MNB Recommendation 8/2025 (VI. 26.)

on data reporting requirements relating to transfers of funds and certain crypto-asset transfers

I. Purpose and effect of the Recommendation

The purpose of this Recommendation is to set out the requirements of the Magyar Nemzeti Bank (hereinafter referred to as 'MNB') and thereby increase the predictability of the application of the law and promote the uniform application of the relevant legislation by specifying the factors that payment service providers, intermediary payment service providers, crypto-asset service providers and intermediary crypto-asset service providers supervised by the MNB are advised to take into account when establishing procedures and implementing measures relating to transfers of funds and crypto-asset transfers, that aim to detect missing or incomplete data relating to the payer, the originator or the payee, as well as the crypto-asset beneficiary, and to handle the transfers of funds and crypto-asset transfers concerned.

The Recommendation also aims to set out the MNB's requirements regarding the procedures to be established by payment service providers, crypto-asset service providers, intermediary payment service providers and intermediary crypto-asset service providers to manage the risks of money laundering and terrorist financing if the required information relating to the payer, the originator, the payee or the crypto-asset beneficiary is missing or incomplete.

The Recommendation transposes the guidelines of the European Banking Authority (hereinafter referred to as 'EBA') published on 4 July 2024, entitled *'Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113 (Travel Rule Guidelines)'* (EBA/GL/2024/11)[1] (hereinafter referred to as 'EBA Guidelines'). Based on the requirements set out in the EBA Guidelines, the MNB defines the practices to be followed by service providers in this Recommendation. By publishing this Recommendation, the MNB ensures compliance with the provisions of the EBA Guidelines.

Prior to publication of the EBA Guidelines, Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 amending Directive (EU) 2015/849 as regards data accompanying transfers of funds and certain transfers of crypto-assets (hereinafter referred to as 'Regulation') was published, and the requirements of the MNB related to applying the provisions of the Regulation to direct debits are set out in this Recommendation.

In addition to the above, this Recommendation sets out guidelines on measures to identify and assess money laundering and terrorist financing risks associated with crypto-asset transfers to or from self-hosted addresses.

The Recommendation is addressed to payment service providers with their registered office or branch in Hungary, as well as payment service providers registered or established in another Member State of the European Union and offering services directly to customers in the form of a permanent domestic presence through a permanent business unit established in Hungary, participating in the transfer of funds or crypto-asset transfers, as well as payment service providers as defined in paragraph (5), intermediary payment service providers as defined in paragraph (6), crypto-asset service providers as defined in paragraph (15) and intermediary crypto-asset service providers as

[1] https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf

defined in paragraph (16) of Article 3 of the Regulation (hereinafter jointly referred to as 'Service Provider').

This Recommendation does not refer comprehensively to the legislative provisions when formulating principles and requirements, but the addressees of the Recommendation are still naturally obliged to comply with the relevant legislative requirements. The recommendations are consistent with the provisions of the European framework for the functioning of financial institutions.

This Recommendation does not provide guidance on data processing or data protection issues, and the requirements set out herein may not be interpreted in any way as authorisation to process personal data. Data processing in connection with the fulfilment of the supervisory requirements set out in the Recommendation shall be carried out in accordance with the provisions of the Regulation and in compliance with the prevailing data protection legislation in force.

II. Interpreting provisions

1. For the purposes of this Recommendation:

1.1 'transfer chain' shall mean the end-to-end sequence of parties, processes and interactions involved in facilitating the transfer of funds and transfer of crypto-assets, as defined in the Regulation, from the payer or originator to the payee or crypto-asset beneficiary;

1.2 'risk' shall mean the impact and likelihood of money laundering and terrorist financing occurring;

1.3 'risk-based approach' shall mean an approach whereby payment service providers, intermediary payment service providers, crypto-asset service providers and intermediary crypto-asset service providers identify, assess and interpret the money laundering and terrorist financing risks to which payment service providers, intermediary payment service providers, crypto-asset service providers and intermediary crypto-asset service providers are exposed, and take measures to combat money laundering and terrorist financing that are proportionate to those risks;

1.4 'risk factors' shall mean variables which, either on their own or in combination, may increase or decrease the risk of money laundering and terrorist financing associated with a particular business relationship, occasional transaction or transfer.

