provisions of Article 10 of the Draft RTS on authorization (Article 62(2)(k) MiCA and Article 11 of the Draft RTS)
- a description of the applicant crypto-asset service provider's **complaints-handling procedures** (Article 62(2)(l) MiCA)
- where the applicant crypto-asset service provider intends to provide custody and administration of crypto-assets on behalf of clients, a description of the **custody and administration policy** (based on Article 62(2)(m) MiCA and Article 12 of the Draft RTS on authorization)
- where the applicant crypto-asset service provider intends to operate a trading platform for crypto-assets, a description of the **operating rules of the trading platform** and of the procedure and system to **detect market abuse** (as required by Article 62(2)(n) MiCA and Article 13 of the Draft RTS on authorization)
- where the applicant crypto-asset service provider intends to exchange crypto-assets for funds or other crypto-assets, a description of the **commercial policy**, **which shall be non-discriminatory**, governing the relationship with clients as well as a description of the methodology for determining the price of the crypto-assets that the applicant crypto-asset service provider proposes to exchange for funds or other crypto-assets (based on Article 62(2)(o) MiCA and Article 14 of the Draft RTS on authorization)
- where the applicant crypto-asset service provider intends to execute orders for crypto-assets on behalf of clients, a description of the **execution policy** (Article 62(2)(p) MiCA and Article 15 of the Draft RTS on authorization)
- where the applicant crypto-asset service provider intends to provide advice on crypto-assets or **portfolio management** of crypto-assets, proof that the natural persons giving advice on behalf of the applicant crypto-asset service provider or managing portfolios on behalf of the applicant crypto-asset service provider have the **necessary knowledge** and expertise to fulfil their obligations (as referred to in Article 62(2)(q) MiCA and Article 16 of the Draft RTS on authorization)
- where the applicant crypto-asset service provider intends to provide transfer services for crypto-assets on behalf of clients, information on the manner in which such transfer services will be provided (as referred to in Article 62(2)(r) MiCA and Article 17 of the Draft RTS on authorization)
- the **type of crypto-asset** to which the crypto-asset service relates (Article 62(2)(s) MiCA)
- proof of the qualifications and professional experience required by Section 2 of Government Decree 294/2024 (X. 9.) on the requirements for the qualifications and professional experience of natural persons providing crypto-asset advice or information on behalf of a crypto-asset service provider in relation to **natural persons providing advice on crypto-assets or information** on behalf of a crypto-asset service provider.

III.4 Prevention of money laundering and terrorist financing

The applicant shall submit, as an annex to the application, a description of its internal control mechanisms, policies and procedures to identify, assess and manage risks, including money laundering and terrorist financing risks, and business continuity plan, as referred to in Article 62(2)(i) MiCA. According to Article 6 of the Draft RTS on authorization, the following documents are required to be submitted:
(a) the applicant's assessment of the inherent and residual risks of money laundering and terrorist financing associated with its business, including the risks relating to the applicant's customer base, to the services provided, to the distribution channels used and to the geographical areas of operation;
(b) the measures that the applicant has or will put in place to prevent the identified risks and comply with applicable anti-money laundering and counter-terrorist financing requirements, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;
(c) detailed information on how such mechanisms, systems and procedures are adequate and proportionate to the scale, nature, inherent money laundering and terrorist financing risk, range of crypto-asset services provided, the complexity of the business model and how they ensure the applicant's compliance with Directive (EU) 2015/849 and Regulation (EU) 2023/1113;

(d) pursuant to Article 6(d) of the Draft RTS on authorization and Section 63 (4a) and (5) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing ('**AML Act**'), the application must be accompanied by a document containing the results of the assessment of the suitability of the designated responsible manager (or the senior manager performing this function) and the compliance manager, approved by the board of directors/supervisory board/other body. If the compliance manager, as detailed in MNB Recommendation 3/2024[2]:

- is not appointed on the basis of proportionality,
- the related tasks are carried out by the designated responsible manager,
- only one compliance manager is appointed within the group, or
- his or her tasks are outsourced,

the relevant decision of the Board and the reasons for it;
(e) arrangements, human and financial resources devoted to ensuring that staff of the applicant is appropriately trained in anti-money laundering and counter-terrorist financing matters (annual indications) and on specific crypto-asset related risks;
(f) a copy of the applicant's anti-money laundering and counter-terrorism policies and procedures, and systems;
(g) the frequency of the assessment of the adequacy and effectiveness of such mechanisms, systems and policies and procedures as well as the person or function responsible for such assessment.

As of 1 January 2025, a crypto-asset service provider is considered a financial service provider within the meaning of Section 3, point 28, subpoint o) of the AML Act. Crypto-asset service provider according to Section 20a of the AML Act: a crypto-asset service provider as defined in Article 3(1)(15) MiCA, where it provides one or more of the crypto-asset services defined in Article 3(1)(16) MiCA, except for the provision of advice on crypto-assets as defined in Article 3(1)(16)(h) MiCA.

