UNOFFICIAL TRANSLATION

Recommendation 3/2026 (III.25.) of the Magyar Nemzeti Bank on internal policies, procedures, and controls ensuring the implementation of EU and national restrictive measures related to transfers of funds and transfers of certain crypto-assets

I. Purpose and effect of the Recommendation

The purpose of this recommendation is to set forth the expectations of Magyar Nemzeti Bank (hereinafter: "MNB") and thereby increase the predictability of law enforcement, and to facilitate the uniform application of relevant legislation by defining the factors that payment service providers and crypto-asset service providers supervised by the MNB must introduce with respect to their internal policies, procedures, and control mechanisms in the execution of their transfer of funds and transfers of crypto-assets under Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 to ensure the effective implementation of EU and national restrictive measures.

These policies, procedures, and controls must enable payment service providers and crypto-asset service providers to identify persons subject to restrictive measures, and must also ensure that payment service providers and crypto-asset service providers take the necessary measures to ensure that they do not make funds or crypto-assets available to such persons, do not execute financial transactions or provide services prohibited by the restrictive measures, and manage the risk of circumvention of the restrictive measures.

The recommendation transposes the Guidelines of the European Banking Authority (hereinafter: "EBA") published on 13 November 2024, titled "Guidelines on internal policies, procedures, and controls to ensure the implementation of Union and national restrictive measures" (EBA/GL/2024/15;[1] hereinafter: "EBA Guidelines"). Based on the requirements set forth in the EBA Guidelines, the MNB defines in this recommendation the practices to be followed by service providers falling within the scope of this recommendation. By publishing this recommendation, the MNB ensures compliance with the provisions of the EBA Guidelines.

The addressees of this recommendation are payment service providers as defined in Article 3(5) and crypto-asset service providers as defined in Article 3(15) of Regulation (EU) 2023/1113 of the European Parliament and of the Council (hereinafter collectively: Service Provider) with a registered office or branch in Hungary, as well as those registered or established in another Member State of the European Union and offering services directly to customers and participating in the transfer of funds and transfer of crypto-assets through a permanent business

[1] https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-countering-financing-terrorism/guidelines-internal-policies-procedures-and-controls-ensure-implementation-union-and-national

unit in Hungary in the form of a permanent domestic presence.

This recommendation does not refer comprehensively to the legislative provisions when formulating principles and requirements, but the addressees of the recommendation remain, of course, obliged to comply with the relevant legislative requirements. The contents of the recommendation are in accordance with the regulations that define the European framework for the operation of financial entities.

This recommendation does not provide guidance on data processing or data protection issues, and the requirements set forth herein shall in no way be construed as authorisation to process personal data. Data processing in connection with the fulfilment of the supervisory requirements set out in this recommendation, subject to the provisions of Regulation (EU) 2023/1113 of the European Parliament and of the Council, may only be carried out in compliance with the data protection laws in force at any given time.

II. Interpretative provisions

1. For the purposes of this recommendation:

1.1. *sector-specific restrictive measures:* restrictive measures such as embargoes on arms and related equipment or economic and financial measures (e.g., import and export restrictions, as well as restrictions on the provision of certain services, such as banking services);

1.2. *targeted financial sanctions:* with respect to persons and entities listed pursuant to Council Decisions adopted under Article 29 of the Treaty on European Union and Council Regulations adopted under Article 215 of the Treaty on the Functioning of the European Union, both the freezing of assets, as well as the prohibition on making funds or other financial assets available to them, either directly or indirectly;

1.3. *restrictive measures:* the financial and asset-related restrictive measures specified in Section 2(5) of Act LII of 2017 on the Implementation of Financial and Asset-related Restrictive Measures Ordered by the European Union and the UN Security Council (hereinafter: "FRM Act"), the atypical financial restrictive measures referred to in Section 3(2a) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: "AML Act"), as well as national restrictive measures adopted in accordance with the Hungarian legal system, insofar as they apply to financial institutions.

1.4. In addition to the provisions of Sections 1.1–1.3, the terms used in this recommendation shall be interpreted in accordance with the definitions set forth in the AML Act and Regulation (EU) 2023/1113 of the European Parliament and of the Council.