2. Unless otherwise specified, the terms used and defined in Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter referred to as 'AML Act') and in the Regulation shall also have the same meaning in this Recommendation.

III. Information requirements in relation to transfers of funds and certain crypto-asset transfers pursuant to the Regulation

III.1 General provisions

Transfers of funds and crypto-asset transfers

3. To determine what information should accompany a transfer of funds or crypto-assets, the MNB expects the Service Provider to set out in its rules and procedures how it will establish whether it acts as:

(a) the payment service provider of the payer, the payee, or an intermediary payment service provider;

(b) the crypto-asset service provider of the originator, the crypto-asset beneficiary, or as an

intermediary crypto-asset service provider.

4. The Service Provider is expected to ensure that the rules and procedures it has put in place to comply with Article 7 (1) and (2), Article 8 (1), Article 11 (1) and (2), Article 12 (1), Article 16 (1), Article 17 (1), Article 20 and Article 21 (1) of the Regulation are effective and remain effective, for example by testing a random sample from all processed transfers.

5. The MNB expects the Service Provider to keep its rules and procedures up to date and to improve them where necessary.

III.2 Exclusions from the scope of the Regulation and derogations

Transfers of funds and crypto-asset transfers

6. The MNB expects payment service providers and crypto-asset service providers to set out in their rules and procedures how they will determine whether the conditions for applying the exclusions or derogations set out in Article 2 of the Regulation are met. A payment service provider and crypto-asset service provider that is unable to determine whether these conditions are met should comply with the Regulation in respect of all transfers of funds and crypto-asset transfers.

III.2.1 Determining whether a card or instrument is used exclusively for the payment of goods or services within the meaning of Article 2 (3) (a) and (5) (b) of the Regulation

Transfers of funds and crypto-asset transfers

7. The payment service provider and the crypto-asset service provider are expected to treat the transfer of funds or crypto-assets transfer as payment for goods or services if the transfer is made from a customer (buyer) to a merchant (seller) in exchange for the purchase of goods or the provision of services. In order to determine whether a payment card or instrument is used exclusively for the payment of goods or services, the MNB requires that the following conditions be examined and that at least one of these conditions be met for a positive assessment:

a) the function of the payment card or instrument used is limited to the payment of consideration for the goods or services;

b) a merchant category code is assigned to customers, including the merchant category code for payment card schemes, which is used to categorise the type of goods or services sold;

c) regardless of the legal form of the customer, it carries out economic or professional activities, using the information collected in the course of customer due diligence, where available, or information accessible through third-party service providers or publicly available sources, in accordance with the provisions of subheading 4 of the AML Act; or

d) the analysis of trends and behaviours, including transfer history and patterns, which is performed by the payment service provider or crypto-asset service provider enables it to determine whether the payer and the originator are paying for goods or services, or whether the payee and crypto-asset beneficiary are receiving payments for goods or services.

III.2.2 Transfers which appear to be linked in relation to the threshold of EUR 1,000 referred to in Article 2 (5) (c), Article 5 (2), Article 6 (2) and Article 7 (3) to (4) of the Regulation

Transfers of funds

8. The MNB expects payment service providers to have rules and procedures in place for detecting transfers that appear to be linked.

9. The payment service provider is expected to treat as transfers which appear to be linked any transfers that

a) are carried out in the framework of one or more transactions and are sent by the same payer to the same payee within a short period of time; or

b) are sent by a payer to different payees or sent by different payers to the same payee, including cases where different accounts of the same person are used or different transactions are carried out for the same person, insofar as this information is known to the payment service provider.