The Regulation on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 ('**TFR**') was prepared as part of the EU's Money Laundering and Terrorist Financing Prevention Package and later developed together with the MiCA in order for the so-called Travel Rule (transmission of originator and beneficiary data with the transaction) to be adopted, in harmony with Recommendation 16 by the Financial Action Task Force ('**FATF**'), to also cover crypto-asset transfer service providers. The TFR entered into force under No (EU) 2023/1113 on 29 June 2023 and shall apply from 30 December 2024.

According to the FATF Recommendation[3], a virtual asset service provider is any natural or legal person not covered by the FATF Recommendations elsewhere who, as an undertaking, carries out one or more of the following activities or operations on behalf of or for another natural or legal person:
i. exchange between virtual assets and fiat currencies,
ii. exchange between one or more forms of virtual assets.

The TFR contains detailed rules on the **internal procedures and organisational structure** of covered service providers, closely linked to FATF Recommendation 15 on licensing and supervision requirements for virtual assets and virtual asset service providers, and therefore the design of procedures and policies should be developed taking into account the aspects of the Recommendation.

Recommendations and guidance for applicants on how to comply with the fight against money laundering and terrorist financing are available on the MNB website[4].

III.5 Conditions for members of the management body

According to Article 3(27) of MiCA, 'management body' means the body or bodies of an issuer, offeror or person seeking admission to trading, or of a crypto-asset service provider, which are appointed in accordance with national law, which are empowered to set the entity's strategy, objectives and overall direction, and which oversee and monitor management decision-making in the entity and include the persons who effectively direct the business of the entity;

[2] https://www.mnb.hu/letoltes/3-2024-aml-compliance-officer-ajanlas.pdf.
[3] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF Recommendations 2012.pdf.coredownload.inline.pdf
[4] https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/kotelezo-es-iranyado-szabalyok/ajanlasok.

The definition of a management body, regardless of the designation, includes:

- the person who effectively controls the business activity (e.g. CEO)
- a member of the board of directors, including the chairperson,
- a member of the supervisory board, including the chairperson.

III.5.1 Management and professional competence

Pursuant to Articles 62(2)(g), (3)(b) and 68(1) MiCA, members of the management body are of sufficiently good repute and possess the appropriate knowledge, skills and experience to manage the applicant issuer, both individually and collectively.

The MNB would like to inform applicants that EBA-ESMA Joint Guidelines[5] **(Guidelines**) are available for the assessment of the suitability of the members of the management body, and it is recommended that they be taken into account in the procedure.

The Guidelines assess the suitability criteria taking into account the proportionality principle, based on the crypto-asset service provider's legal form, its membership in a group of companies, the nature and complexity of all activities, the size of its balance sheet total and whether the applicant crypto-asset service provider would also carry out cross-border activities. (Guidelines, point C.1.8-12)

The Guidelines present separately the exemplary criteria to be evaluated individually (C.2.2 points 16-27) and collectively (C.2.3 point 28).

III.5.2 Statements

Article 7(f) and (g) of the Draft RTS on authorization sets out the information to be provided during the authorisation procedure in relation to the assessment of suitability and good repute in relation to potential conflict of interest positions, family or business relationships.[6]

III.5.3 Sufficient time

Pursuant to Articles 62(2)(g), 62(3)(b) and 68(1) MiCA, the members of the board of a crypto-asset service provider are required to commit sufficient time to perform their duties. The Guidelines (point C.2.4) specify that the time allocated for the performance of the duty must take into account all the positions of the management body members, the size of the companies, their scope of activity and their geographical location.

---

[5] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/asset-referenced-and-e-money-tokens-micar/joint-0#:~:text=The%20Joint%20EBA%20and%20ESMA,management%20body%20as%20well%20as

[6] *(f) personal history, including all of the following:*
(i) criminal records, including criminal convictions and any ancillary sanctions and information on pending criminal proceedings or investigations or sanctions (including relating to commercial law, financial services law, money laundering, and terrorist financing, fraud or professional liability), information on enforcement proceedings or sanctions, information on relevant civil and administrative cases and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures, through an official certificate (if and insofar as it is available from the relevant Member State or third country), or through another equivalent document or, where such certificate does not exist. For ongoing investigations, the information may be provided through a declaration of honour. Official records, certificates and documents shall have been issued within three months before the submission of application for an authorisation;
(ii) information on any refusal of registration, authorisation, membership or licence to carry out a trade, business or profession; or the withdrawal, revocation or termination of such a registration, authorisation, membership or licence to carry out a trade, business or profession; or any expulsion by a regulatory or government body or by a professional body or association;
(iii) information on dismissal from employment or a position of trust, fiduciary relationship, or similar situation;
(iv) information on whether another competent authority has assessed the reputation of the individual, including the identity of that authority, the date of the assessment and information about the outcome of that assessment. The applicant shall not need to submit such information about the previous assessment where the competent authority is already in possession of such information;
(g) a description of any financial and non-financial interests or relationships of the person and his/her close relatives to members of the management body and key function holders in the same institution, the parent institution and subsidiaries and shareholders. Such description shall include any financial interests, including crypto-assets, other digital assets, loans, shareholdings, guarantees or security interests, whether granted or received, commercial relationships, legal proceedings and whether the person was a politically exposed person as defined in point (9) of article 3 of Directive (EU) 2015/849 over the past two years.