III. Internal policies, procedures, and controls ensuring the implementation of EU and national restrictive measures pursuant to Regulation (EU) 2023/1113 of the European Parliament and of the Council

III.1. General provisions

2. The MNB expects the Service Provider to implement policies, procedures, and controls to ensure compliance with restrictive measures. The MNB expects these policies, procedures, and controls to be developed in accordance with the provisions of MNB Recommendation 1/2026 (II.24) on compliance officers, their duties and responsibilities and on related internal procedures and controls to combat money laundering and terrorist financing.

3. It is expected that these policies, procedures, and controls will enable the Service Provider to identify persons subject to restrictive measures and also allow the Service Provider to take the necessary measures to ensure that it does not make funds or crypto-assets available to such persons, does not execute financial transactions or services prohibited by the restrictive measures, or manages the risk of circumvention of the restrictive measures.

III.2. Screening related to restrictive measures

4. The MNB expects the Service Provider to implement an effective screening system to reliably identify the subjects of the restrictive measures specified in detail in Section III.4.5.

III.2.1. Selection of the screening system

5. The Service Provider is expected to use its assessment of exposure to restrictive measures to determine which screening system to use or to validate the screening system it uses to ensure compliance with restrictive measures. The Service Provider is expected to tailor the screening system to the size, nature, and complexity of its business activities, as well as to its exposure to restrictive measures.

6. When making a decision regarding the screening system, the MNB expects the Service Provider, to assess whether it can provide the resources necessary for the effective use of the selected system.

7. The MNB expects the Service Provider to regularly review the performance of its screening system to ensure that it remains effective and continues to reliably identify the targets of restrictive measures. The Service Provider is expected to review the screening system at least once a year, and immediately if it has reason to believe that the system may not be fit for purpose.

8. Taking into account Article 7 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) 1060/2009, (EU) 648/2012, (EU) 600/2014, (EU) 909/2014 and (EU) 2016/1011, the Service Provider must understand and document the capabilities and limitations of the screening system. The MNB expects the Service Provider to be able to demonstrate, upon request by the MNB, that its screening system is adequate.

III.2.2. List management

9. The MNB expects the Service Provider to refer in its policies and procedures to the restrictive measures it is required to apply.

10. The MNB expects the Service Provider to have policies and procedures in place
    a) that identify when new restrictive measures are to be adopted, or when existing restrictive measures are to be updated or terminated;
    b) based on which, in accordance with Section III.2.3, following the entry into force of a new restrictive measure or the updating or termination of an existing restrictive measure, the Service Provider shall immediately update its dataset; and if the Service Provider uses a screening system provided by an external service provider, it shall select a screening system that ensures the immediate updating of the dataset.

III.2.3. Determining the scope of data to be screened

11. The Service Provider is required to specify in its policies and procedures what types of data it will screen for each type of restrictive measure, taking into account the results of its assessment of exposure to restrictive measures and the restrictive measures it applies.

12. The MNB expects that, when determining the dataset to be screened by type of restrictive measure, the Service Provider shall take into account all data it holds on its customers, including information received

    a) in the course of application of customer due diligence measures; and
    b) compliance with Regulation (EU) 2023/1113 of the European Parliament and of the Council.

13. In accordance with the requirements of Regulation (EU) 2023/1113 of the European Parliament and of the Council, the Service Provider must assess whether the data in its possession are sufficiently accurate, up-to-date, and detailed enough to enable it to determine whether the party involved in the data transfer, its beneficial owner, or any person acting on their behalf or authorised by them is subject to restrictive measures.

14. The MNB expects the Service Provider to include natural or legal persons, organisations, or bodies that are not subject to restrictive measures but have been incorrectly identified by the existing screening system on an internal list (whitelisting) in order to avoid repeated false alerts regarding such persons. It is also required that the Service Provider document the grounds for the decision to add a given person to the whitelist, review the list immediately following the entry into force of a new or modified restrictive measure or a change in customer data, and that the Service Provider disclose the fact that it uses a whitelist and the possibility of data processing related to this listing in its general privacy notice.

III.2.4. Screening of the customer base

15. The MNB expects the Service Provider to specify in its policies and procedures for how it will screen its customer base.

16. The Service Provider is expected to regularly review its entire customer database and determine the frequency of customer screening based on an assessment of its exposure to restrictive measures.