10. The MNB expects payment service providers to specify the following in their internal risk assessments and internal rules:

a) what constitutes a short period of time for different types of transfers;

b) how it will identify attempts to circumvent the threshold or avoid detection; and

c) any other case which may also result in transactions that appear to be linked.

11. Based on the MNB's expectations, payment service providers should set the time frame specified in paragraph 10 *a)* in such a way that it corresponds to the money laundering and terrorist financing risk to which their business activities are exposed, based on risk assessments carried out in accordance with the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures[2] (hereinafter referred to as 'MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures').

12. The MNB expects payment service providers to determine, at the time of the transfer order or the initiation of the transfer, taking into account the absolute value of the transfer, whether the transfer can be linked to other transfers, regardless of the fees charged by the payment service provider.

III.3 Transmission and receipt of data together with the transfer[3]

III.3.1 Messaging or payment and settlement systems

Transfers of funds and crypto-asset transfers

13. The Service Provider is expected to use infrastructure and services for the transmission and reception of information that are technically capable of transmitting and receiving all information without any deficiencies or errors in the presentation of the information contained in this Recommendation.

14. The MNB expects the Service Provider to ensure that its systems are capable of maintaining data integrity, especially if the information needs to be converted into a different format before transmission or after receipt. It is expected that a Service Provider which cannot ensure that its systems are capable of transmitting, receiving or converting information without error or omissions

[2] At the time of publication of this Recommendation: MNB Recommendation 15/2022 (IX.15) on the assessment of money laundering and terrorist financing risks and the determination of related measures. https://www.mnb.hu/letoltes/15-2022-aml-cft-kockazatertekeles-ajanlas.pdf

[3] In accordance with Articles 4 to 8, 10 to 12, 14 to 17 and 19 to 21 of the Regulation

should switch to a system that is capable of doing so.

15. The Service Provider is expected to ensure the security of the systems used for information transmission. The MNB expects crypto-asset service providers to apply the MNB Recommendation on security measures relating to the operational and security risks of payment services[4] and the guidelines for payment service providers which are set out in the MNB Recommendation on the use of external service providers.[5]

Crypto-asset transfers

16. Notwithstanding paragraph 13, crypto-asset service providers and intermediary crypto-asset service providers may, on an exceptional basis until 31 July 2025, use infrastructures or services where technical limitations in relation to the completeness of data need to be compensated by additional technical steps or fixes to fully comply with the requirements set out in this Recommendation. These additional procedures should include alternative ways to collect, store and make available data that cannot be transferred, at least for technical reasons, to the receiving crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain.

17. The MNB expects that, during the transfer of data accompanying crypto-asset transfers pursuant to Article 14 of the Regulation, the originator crypto-asset service provider and the intermediary crypto-asset service provider should transmit:

a) the data as part of or incorporated into a blockchain or other distributed ledger technology (DLT) platform, or independently of it, through other communication channels, including direct communication between intermediary crypto-asset service providers, application programming interfaces (hereinafter referred to as 'APIs'), code solutions running on top of the blockchain, and other third-party solutions; and

b) the required data immediately and securely, at the latest by the time the transaction to be completed is initiated on the blockchain or other DLT.

18. When selecting the messaging or payment and settlement system(s), the crypto-asset service provider and intermediary crypto-asset service provider are expected to take proportionate, risk-sensitive measures to assess the following:

a) the ability of the system to communicate with other internal core systems and with the messaging or payment and settlement systems of the counterparty of a transfer, as well as its compatibility with other blockchain networks;

b) the reachability of the protocol (i.e. the diversity and accuracy of counterparties that can be reached using the protocol, subject to the intermediary crypto-asset service provider's own due diligence assessment, and the rate of transfers that would successfully be sent to the intended crypto-asset beneficiary or received from the originator);

c) how the system enables the crypto-asset service provider or intermediary crypto-asset service provider to detect a transfer with missing or incomplete information; and

d) the system's data integration capabilities in terms of data security and reliability.