III.5.4 Education

The MiCA does not explicitly prescribe what qualifications a management body member must have. The Draft Recommendation proposes to examine the level and direction of the qualification in relation to the existence of adequate knowledge and skills as described in Article 62(2)(g) MiCA. It is considered acceptable if the qualification is related to economics, law, accounting, administration, finance, financial management, information technology. It stresses, however, that education alone is not enough and that it is essential to have the right practical skills.

III.5.5 Good business reputation, no criminal record

According to Articles 62(2)(g) and 68(1) of the MiCA, members of the management body, persons shall be of sufficiently good repute. Pursuant to Article 68(3) MiCA, for the purposes of point (a), the crypto-asset service provider shall provide proof of the following: for all members of the management body of the applicant crypto-asset service provider, the absence of a criminal record in respect of convictions and the absence of penalties imposed under the applicable commercial law, insolvency law and financial services law, or in relation to anti-money laundering, and counter-terrorist financing, to fraud or to professional liability. Under Article 68(2) of the MiCA, a management body member shall not have been convicted of offences relating to money laundering or terrorist financing or of any other offences that would affect their good repute. Article 7 of the Draft RTS on authorization further details the requirements for a clean criminal record.

Further information related to certain aspects of the licensing procedures (e.g. ascertaining the good business reputation) is available at:
https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/engedelyezes/tajekoztatok

III.5.6 Documents to be submitted in relation to the members of the management body during the authorisation procedure:

- to be submitted on form: identification data of the members of the applicant crypto-asset service provider's management body;
- proof of good repute requires a certificate of good repute with enhanced content, i.e. an official certificate of clean criminal record no more than 90 days old, which, in addition to confirming a clean criminal record, must also state that the applicant is not banned from exercising civil rights or exercising a profession. With regard to Section 71 (7) of the PRJ Act, the MNB also accepts the extended certificate of good conduct if it contains information that the candidate has no criminal record and is not under a ban from exercising civil rights.[7]
- a document proving qualifications;
- a signed CV attesting professional and managerial experience, completed in the detail set out in Article 7 (d)-(e) of the Draft RTS on authorization;
- the Business Reputation Questionnaire completed and signed by the management body member: the Good business reputation questionnaire, which is a mandatory attachment to the application, is available, without registration or logging in, on the ERA interface (Public Services/Forms/Select Forms/Good Business Reputation Questionnaires/Personal Licences), as a pdf file to be filled in, saved and validated.
The filled in and electronically signed questionnaire can be attached to the prescribed electronic form as an annex. The questionnaire is available at: https://era.mnb.hu/ERA.WEB/PublicServices/Current?code=eraformanyomtatvany
- a statement by the member of the management body on the minimum time spent performing his/her duties within the undertaking (the time spent on performing the function undertaken must be specified, subject to the details of the positions held in other institutions, organisations in employment or other employment relationships as set out in Article 7 of the Draft RTS on authorization);
- declaration on Article 7(h) and (f) of the Draft RTS on authorization

[7] According to Section 71 (7) of Act XLVII of 2009 on the Criminal Records System, the Register of Rulings by the Courts of the Member States of the European Union against Hungarian Citizens and on the Register of Biometric Data in Criminal and Law Enforcement Matters (PRJ Act), if the applicant is prohibited from an occupation or activity, then the fact specified in Paragraph (5) (e) (the occupation or activity from which the applicant is prohibited) must be indicated in the official certificate of good conduct in the case of an application to prove the fact specified in Paragraph (5) (b) (i.e. that the applicant has no criminal record), even in the absence of such an application.

- a suitability policy prepared by the crypto-asset service provider in relation to the member of the management body, as set out in Article 7(3) of the Draft RTS on authorization and point C.3 of the Guidelines.

III.6 Expectations of owners or members with a qualifying holding

A qualifying holding within the meaning of Article 3(36) of the MiCA is any direct or indirect holding in an issuer of asset-referenced tokens or in a crypto-asset service provider which represents at least 10% of the capital or of the voting rights, as set out in Articles 9 and 10 of Directive 2004/109/EC of the European Parliament and of the Council, respectively, taking into account the conditions for the aggregation thereof laid down in Article 12(4) and (5) of that Directive, or which makes it possible to exercise a significant influence over the management of the issuer of asset-referenced tokens or the management of the crypto-asset service provider in which that holding subsists

Pursuant to Article 83(1) MiCA, any natural or legal person or such persons acting in concert who have taken a decision either to acquire, directly or indirectly, (the ' proposed acquirer') a qualifying holding in a crypto-asset service provider or to increase, directly or indirectly, such a qualifying holding so that the proportion of the voting rights or of the capital held would reach or exceed 20 %, 30 % or 50 % or so that the crypto-asset service provider would become its subsidiary, shall notify the competent authority of that crypto-asset service provider thereof in writing indicating the size of the intended holding and the information required pursuant to the regulatory technical standards adopted by the Commission in accordance with Article 84(4).