17. The MNB expects the Service Provider to establish internal procedures specifying when customer screening must take place in all cases and to keep these decisions up to date. It is expected that the range of events triggering screening shall include at least the following:

a) any modification of existing listings or restrictive measures, the entry into force of a new designation or a new restrictive measure;
b) prior to the execution of a transaction order or the establishment of a business relationship;
c) if significant changes occur in an existing customer's customer due diligence data, such as a change of name, residence, nationality, or business activity;
d) if there are reasonable grounds to suspect that the customer or a person intending to act on the customer's behalf or authorised to do so is attempting to circumvent the restrictive measures.

18. The Service Provider is required to verify, in accordance with the restrictive measures, at least the following customer information:

a) in the case of a natural person: first name and last name, in both the original and transliterated[2] versions, as well as the date of birth;
b) in the case of a legal entity: the name of the legal entity, in both the original and transliterated versions;
c) in the case of a natural person, legal entity, body, or organisation: other names, including trade names and wallet addresses, if available in the lists related to restrictive measures; the MNB expects the Service Provider to adequately justify, through an assessment of its exposure to restrictive measures, why it does not examine such information if it is available.

19. It is expected that when screening legal entities, natural persons, bodies, or organisations, the Service Provider, should also screen, provided that this information is available, the following:

a) beneficial owners through ownership interests;
b) beneficial owners exercising controlling influence;
c) persons intending to act on behalf of the customer or authorised to do so.

The MNB also considers it good practice for the Service Provider to extend the above screening to owners who do not qualify as beneficial owners.

[2] Transliteration is a type of transcription in which, for two alphabets with different letter or syllable systems, each letter of the source text corresponds to a single, double, or triple-letter character, a diacritical mark, or a combination thereof in the target script. Transcription is a phonetic transcription in which the letters of one writing system correspond to letters in the other writing system based on their pronunciation. (source: https://www.offi.hu/sites/default/files/media/files/8-ugroczky-maria.pdf, p. 142)

III.2.5. Screening of transfer of funds and crypto-asset transfers

20. The MNB expects that, with the exception of cases falling under Article 5d of Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009, the payment service provider should review transfers of funds before making the funds available to the payee, and that the crypto-asset service provider should review all crypto-asset transfers before making the crypto-assets available to the crypto-asset beneficiary, regardless of whether they are executed as part of a business relationship or as part of a one-off transaction.

21. The MNB expects the Service Provider to screen all parties involved in transfers of funds or crypto-asset transfers in accordance with the relevant restrictive measures. The MNB expects the Service Provider, when assessing its exposure to restrictive measures, to pay particular attention to the soundness and reliability of the policies and procedures regarding restrictive measures implemented by other Service Providers with whom it has a business relationship to ensure compliance with such measures.

22. The MNB expects the Service Provider to examine all data that may be relevant to assessing whether a transaction is subject to the restrictive measures in order to apply such measures. The data to be examined is expected to cover at least the following:

a) data concerning the payer and the payee pursuant to Article 4 of Regulation (EU) 2023/1113 of the European Parliament and of the Council;
b) information regarding the originator and the beneficiary as specified in Article 14 of Regulation (EU) 2023/1113 of the European Parliament and of the Council;
c) the purpose of the transfer of funds or the transfer of crypto-assets, as well as, where available and subject to an assessment of exposure to restrictive measures, other free-text fields providing additional information on the actual sender or recipient of the funds or crypto-assets;
d) the details of payment service providers and crypto-asset service providers involved in the transfer of funds or crypto-assets, including intermediary institutions and correspondent banks, by screening identification codes such as BIC, SWIFT, and other identification codes;
e) other details regarding the transfer of funds or the transfer of crypto-assets, depending on the nature and type of the transaction, the supporting documentation received, if information is available and falls within the scope of the exposure assessment for restrictive measures;
f) the wallet addresses of the initiator and beneficiary of the crypto-asset transfer, provided that this information is available on the official lists of wallet addresses related to restrictive measures.

23. In accordance with the provisions of the MNB recommendation on data reporting

requirements related to transfers of funds and certain crypto-asset transfers[3] regarding missing or incomplete data, new information obtained subsequently, either before or after the execution of the transfer, is also expected to be reviewed.

24. The MNB considers it good practice for the crypto-asset service provider, where appropriate, to assess – based on the volume and number of crypto-asset transfers – whether to incorporate blockchain analysis into its existing operational system for the purpose of monitoring transactions.