[4] At the time of publication of this Recommendation: MNB Recommendation 26/2018. (VIII.16.) on security measures relating to the operational and security risks of payment services. https://www.mnb.hu/letoltes/26-2018-penzforgalmi-biztonsagi-intezkedesek.pdf

[5] At the time of publication 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

III.3.2 Multi-intermediation and cross-border transfers

Transfers of funds

19. In the case of a payment service provider and an intermediary payment service provider that enables cross-border transfers with two or more intermediary payment service providers or payment service providers, the MNB expects these service providers to specify in their rules and procedures how the data relating to the payer and the payee are transmitted to the next payment service provider and intermediary payment service provider in the transfer chain.

20. For transfers that have not been batched, the payment service provider or the intermediary payment service provider is expected to:

a) consider the transfer chain (from end to end) in such a manner that the flow of information on the original payer and payee is preserved;

b) where the transfer is made from a cross-border channel to a domestic channel, select the domestic system that maximises the transparency of the cross-border nature of the transfer and ensures that the information on the parties transmitted to the next payment service provider in the payment chain can be readily understood by all intermediary and/or beneficiary payment service providers; and

c) in cases of doubt, assume that the transfer is a cross-border transfer, resulting in the use of appropriate payment channels that may facilitate the necessary transmission of information.

21. Intermediary payment service providers are only responsible for passing through the payment message using the data that they have been provided with by the previous payment service provider or intermediary payment service provider in the transfer chain, subject to the specific check required by Articles 10 to 13 of the Regulation.

22. The MNB expects payment service providers and intermediary payment service providers not to treat a transfer from the payer to the payee as liquidity movement or settlement on the payment service provider’s and intermediary payment service provider’s own account.

Transfers of funds and crypto-asset transfers

23. Where the intermediary does not receive the required information related to a transfer, particularly in the case of batch transfers, the intermediary payment service provider or intermediary crypto-asset service provider should obtain the missing information via an alternative channel mechanism, including methods such as APIs and third-party solutions, to comply with the requirements set forth in the Regulation.

III.4 Information to be transmitted with the transfer[6]

Transfers of funds and crypto-asset transfers

24. Payment service providers and crypto-asset service providers should not change the initial submission, unless:

a) they are requested to do so by the intermediary payment service provider, the payee's payment service provider, the intermediary crypto-asset service provider or the crypto-asset beneficiary’s crypto-asset service provider, if the intermediary payment service provider, the payee’s payment service provider, the intermediary crypto-asset service provider or the crypto-asset beneficiary’s

[6] In accordance with Articles 4 and 14 of the Regulation

crypto-asset service provider considers that some of the information pursuant to Articles 7, 11, 19 or 20 of the Regulation is missing; or

b) following the transfer, the payer's payment service provider or the originator's crypto-asset service provider detects an error in the data they transmitted to comply with Articles 4 and 14 of the Regulation.

25. Where, on the basis of the causes described in paragraph 24, there is a change to the initial submission, the MNB expects the payer's payment service provider or the originator's crypto-asset service provider to inform the next payment service provider and crypto-asset service provider in the transfer chain and submit the correct information. The next payment service provider and crypto-asset service provider in the transfer chain should then perform, once again, the necessary tasks to detect the missing or incomplete information.

III.4.1 Providing the payment account number of the payer and the payee[7]

Transfers of funds

26. The MNB expects payment service providers to ensure that the transfer of funds is accompanied by the payment account number. Where the transfer of funds is made using a payment card, the number of that card (the primary account number) can take the place of the payment account number, on the condition that that number allows the funds transfer to be traced back to the payer or the payee.