Detailed information on the assessment of the reputation, integrity and suitability of a direct or indirect acquirer of influence can be found in the Draft RTS *(Draft Regulatory Technical Standards supplementing Regulation EU (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the detailed content of information necessary to carry out the assessment of a proposed acquisition of a qualifying holding in a crypto-asset service provider)* **(Draft RTS on acquisition of a qualifying holding)**[8], and, in relation to the assessment, the Guidelines refer back to the Joint Guidelines on the supervisory assessment of acquisitions and increase of qualifying holdings in the financial sector ('**Joint Guidelines**'[9]).

On the basis of Article 84(1) of the MiCA, the Draft RTS on the acquisition of qualifying holdings and the Guidelines, the MNB assesses the following in relation to the suitability of the proposed acquirer:

- the good repute of the proposed acquirer (Article 62(2)(h), Article 68(2), Article 84(1)(a), Article 8(b) of the Draft RTS on authorization, Articles 1 to 3 of the Draft RTS on the acquisition of qualifying holdings
- the reputation, knowledge, skills and experience of any person who will direct the business of the crypto-asset service provider as a result of the proposed acquisition; (Article 84(1)(b); Article 8(c) of the Draft RTS on authorization, Article 5 of the Draft RTS on the acquisition of qualifying holdings) and point F.3 of the Guidelines;
- the financial soundness of the proposed acquirer, in particular in relation to the type of business envisaged and pursued in respect of the crypto-asset service provider in which the acquisition is proposed (Article 84(1)(c)), the information provided for in Article 6(b), (d) and (e), Article 8 of the Draft RTS on the acquisition of qualifying holdings pursuant to Article 8 of the Draft RTS on authorization
- whether the crypto-asset service provider will be able to comply and continue to comply with the provisions of this Title (Article 84(1)(d));
- whether, in connection with the proposed acquisition, there are reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted within the meaning of Article 1(3) and (5) of Directive (EU) 2015/849 or that the proposed acquisition may increase the risk thereof (Article 84(1)(e)), and applies paragraph 28 of the Joint Guidelines whenever the funds for the acquisition of the qualifying holdings consist in crypto-assets or whenever they derive from the exchange of crypto-assets into fiat currency[10]

[8] https://www.esma.europa.eu/press-news/esma-news/esma-finalises-first-rules-crypto-asset-service-providers.

[9] https://www.eiopa.europa.eu/publications/joint-guidelines-prudential-assessment-acquisitions-and-increases-qualifying-holdings-banking_en

[10] Whenever the funds for the acquisition of the qualifying holdings consist in crypto-assets or whenever they derive from the exchange of crypto-assets into fiat currency, competent authorities, in addition to the application of the assessment methodology laid down in Title II, Chapter 3, Section 14 of the Joint ESAs Guidelines on QH, on the suspicion of money laundering or terrorist financing, should also identify:

- in the case of a direct acquirer, the information required under Article 4 of the Draft RTS on the acquisition of qualifying holdings
- information in Article 6 of the Draft RTS on authorization on the acquisition of qualifying holdings pertaining to qualifying holdings, pursuant to Article 8(e) of the Draft RTS on authorization
- information under Article 7 of the Draft RTS on qualifying holdings – Information on the new proposed group structure and its impact on supervision, subject to paragraphs 9.1-3 of Section 9 of Chapter 3 of Title II of the Joint Guidelines;
- proof of the legal origin of the financial resources according to the information in Article 8 of the Draft RTS on the acquisition of qualifying holdings pursuant to Article 8(e) of the Draft RTS on authorization.

III.6.1 Good business reputation

Pursuant to Article 62(2)(h) MiCA, it is necessary to demonstrate that the owners or members who directly or indirectly hold a qualifying holding in the applicant crypto-asset service provider are of sufficiently good repute. Article 62(3)(c) and Article 68(2) of the MiCA provide that the applicant crypto-asset service provider shall provide proof for all shareholders and members, whether direct or indirect, that have qualifying holdings in the applicant crypto-asset service provider, of the absence of a criminal record in respect of convictions and the absence of penalties imposed under the applicable commercial law, insolvency law and financial services law, or in relation to anti-money laundering and counter-terrorist financing, to fraud or to professional liability.

With regard to the assessment of the good reputation, integrity and suitability of a direct or indirect acquirer of the holding, the Guidelines refer back to the provisions of Title II, Chapter 1, Subchapters 7 to 8, Chapter 2, Subchapter 9 and Chapter 3, Subchapters 10, 12, 13 and 14 of the Joint Guidelines.

For the purposes of assessing the reputational aspects of the proposed acquirer's professional competence, the MNB applies the proportionality principle in line with paragraph 3 of Section 8 (Proportionality principle) of the Joint Guidelines.