III.2.6. Calibration

25. The MNB expects the Service Provider to determine how to calibrate the settings of the automated screening system in a manner that, on the one hand, maximises the quality of alerts and leads to unambiguous identification, while also ensuring compliance with restrictive measures. The MNB expects that, in order to assess exposure to restrictive measures and based on regular testing, the Service Provider shall, for at least

a) each restrictive measure, determine the appropriate reconciliation parameters that are likely to result in a reasonable alert, that enables the Service Provider to fulfil its obligations regarding restrictive measures, while verifying the thresholds for true positive results associated with different compliance rates. The calibration must not be too sensitive, which would result in a large number of false positives, nor too lax, which would result in listed individuals, organisations, or entities not being detected, or in free-form information not being used for other restrictive measures;
b) use a screening system that allows for the application of an algorithm-based technique capable of matching a given name or phrase, even if the content of the information being screened is not identical, but its spelling, or sound closely matches the content in the dataset used for screening ("partial match" techniques) and is capable of calibrating the degree of "partial match" in its screening system.

26. The Service Provider is expected to decide on calibration both prior to the development of the new screening system and periodically, in accordance with the assessment of its exposure to restrictive measures, and to document this decision with justification and make it available to the MNB upon request.

III.2.7. Use of third-party services and outsourcing

27. The MNB expects the Service Provider to specify in its policies and procedures what steps the Service Provider or the service providers performing outsourced activities will take to ensure compliance with restrictive measures. The MNB expects that, with regard to the outsourcing of services, the Service Provider apply the following key principles taking into account, where relevant, the MNB recommendation on the use of external service providers[4]:

[3] At the time of issuance of this recommendation: Section III.6 of MNB Recommendation 8/2025(VI.26) on data reporting requirements relating to money transfers and certain crypto-asset transfers (https://www.mnb.hu/letoltes/8-2025-adatkozlesi-kovetelmenyekrol-ajanlas.pdf).

[4] At the time of issuance of this recommendation: MNB Recommendation 7/2020 (VI.3.) on the use of external service providers (https://www.mnb.hu/letoltes/7-2020-kulso-szolgaltato-igenybevetele.pdf).

a) the ultimate responsibility for compliance with restrictive measures, regardless of whether certain tasks have been outsourced or not, rests with the Service Provider;
b) the rights and obligations of the Service Provider and the service provider performing the outsourced activity must be clearly distinguished and defined in a written agreement;
c) the Service Provider relying on the outsourcing agreement must remain accountable for monitoring and supervising the quality of services provided by the service providers performing the outsourced activities;
d) the same regulatory framework must apply to intra-group outsourcing as to outsourcing to service providers outside the group.

28. The MNB expects the Service Provider to implement and apply the necessary controls to ensure that the use of a service provider performing the outsourced activity does not expose it to the risk of violating restrictive measures, and that these controls are documented in the outsourcing agreement.

29. If the Service Provider needs to update the data to be used regarding natural persons, legal entities, organisations, and bodies subject to restrictive measures, the MNB expects the Service Provider to ensure that the service agreement minimises the risk of the Service Provider violating the restrictive measures to the greatest extent possible.

30. The MNB expects that, during the term of the outsourcing agreements, the Service Provider regularly verify whether the service provider performing the outsourced activity complies with the obligations arising from the agreement, assess the effectiveness of the services covered by the agreement, and take the necessary risk-mitigation measures, including renegotiating the agreement.

31. The requirements set forth in paragraphs 27–30 do not affect the obligations and tasks of Service Providers regarding digital operational resilience as defined in Regulation (EU) 2022/2554 of the European Parliament and of the Council.

III.3. Screening and control measures for the analysis of alerts

III.3.1. Policies and procedures for handling and analysing alerts

32. The MNB requires the Service Provider to have policies and procedures in place for investigating alerts related to restrictive measures, which enable the Service Provider to confirm whether the alert is indeed a positive match and, if so, determine the actions necessary to comply with the restrictive measure.

33. It is expected that this policy and procedure cover the following:
a) steps to initiate the investigation of all potential matches without delay for each individual transfer of funds or crypto-asset transfer;
b) rules consistent with the Service Provider's general record-keeping policy regarding the documentation of decisions made in connection with alerts;
c) measures aimed at compliance with Section III.3.2;
d) conducting reviews at various levels in accordance with the assessment of exposure to restrictive measures, with reviews in cases of higher exposure being performed by at

least two persons.