III.4.2 Providing the name of the payer, the payee, the originator and the crypto-asset beneficiary[8]

Transfers of funds and crypto-asset transfers

27. The payment service provider of the payer or the payee, or the originator's crypto-asset service provider is expected to provide the following data:

a) for natural persons, the full names and surnames of the customer as they appear in the customer's identity document, or in the electronic identification carried out in compliance with the customer due diligence measures in sub-heading 4 of the AML Act, or, if either is unavailable for a legitimate reason, documentation in accordance with the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures. Where technical limitations exist as referred to in paragraph 16 that prevent the transmission of the customer's names and surnames, the originator's crypto-asset service provider should, as a minimum, include the first given name and last surname;

b) for legal persons, the name under which the legal person is registered. Where technical limitations exist as referred to in paragraph 16 that prevent the transmission of the full registered legal name, the originator's crypto-asset service provider should transmit the trading name. The MNB expects that the trading names used should be able to be traced back unequivocally to the legal person and match any such names recorded in official registries;

c) for transfers from a joint account, address or wallet, the names of all holders of the account, address or wallet. Where technical limitations exist as referred to in paragraph 16 that prevent the transmission of all names of all parties to the transfer, the originator's crypto-asset service provider is expected transmit the name of the holder of the account, address or wallet that is initiating the

[7] In accordance with Article 4 (1) (b) and Article 4 (2) (b) of the Regulation
[8] In accordance with Article 4 (1) (a), Article 4 (2) (a), Article 14 (1) (a) and Article 14 (2) (a) of the Regulation

transfer, or, where that is not possible, the name of the primary account, address or wallet holder.

III.4.3 Providing the address of the payer and of the originator including the name of the country, official personal document number and customer identification number or, alternatively, the date and place of birth of the payer[9]

Transfers of funds and crypto-asset transfers

28. The MNB expects the payment service provider of the payer or the payee, or the originator's crypto-asset service provider to provide the following data:

a) for natural persons, the usual place of residence of the payer or originator or, where there is no fixed residential address, the postal address at which the natural person can be reached. In the case of a vulnerable person, as referred to in the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures, who cannot reasonably be expected to provide an address in relation to their usual place of residence or, in the absence of that, their place of abode, the payment service provider or the crypto-asset service provider may use an address that is provided in documentation obtained on the basis of the alternative identification method as referred to in the above Recommendation, where such documentation contains an address and where its use is permitted under the national law of the payer;

b) for legal persons, the payer's or originator's registered or official office address.

29. The address should be provided, to the extent possible, in the following order of priority: the full country name or the abbreviation in accordance with the International Standard for country codes (ISO 3166) (alpha-2 or alpha-3), postal code, city, state, province and settlement, street name, building number or building name.

30. The MNB expects the payment service provider of the payer and the originator's crypto-asset service provider to provide the postal address as referred to in paragraph 29. Without prejudice to paragraph 17 *a)*, any alternatives to postal addresses, including post office box numbers and virtual addresses, should not be considered to meet the requirements under Article 4 (1) (c) and Article 14 (1) (d) of the Regulation.

31. The combination of the alternative information items to be provided in accordance with Article 4 (1) (c) and Article 14 (1) (d) of the Regulation should not only be based on availability but also on the set of information which best provides for unambiguous identification of the payer or originator.

32. For transfers from a joint account, address or wallet, the data of all holders of the account, address or wallet should be provided. Where the transmission of the respective information of all the parties cannot take place due to technical limitations as referred to in paragraph 16, the payer's payment service provider and originator's crypto-asset service provider should transmit the information of the holder of the account, address or wallet initiating the transfer, or, alternatively, of the primary account, address or wallet holder.

III.4.4 Providing an equivalent identifier to the legal entity identifier of the payer, the payee, the originator and the crypto-asset beneficiary[10]

Transfers of funds and crypto-asset transfers

[9] In accordance with Article 4 (1) (c) and Article 14 (1) (d) of the Regulation
[10] In accordance with Article 4 (1) (d), Article 4 (2) (c), Article 14 (1) (e) and Article 14 (2) (d) of the Regulation

33. According to the position of the MNB, the payer's payment service provider and the originator's crypto-asset service provider should consider only those official identifiers as equivalent to a legal entity identifier that

a) are a single identification code that is unique to the legal entity;

b) are published in public registries;

c) are issued upon entity formation by a public authority in the jurisdiction in which the legal entity is based;

d) allow for the identification of the name and address elements; and

e) are accompanied by a description of the type of identifier used in the messaging system.