III.6.2 Documents to be submitted during the authorisation procedure in relation to holders of qualifying holdings:

III.6.2 a) Documents to be submitted for natural persons

- to be submitted on form: identification data of the proposed acquirer in the applicant crypto-asset service provider;
- proof of good repute requires a certificate of good repute with enhanced content, i.e. an official certificate of clean criminal record no more than 90 days old, which, in addition to confirming a clean criminal record, must also state that the applicant is not banned from exercising civil rights or exercising a profession. With regard to Section 71 (7) of the PRJ Act, the MNB also accepts the extended certificate of good conduct if it contains information that the candidate has no criminal record and is not under a ban from exercising civil rights.[11]
- Good Business Reputation Questionnaire: a mandatory annex to the application, the Good Business Reputation Questionnaire is available, without registration or logging in, on the ERA interface (Public Services/Forms/Select Forms/Good Business Reputation Questionnaires/Personal Licences), as a pdf file to be filled in, saved and validated. The filled in and electronically signed questionnaire can be attached to the prescribed electronic form as an annex. The questionnaire is available at: https://era.mnb.hu/ERA.WEB/PublicServices/Current?code=eraformanyomtatvany

a. the distributed ledger address used by the proposed acquirer, where a transfer of crypto-assets is registered on a network using distributed ledger technology or similar, and the crypto-asset account number used by the proposed acquirer, where such an account exists and is used to process the transaction;
b. the crypto-asset account number used by the proposed acquirer, where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar;
c. where a transfer of crypto-assets is not registered on a network using distributed ledger technology or similar technology and not made from or to a crypto-asset account, a unique transaction identifier; and
d. the crypto-asset service provider(s) of the parties to the transaction, as applicable.

[11] According to Section 71 (7) of Act XLVII of 2009 on the Criminal Records System, the Register of Rulings by the Courts of the Member States of the European Union against Hungarian Citizens and on the Register of Biometric Data in Criminal and Law Enforcement Matters (PRJ Act), if the applicant is prohibited from an occupation or activity, then the fact specified in Paragraph (5) (e) (the occupation or activity from which the applicant is prohibited) must be indicated in the official certificate of good conduct in the case of an application to prove the fact specified in Paragraph (5) (b) (i.e. that the applicant has no criminal record), even in the absence of such an application.

- a detailed curriculum vitae stating the information required under Article 1(1)(b) of the Draft RTS on the acquisition of qualifying holdings
- in the case of a direct acquirer, the information required under Article 4 of the Draft RTS on the acquisition of qualifying holdings
- information in Article 6 of the Draft RTS on the acquisition of qualifying holdings pertaining to qualifying holdings, pursuant to Article 8 of the Draft RTS on authorization
- information in Article 7 of the Draft RTS on the acquisition of qualifying holdings
proof of the legal origin of the financial resources according to the information in Article 8 of the Draft RTS on the acquisition of qualifying holdings pursuant to Article 9(e) of the Draft RTS on authorization;
depending on the rate of the acquisition – upon acquiring a qualifying holding of not more than 20 percent, the documentation specified in Article 9 of the Draft RTS on the acquisition of qualifying holdings;
- upon acquiring a qualifying holding between 20 and 50 percent, the documentation prescribed in Article 10 of the Draft RTS on the acquisition of qualifying holdings;
- upon acquiring a qualifying holding exceeding 50 percent, the documentation prescribed in Article 11 of the Draft RTS on the acquisition of qualifying holdings.

III.6.2 b) Documents to be submitted for non-natural persons

- to be submitted on form: identification data of the proposed acquirer in the applicant crypto-asset service provider;
- in respect of a senior executive and member, beneficial owner, proof of good repute requires a certificate of good repute with enhanced content, i.e. an official certificate of clean criminal record no more than 90 days old, which, in addition to confirming a clean criminal record, must also state that the applicant is not banned from exercising civil rights or exercising a profession. With regard to Section 71 (7) of the PRJ Act, the MNB also accepts the extended certificate of good conduct if it contains information that the candidate has no criminal record and is not under a ban from exercising civil rights.[12]
- Good Business Reputation Questionnaire: a mandatory annex to the application, the Good Business Reputation Questionnaire is available, without registration or logging in, on the ERA interface (Public Services/Forms/Select Forms/Good Business Reputation Questionnaires/Personal Licences), as a pdf file to be filled in, saved and validated. The filled in and electronically signed questionnaire can be attached to the prescribed electronic form as an annex. The questionnaire is available at: https://era.mnb.hu/ERA.WEB/PublicServices/Current?code=eraformanyomtatvany
- the memorandum and articles of association of the legal person, a summary explanation of the main legal features of the legal form of the legal person as well as an up-to-date overview of its business activity, pursuant to Article 1(2)(g) of the Draft RTS on the acquisition of qualifying holdings
- a statement, pursuant to Article 1(2)(h) of the Draft RTS on the acquisition of qualifying holdings, as to whether the legal person has ever been or is regulated by a competent authority in the financial services sector or other government body
- the Anti-Money Laundering Regulations referred to in Article 1(2)(i) of the Draft RTS on the acquisition of qualifying holdings, where the acquirer is an obliged entity under Article 2 of Directive 2015/849/EC on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC
- statement pursuant to Article 1(2)(j)of the Draft RTS on the acquisition of qualifying holdings, of the persons who effectively direct the business of the proposed acquirer (managing directors) and their personal identification details (name, date and place of birth, address, contact details, a copy of the official identity document), the detailed curriculum vitae stating relevant education and training, relevant functions performed, including experience in particular in financial services, crypto-asset services, distributed ledger technology (DLT), cybersecurity or digital innovation, together with the information referred to in points (a) and (b) of Article 2 of the Draft RTS on the acquisition of qualifying holdings.
- a declaration by the acquirer of the holding as set out in Article 8 of the Draft RTS on authorization,