III.3.2. Measures to be applied during the screening necessary for the analysis of alerts

34. The MNB expects that the relevant element of the restrictive measure be indicated in the alert generated by the screening system. It is good practice for alerts to be analysed by employees who possess the necessary expertise and appropriate training[5].

35. The MNB considers it good practice that, if doubts arise regarding the authenticity of a match, the Service Provider should use additional information in its possession or that can be obtained to support the analysis of the alerts, provided that such information is available and was not used during the screening stage, for example

a) identification data of a natural person, legal entity, organisation, or body;
b) information regarding the place of residence of a natural person, and the registered office or registered address of a legal entity, organisation, or body;
c) information regarding the citizenship and nationality of a natural person;
d) data regarding representation, management, and organisational structure with respect to a legal entity;
e) contact information.

36. The Service Provider is expected to specify in its policies and procedures how to handle cases where, following further review, it cannot be clearly determined whether the match is a true positive, a false positive, or a case of homonyms. The MNB expects the Service Provider to refrain from providing financial services to the party involved in the transfer or transfer until a well-founded decision has been made.

III.3.3. Assessment of whether an entity is owned or controlled by a listed person

37. The Service Provider is expected to specify in its policies and procedures how it will assess whether a legal entity or organisation is owned or controlled by a listed person or organisation.

38. The MNB expects the Service Provider to

a) apply the criteria set forth in the European Council's guidelines on sanctions[6] and in Section VIII of its best practices[7] to determine whether a legal entity is owned or controlled by another person or entity;
b) apply the criteria used to identify beneficial owners under applicable law[8];
c) use publicly available information sources at its disposal, such as registries of ownership and governance structures of organisations and beneficial ownership registries.

---

[5] See at the time of issuance of this recommendation: as to be determined in the internal procedure referred to in Section 5(i) of Annex 1 to MNB Recommendation 1/2026 (II.24) on compliance officers, their duties and responsibilities and on related internal procedures and controls to combat money laundering and terrorist financing.

[6] At the time of issuance of this recommendation: https://data.consilium.europa.eu/doc/document/ST-11618-2024-INIT/hu/pdf (document no. 11618/24).

[7] At the time of issuance of this recommendation: https://data.consilium.europa.eu/doc/document/ST-11623-2024-INIT/hu/pdf (document no. 11623/2024).

[8] At the time of issuance of this recommendation: Section 3(38) of Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing.

39. If the assessment remains inconclusive, the MNB considers it good practice for the Service Provider to consider contacting the Central Directorate of the National Tax and Customs Administration's Office for Combating Money Laundering and Terrorist Financing (hereinafter: "NTCA KI PEI"). Ultimate responsibility for compliance with restrictive measures rests with the Service Provider.

III.3.4. Checks and screenings necessary to ensure compliance with sector-specific restrictive measures

40. The MNB expects the Service Provider to take into account the assessment of exposure to restrictive measures when determining what types of checks it will apply to ensure compliance with restrictive measures. As part of this, the Service Provider should determine what available information it will screen in connection with a given transaction.

41. The MNB expects the Service Provider to pay particular attention to sector-specific restrictive measures related to a given jurisdiction or territory. In the event that such restrictive measures are in place, the Service Provider is expected to review transfer of funds or crypto-asset transfers to or from the given jurisdiction or territory, or from that jurisdiction or territory, as well as all underlying information regarding transfer of funds or crypto-asset transfers initiated by customers known to conduct business activities in that jurisdiction or territory. Where available, the MNB expects the Service Provider to review the following:

a) information regarding the country(ies) of citizenship and place of birth;
b) information regarding the usual place of residence or the principal place of business through other addresses, in accordance with the assessment of exposure to restrictive measures;
c) information regarding the country to or from which the funds transfer is made, where the funds transfer is executed;
d) the purpose of the transfer of funds or crypto-assets and other free-text fields that provide additional information, in accordance with the assessment of exposure to restrictive measures, regarding the goods, vessels, country of destination, or country of origin of the goods in connection with which the payment is made.

42. Where the assessment of exposure to restrictive measures justifies it, the MNB considers it good practice for the Service Provider to consider incorporating geolocation tools and tools for detecting the use of proxy services into its screening system, in order to identify and prevent IP addresses originating from countries subject to restrictive measures due to the situation affecting that country from accessing the Service Provider's website and services in connection with activities prohibited by the regulatory framework governing such restrictive measures.