III.5 Detecting missing information[11]

III.5.1 Procedures to detect missing information

Transfers of funds and crypto-asset transfers

34. According to the MNB, procedures as referred to in Articles 7, 11, 16 and 20 of the Regulation should at least contain the following:

a) the steps for the detection of missing, incomplete and meaningless information or inadmissible characters or inputs;

b) a combination of monitoring practices during and after the transfer commensurate with the level of money laundering and terrorist financing risk to which the transfers are exposed, determined in accordance with the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures; and

c) the criteria that help payment service providers, intermediary payment service providers, crypto-asset service providers and intermediary crypto-asset service providers to identify risk-increasing factors, as described in paragraph 44.

III.5.2 Admissible characters or inputs checks for transfers of funds[12]

Transfers of funds

35. In relation to their messaging or payment and settlement systems, the MNB expects payees' payment service providers and intermediary payment service providers to ensure that:

a) payment service providers and intermediary payment service providers understand the system's validation rules;

b) the system contains all of the fields necessary to obtain the information required in the Regulation, as specified in Chapter III.4;

c) the system prevents the sending or receipt of transfers where inadmissible characters or inputs are detected; and

d) the system flags rejected transfers for manual review and processing.

[11] In accordance with Articles 7, 11, 16 and 20 of the Regulation
[12] In accordance with Article 7 (1) and Article 11 (1) of the Regulation

36. Where a payment service provider's or intermediary payment service provider's messaging or payment and settlement system does not meet all of the criteria set out in paragraph 33, the MNB holds as a good practice for the payment service provider or intermediary payment service provider to put in place controls to mitigate the shortcomings.

37. Payees' payment service providers or intermediary payment service providers are expected to set out in their rules and procedures:

a) how they will detect whether the fields relating to the information in the messaging or payment and settlement system have been filled with characters or inputs that comply with the conventions of that system; and

b) the steps they will take where the characters or inputs are not in line with the conventions of that system.

III.5.3 Monitoring of transfers[13]

Transfers of funds and crypto-asset transfers

38. In its rules and procedures, the payees' Service Provider should set out how it will determine which transfers will be monitored during or after the transfer in accordance with Article 7 (2), Article 11 (2), Article 16 (1) and Article 20 of the Regulation. In this respect, payment service providers, intermediary payment service providers, crypto-asset service providers and intermediary crypto-asset service providers are expected to define at least the following:

a) which risk factors they will take into account in this assessment; and

b) which risk-increasing factors, or combination of risk-increasing factors, will always trigger monitoring during the transfer, and which will trigger a targeted review after the transfer has taken place.

39. The Service Provider is expected to determine the risk factors based on those set out in the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures, as well as relevant risk factors from its business-wide risk assessment, and the sectoral or national risk assessment to the extent that this is available. The risk factors should at least include:

a) transfers that exceed a predefined value threshold taking into account the average value of transfers the Service Provider routinely processes and what constitutes an unusually large transfer, based on the Service Provider's particular business model;

b) transfers where the payer, originator, payee, crypto-asset beneficiary, payer's payment service provider, originator's crypto-asset service provider, payee's payment service provider or crypto-asset beneficiary's crypto-asset service provider are located in countries or territories that are subject to restrictive measures including targeted financial sanctions, or countries or territories that present a high risk of circumvention of restrictive measures or targeted financial sanctions;

c) transfers where the payer, originator, payee, crypto-asset beneficiary, payer's payment service provider, originator's crypto-asset service provider, payee's payment service provider or crypto-asset beneficiary's crypto-asset service provider are based in a country associated with high money laundering and terrorist financing risk, including, but not limited to:

i) countries[14] identified as high risk by the European Commission in accordance with Article 9

[13] In accordance with Article 7 (2), Article 11 (2), Article 16 (1) and Article 20 of the Regulation