[12] According to Section 71 (7) of Act XLVII of 2009 on the Criminal Records System, the Register of Rulings by the Courts of the Member States of the European Union against Hungarian Citizens and on the Register of Biometric Data in Criminal and Law Enforcement Matters (PRJ Act), if the applicant is prohibited from an occupation or activity, then the fact specified in Paragraph (5) (e) (the occupation or activity from which the applicant is prohibited) must be indicated in the official certificate of good conduct in the case of an application to prove the fact specified in Paragraph (5) (b) (i.e. that the applicant has no criminal record), even in the absence of such an application.

proof of the legal origin of the financial resources according to the information in Article 8 of the Draft RTS on the acquisition of qualifying holdings pursuant to Article 8(e) of the Draft RTS on authorization,
- a detailed diagram of the ownership structure pursuant to Article 8(a) of the Draft RTS on authorization and a statement of beneficial owners pursuant to Article 1(2)(k) of the Draft RTS on the acquisition of holdings,
- Annual financial statements pursuant to Article 3(i) of the Draft RTS on the acquisition of qualifying holdings for the last three financial years, on an individual and/or consolidated, sub-consolidated basis. The acquirer is required to attach each of the following, where relevant, audited by an auditor in accordance with Article 2(2) to (3) of Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC: (i) balance sheet, (ii) profit and loss statement (iii) the annual financial reports and financial annexes and other documents registered with the authority that registered and keeps records of the legal person (iv) if the acquirer is a newly created legal entity or organisation, in the absence of financial statements, a summary of the financial position of the acquirer, projections for the next three years and the planning assumptions used in the base case and stress scenario.
- If the acquirer is established in a third country, a statement of the information required under Article 3(2) of the Draft RTS on the acquisition of qualifying holdings and related documentation;
depending on the rate of the acquisition – upon acquiring a qualifying holding of not more than 20 percent, the documentation specified in Article 9 of the Draft RTS on the acquisition of qualifying holdings;
- upon acquiring a qualifying holding between 20 and 50 percent, the documentation prescribed in Article 10 of the Draft RTS on the acquisition of qualifying holdings;
- upon acquiring a qualifying holding exceeding 50 percent, the documentation prescribed in Article 11 of the Draft RTS on the acquisition of qualifying holdings.

Article 1(3) to (5) of the Draft RTS on the acquisition of qualifying holdings require the submission of additional specific documents if the acquirer is a trust, alternative investment fund or sovereign wealth fund.

III.7 Material, IT requirements for the crypto-asset service provider

Pursuant to Article 62(2)(i) and (j) of the MiCA, the applicant must submit the following documents:

- a technical documentation of the ICT systems and security arrangements and a description thereof in non-technical language; a description of the procedure for segregating clients' crypto-assets and funds;
- the applicant crypto-asset service provider's business continuity plan, which should be designed to take into account the requirements of Article 5 of the Draft RTS on authorization (Article 62(2)(i) MiCA).

Presentation of the governance, organisational and regulatory framework for the security of information systems pursuant to Article 64 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (**DORA**), the Regulation that entered into force shall apply from 17 January 2025 in respect of crypto-asset providers authorised under the MiCA pursuant to Article 2(1)(f) of the DORA. The requirements in III.6.1 are therefore only to be met for authorisation procedures pending or launched after 17 January 2025.

III.7.1 Documents to be submitted during the licensing procedure to demonstrate the existence of IT material conditions, taking into account Article 9 of the Draft RTS on authorization:

a) a description of the governance, organisational and regulatory framework for the security of information systems in accordance with Article 2 of 'Commission Delegated Regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework' ('**RMF RTS**') contained in Article 15 of *'Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011';*
b) a description of the project management arrangements for the establishment of ICT systems and the security principles applied, in accordance with Article 5 of the DORA and Article 15 of the RMF RTS;
c) the requirements for employees using or having access to the applicant's ICT facilities and the third party ICT service provider's personnel in accordance with the requirements of Article 5 of the DORA and Article 19 of the RMF RTS;