43. The MNB considers it good practice for the Service Provider to consider applying specific controls based on an assessment of exposure to restrictive measures, such as

a) requesting additional information from the customer, such as a description of dual-use items or items subject to sector-specific restrictive measures, information regarding the appropriate license required for the handling of dual-use items, the country of origin of the goods, and information regarding the end-user of the goods;
b) requesting more detailed information from the customer regarding the purpose of the

transfer of funds;

c) the use of the following data: shipping registers, real estate registers, and other publicly available datasets (where available).

44. If the Service Provider uses functions to automatically read information from documents related to transfer of funds or crypto-asset transfers, such as optical character recognition algorithms or machine-readable zone verification, it is expected to take the necessary steps to ensure that these tools capture the information accurately and consistently.

III.3.5. Screening mechanisms designed to detect attempts to circumvent restrictive measures

45. The MNB expects the Service Provider to stay continuously informed about the typology and trends of attempts to circumvent restrictive measures. With regard to the range of relevant information sources, the Service Provider is expected to always take into account at least the reports shared by the following:

a) the MNB, the NTCA, the PEI, and law enforcement authorities;
b) relevant national or EU-level public-private partnerships;
c) European Union authorities[9].

46. The MNB expects that the screening policy and procedure shall enable the Service Provider to detect possible attempts to circumvent restrictive measures, such as attempts to do the following:

a) omission, deletion, or altering information contained in payment messages;
b) transfers made through persons associated with a customer subject to restrictive measures;
c) structuring transfers of funds or crypto-asset transfers in such a way as to concealing the involvement of a listed party;
d) using falsified or fraudulent supporting documentation for transfer of funds or crypto-asset transfers;
e) the use of falsified or fraudulent supporting documentation for the transfer of funds or crypto-asset transfer.

47. If the Service Provider is particularly exposed to the risk of being used to circumvent restrictive measures, the MNB considers it good practice for the Service Provider to consider conducting a comprehensive analysis of payment transactions to or from countries subject to restrictive measures, as well as to countries known to be used to circumvent such measures.

III.4. Freezing and measures regarding the filing of reports

III.4.1. Suspension of the execution of money transfers and freezing of funds

48. The MNB requires that the payment service provider have policies and procedures in place to ensure the immediate suspension of any transaction that triggers an alert for a potential match

[9] See for example: https://finance.ec.europa.eu/news/sanctions-commission-publishes-guidance-help-european-operators-assess-sanctions-circumvention-risks-2023-09-07_en.

with a listed person or entity, or with a person or entity owned, held, or controlled by a listed person or entity, or with the beneficial owner of a listed person or entity.

49. If the payment service provider's internal analysis of such an alert confirms that a potential match exists with a listed person or entity, or with a person or entity owned, held, or controlled by a listed person or entity, or with the beneficial owner of a listed person or entity, the payment service provider is required to immediately perform the following tasks:

a) freezing the relevant funds;
b) suspending the execution of any transfer of funds that would violate the restrictive measures.

III.4.2. Freezing the transfer of crypto-assets

50. The MNB expects the crypto-asset service provider to have policies and procedures in place in the event that an internal analysis of an alert confirms a potential match with a listed person or entity, or with a person or entity owned, held, or controlled by a listed person or entity, or with the beneficial owner of a listed person or entity, in order to immediately freeze and lock the crypto-assets in the suspended crypto-asset account until the NTCA KI PEI has instructed the crypto-asset service provider on what steps to take regarding the crypto-assets concerned. The crypto-asset service provider bears ultimate responsibility for the implementation of these restrictive measures.

III.4.3. Measures regarding reporting

51. The Service Provider is required to have a clear procedure, set forth in a policy or procedure, to enable it to report the following to the NTCA KI PEI immediately or within a specified time limit:

a) any action taken for the purpose of a specific transfer or conveyance related to the restrictive measure;
b) the discovery of a violation of the restrictive measures; and
c) the execution of a transfer of funds or a transfer of crypto-assets that violates the restrictive measure, while also providing information on the circumstances, such as an incident in the operation of the screening system related to the transfer.

52. If there is a suspicion of circumvention or an attempt to circumvent the restrictive measures, upon detection thereof, the Service Provider must

a) report this to the NTCA KI PEI, provided that this is expressly required by the EU legal act on restrictive measures[10];
b) file a report on the suspicious transaction,[11]
c) immediately notify the NTCA KI PEI if, despite the prohibition, assets are made available to the subject of the restrictive measure[12].