d) a description of the IT systems under Article 7 of the DORA, with the following content:
   i.) the architecture of ICT systems and the elements of the network,
   ii.) business IT systems supporting the business activities provided,
   iii.) for an asset-referenced token-issuing institution, the IT systems that support the organisation and its business (e.g. accounting, statutory reporting systems, human resources, customer relationship management, email servers and internal file servers),
   iv.) the type of external relationships allowed (for example, with partners, service providers, other entities of the group and their teleworking employees, including the justification for the legitimacy of these relationships),
   v.) for each of the services listed in point (iv), the logical security measures and mechanisms put in place, including what control the institution issuing the asset-referenced token has over such access and the nature and frequency of each control – for example, technical or organisational, preventive or detective, real-time monitoring or periodic scanning, such as use of a separate active directory from the group, opening/closing communication lines, configuration of security devices, generation of keys and client IDs, system monitoring, authentication, confidentiality of communications, intrusion detection; anti-virus systems and logs,
   vi.) logical security measures and mechanisms to control internal access to information systems;
e) a detailed assessment of the ICT risks involved in the issuance of asset-referenced tokens, including third-party service providers and all risks arising from dependency on the operating environment, as well as the risk of fraud. A detailed description of the risk mitigation measures introduced or planned, as required by Article 6 of the DORA and Articles 1, 3 and 27 of the RMF RTS;
f) the rules for the registration of the ICT systems' assets and the current records of the assets in accordance with Article 8 of the DORA and Articles 4-5 of the RMF RTS;
g) a description of the preventive protection and security principles applied in the operation of ICT systems, as required by Article 9 of the DORA, with the following scope and level of detail:
   i.) the encryption and cryptographic solutions used (Article 7 of the RMF RTS),
   ii.) ICT systems operating procedures and their regulation (Article 8 of the RMF RTS),
   iii.) capacity and performance management procedures and solutions (Article 9 of the RMF RTS),
   iv.) a description of the measures taken to address vulnerabilities and remediation programmes and updates (Article 10 of the RMF RTS),
   v.) the security classification of the data and ICT systems and the security measures applied based on the classification, as well as the rules for data sharing, transmission and storage, the data storage structure and the security solutions applied to data links (Article 11 of the RMF RTS),
   vi.) a description of the procedures and security measures used to ensure the secure operation of the network and the security of the data transmission, as well as the processes and technical solutions (authentication, registration, fraud prevention, etc.) used to monitor and secure the asset-referenced token transaction processes (Articles 13–14 of the RMF RTS),
   vii.) procedures and contracts for the procurement, development and maintenance of ICT systems (RMF RTS 16),
   viii.) processes, tools and policies to monitor changes to ICT systems (RMF RTS 17),
   ix.) the measures and mechanisms for the physical security of the applicant's premises and data centre, such as access control and environmental security features (RMF RTS 18),
   x.) the policies, procedures and systems in place for the secure management and recording of rights and access (RMF RTS 20–21),
   xi.) a description of the procedures for detecting, monitoring, managing and tracking security events and incidents affecting ICT systems and the information assets managed by them (RMF RTS 22);
h) the rules, systems and procedures in place to log and monitor events affecting ICT systems and to detect and respond to abnormal activities, in accordance with Article 10 of the DORA and Articles 12 and 23 of the RMF RTS;
i) the assessment and regulation of the necessary and applied service continuity, communication and crisis management measures, the related response and recovery plans and testing documents, in accordance with Article 11 of the DORA and Article 26 of the RMF RTS;
j) a description of backup policies and procedures, recovery and restoration procedures and methods in accordance with Article 12 of the DORA and Articles 24–25 of the RMF RTS;
k) pursuant to *'Commission Delegated Regulation (EU) 2024/1774 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk*

management tools, methods, processes, and policies and the simplified ICT risk management framework' , the contracts or agreements governing the activities of third parties providing or supporting as a service the processes for the handling, processing, storage or deletion of data in ICT systems, and the internal procedures for the use of such services; the technological and organisational arrangements for risk management and service continuity and accountability.

IV. Conduct of the procedure

Legal persons or other undertakings intending to provide crypto-asset services should submit **their application for authorisation** as a crypto-asset service provider to the competent authority of the Member State where they are established, or in the case of a company established in Hungary, to the MNB.

The MNB shall acknowledge receipt of the application in writing to the applicant crypto-asset service provider within two working days of receipt of the application **(acknowledgement of receipt**), pursuant to Article 63(1) MiCA.

Pursuant to Article 62(2) MiCA, the MNB shall assess within **25 working days** of receipt of the application whether the application, comprises all of the required information. If the application is missing any required information, the MNB will immediately notify the applicant and set a deadline for the applicant crypto-asset service provider to provide the missing information. If the application is still incomplete after the deadline set by the MNB, the MNB may refuse to process the application.

Pursuant to Article 63(4) MiCA, once the application is complete, the MNB will notify the applicant crypto-asset service provider without delay (**certificate of completeness**).

Pursuant to Article 63(9) MiCA, within **40 working days of receipt of a complete application**, the MNB shall assess whether the applicant crypto-asset service provider complies with the requirements of Title V and take a fully reasoned draft decision granting or refusing authorisation. In making its assessment, the MNB will take into account the nature, scale and complexity of the crypto-asset services that the applicant crypto-asset service provider intends to provide.

Pursuant to Article 63 (12) MiCA within 20 working days of receipt of a complete application, in case of incomplete or incorrect submission of the specified information the MNB **may request information** from the applicant crypto-asset service provider on the application which is necessary to complete the assessment. The period between the MNB's request for missing information and the receipt of the applicant crypto asset provider's response is not included in the assessment deadline. The MNB may set a maximum deadline of 20 working days for the completion. The MNB may also ask for any other information from the applicant to supplement or clarify information is at its discretion, however, the deadline provided for the fulfilment of such request for information is included in the 40-working-day assessment period.

Pursuant to Article 63(5) MiCA, before granting or refusing authorisation as a crypto-asset service provider, the MNB shall consult the competent authorities of another Member State where the applicant crypto-asset service provider is in one of the following positions in relation to a credit institution, a central securities depository, an investment firm, a market operator, a UCITS management company, an alternative investment fund manager, a payment institution, an insurance undertaking, an electronic money institution or an institution for occupational retirement provision, authorised in that other Member State:
a) it is its subsidiary;
b) it is a subsidiary of the parent undertaking of that entity;
c) or it is controlled by the same natural or legal persons who control that entity.

Pursuant to Article 63(6) MiCA, before granting or refusing an authorisation as a crypto-asset service provider, the MNB:
(a) may consult the competent authorities for anti-money laundering and counter-terrorist financing, and financial intelligence units, in order to verify that the applicant crypto-asset service provider has not been the subject of an investigation into conduct relating to money laundering or terrorist financing;
(b) shall ensure that the applicant crypto-asset service provider that operates establishments or relies on third parties established in high-risk third countries identified pursuant to Article 9 of Directive (EU) 2015/849 complies with the provisions of national law transposing Articles 26(2), 45(3) and 45(5) of that Directive;

(c) shall, where appropriate, ensure that the applicant crypto-asset service provider has put in place appropriate procedures to comply with the provisions of national law transposing Article 18a(1) and (3) of Directive (EU) 2015/849.

Where close links exist between the applicant crypto-asset service provider and other natural or legal persons, the MNB shall grant authorisation only if those links do not prevent the effective exercise of their supervisory functions. The MNB shall refuse authorisation if the laws, regulations or administrative provisions of a third country governing one or more natural or legal persons with which the applicant crypto-asset service provider has close links, or difficulties involved in their enforcement, prevent the effective exercise of their supervisory functions.

The MNB shall, within two working days of granting authorisation, communicate to ESMA the information specified in Article 109(5) and any refusals of authorisations. ESMA shall make the information referred to in Article 109(5) available in the register referred to in that Article by the starting date of the provision of crypto-asset services.

In addition to the above, applicants should also take note of the following information published on the MNB website:
'Information on certain issues most frequently arising in certain licensing and registration procedures affecting the practice of the MNB'.[13]

V. Cases of refusal of a request for authorisation

Article 63(10) of the MiCA lists the circumstances in which the MNB shall refuse a request where there are objective and demonstrable grounds that:
(a) the management body of the applicant crypto-asset service provider poses a threat to its effective, sound and prudent management and business continuity, and to the adequate consideration of the interest of its clients and the integrity of the market, or exposes the applicant crypto-asset service provider to a serious risk of money laundering or terrorist financing;
(b) members of the management body of the applicant crypto-asset service provider do not meet the criteria set out in Article 68(1);
(c) the shareholders or members, whether direct or indirect, that have qualifying holdings in the applicant crypto-asset service provider do not meet the criteria of sufficiently good repute set out in Article 68(2);
(d) the applicant crypto-asset service provider fails to meet or is likely to fail to meet any of the requirements of this Title.

VI. Administrative service fee

Pursuant to Section 19/A (1) of MNB Decree 32/2023 (VII. 19.) of the Governor of the Magyar Nemzeti Bank on the administrative service fees of the Magyar Nemzeti Bank applied in certain licensing and registration procedures in the context of the supervision of the financial intermediary system and with respect to fiduciary asset management companies, the conduct of the authorisation procedure is subject to the payment of an administrative service fee of HUF 1,900,000.

Further information about the administrative service fee is available in the following link:
https://www.mnb.hu/letoltes/tajekoztatas-a-magyar-nemzeti-bank-altal-egyes-engedelyezesi-es-nyilvantartasbaveteli-eljarasokban-alkalmazott-igazgatasi-szolgaltatasi-dijrol.pdf

If, after reviewing these guidelines, further questions arise which cannot be answered in a telephone or written consultation on a specific case, the MNB will also provide the applicant with the opportunity for personal consultation. For personal consultations, please contact the Secretariat of the Financial and Capital Markets Licensing Department (phone: +36 1-489-9731; e-mail: ptef@mnb.hu).
If the questions you have are purely IT-related, you may also contact the IT Supervision Department directly for a personal consultation (phone: +36 1-489-9780; e-mail: iff@mnb.hu).

[13] Available at: https://www.mnb.hu/letoltes/tajekoztato-az-egyes-engedelyezesi-illetve-nyilvantartasba-veteli-eljarasok-soran-leggyakrabban-felmerulo-a-ma-gyar-nemzeti-bank-mnb-gyakorlatat-erinto-kerdesekkel-kapcsolatban-1.pdf

Dated: March 2025