[10] the obligation specified in Section 4(1) of the FRM Act.
[11] the obligation specified in Section 30(1) of the AML Act.
[12] the obligation specified in Section 9(1) of the FRM Act.

III.4.4. Procedures regarding exemptions or the termination of restrictive measures

53. The MNB expects the Service Provider to have rules and procedures in place to determine whether exemptions or authorisation systems apply, and if they do, how to proceed in order to comply with the applicable EU legal act, the FRM Act, and other relevant domestic legislation[13]. The Service Provider must specify in its policies and procedures what information it will provide to customers who wish to apply for an exemption regarding the use of their frozen funds, provided that the applicable legal framework permits such an exemption. The MNB expects that the information on the procedure for requesting an exemption should also contain the information regarding the customer's rights in such situations.

54. The Service Provider is expected to have policies and procedures in place that specify the measures to be applied following the lifting of special restrictive measures regarding funds or crypto-assets subject to such measures.

III.4.5. Ensuring the continuous effectiveness of screening policies, procedures, and systems related to restrictive measures

55. To ensure effectiveness, the MNB requires that the Service Provider's screening policies, procedures, and systems regarding restrictive measures enable the Service Provider to

a) reliably detect positive matches;
b) immediately suspend the execution of money transfers following confirmation of positive matches, block incoming transfers and place them in a suspension account, and immediately freeze funds or crypto-assets, and report these measures to the NTCA KI PEI for further instructions;
c) report the frozen assets to the NTCA KI PEI immediately, as specified in the FRM Act, or within the deadline set forth in the applicable EU legal act, in accordance with the provisions of the applicable legislation;
d) report any suspicion of or attempt to circumvent the restrictive measures to the NTCA KI PEI with regard to the enforcement of the restrictive measures; and
e) immediately notify the NTCA KI PEI if, despite the prohibition, assets are made available to the subject of the restrictive measure.

56. The MNB expects the Service Provider to regularly test the settings of its screening system to determine whether the screening system remains suitable for assessing the Service Provider's exposure to restrictive measures and whether it remains effective. It is also expected that the Service Provider will determine the frequency of checks based on the assessment of its exposure to restrictive measures and will set these out in its policies and procedures.

57. The MNB expects that, during the testing of its screening system, the Service Provider

a) test the calibration of the screening system as specified in Section III.2.6;
b) assess the accuracy of list management by applying the applicable and up-to-date restrictive measures;

[13] Government Decree 456/2025 (XII. 29.) on the national list of terrorist entities and the restrictive measures applicable to those listed therein, as well as the scope of such measures, as in effect at the time of issuance of this recommendation.

c) assess whether all customers, transfers of funds and crypto-asset transfers are screened as necessary;
d) assess the adequacy and relevance of the information fields used in the screening system, such as the scope of transfer of funds or crypto-asset transfers checked by the screening system;
e) assess the timeliness of the automatic suspension of transactions;
f) assess whether the processes and resources available for analysing alerts allow for the immediate reporting of true positive matches.

58. The MNB expects the Service Provider's governing body to be informed of any significant weaknesses or deficiencies in the screening system and for the Service Provider to take corrective measures without delay.

IV. Closing provisions

59. The recommendation is a regulatory instrument issued pursuant to Section 13(2) i) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank, which is not binding on supervised financial institutions. The content of the recommendation issued by the MNB expresses the requirements set out in the legislation, the principles and methods recommended for application based on the MNB's practice of applying the law, as well as market standards and customs.

60. Compliance with the recommendation is monitored and assessed by the MNB among the financial institutions under its supervision during its inspection and monitoring activities, in line with general European supervisory practice.

61. The MNB draws attention to the fact that financial institutions may incorporate the content of the recommendation into their rules. In this case, the financial institution is entitled to indicate that the provisions of its relevant rules comply with the recommendation issued by the MNB under the relevant number. If the financial institution only wants to include parts of the recommendation in its rules, it should avoid referring to the recommendation or only use it for the parts taken from the recommendation.

62. The MNB expects the Service Providers concerned to apply this recommendation from 31 March 2026.

Mihály Varga sgd.
Governor of the Magyar Nemzeti Bank