[14] https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/korlatozo-intezkedesek-szankciok/strategiai-hianyossagokkal-rendelkezo-kiemelt-kockazatot-jelento-harmadik-orszagok

of the Money Laundering Directive;[15] and

ii) countries which, on the basis of credible sources such as evaluations, mutual evaluations, assessment reports or published follow-up reports, have anti-money laundering and terrorist financing requirements that are not consistent with the Money Laundering Directive or the FATF[16] Recommendations, and countries that have not effectively implemented those requirements;

d) transfers where the payer's payment service provider, originator's crypto-asset service provider, intermediary payment service provider, intermediary crypto-asset service provider, payee's payment service provider or crypto-asset beneficiary's crypto-asset service provider are located in a country that, based on publicly available information, has not yet implemented the obligation to obtain, hold and transmit information on the originator and the crypto-asset beneficiary when conducting wire and virtual asset transfers;

e) transfers with entities based in a third country that does not have licensing regimes or does not regulate payment service provider activity in the case of funds transfers and crypto-asset service provider activities in the case of crypto-asset transfers;

f) transfers with self-hosted addresses;

g) transfers from or to accounts, addresses or wallets known to be linked to suspicious activity;

h) a negative anti-money laundering and terrorist financing compliance record of the prior Service Provider in the transfer chain, based on public information;

i) transfers from a Service Provider identified as repeatedly failing to provide required information without a justified reason, or from a Service Provider that has previously been known to fail to provide required information on a number of occasions without good reason, even if it did not repeatedly fail to do so;

j) use of other techniques to perform layering of transactions that hinders the tracing of crypto-assets by concealing the trail leading back to the originator, including, but not limited to:

i) funds and crypto-assets received and rapidly transferred further, thus artificially extending the transfer chain; and

ii) anonymity-enhancing techniques, products or services, including, but not limited to, mixers, Internet Protocol (IP) anonymisers and stealth addresses.

40. The MNB expects that, when considering whether or not a transfer raises suspicion, the Service Provider should take a comprehensive view of all money laundering and terrorist financing risk factors associated with the transfer and consider that missing or inadmissible information does not in its own right give rise to a suspicion of money laundering and terrorist financing.

III.5.4 Missing information checks[17]

Transfers of funds and crypto-asset transfers

41. The payee's Service Provider is expected to treat information as missing if fields are left empty, or if the information provided is meaningless or incomplete.

[15] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) 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 (hereinafter referred to as "Money Laundering Directive")
[16] Financial Action Task Force
[17] In accordance with Article 7 (2), Article 11 (2), Article 16 (1) and Article 20 of the Regulation

42. The MNB expects the payee's Service Provider to treat at least the following information as meaningless:

a) strings of random or illogical characters (such as 'xxxxx', or 'ABCDEFG');

b) use of titles (such as 'Dr.') without the person's name; and

c) other designations that are incoherent or unintelligible (such as 'An Other', or 'My Customer').

43. The MNB expects the Service Provider to use a list of terms commonly found to be meaningless, and to periodically review this list to ensure it remains relevant.

III.6 Transfers with missing or incomplete information[18]

III.6.1 Risk-based procedures for determining whether to execute, reject or suspend a transfer[19]

Transfers of funds and crypto-asset transfers

44. In its rules and procedures, the Service Provider should set out how it will determine whether to reject, suspend or execute a transfer in accordance with Article 8 (1), Article 12, Article 17 (1) and Article 21 of the Regulation. As part of this, the Service Provider should list the risk factors that it will consider for each transfer.

45. The MNB expects the Service Provider to consider in its assessment before deciding on the appropriate course of action whether or not:

a) the information allows for determination of the subjects of the transfer; and

b) one or more risk-increasing factors have been identified that may suggest that the transfer presents a high money laundering and terrorist financing risk or gives rise to suspicion of money laundering and terrorist financing.

III.6.2 Rejecting or returning a transfer[20]

Transfers of funds and crypto-asset transfers

46. Insofar as an intermediary payment service provider, payee's payment service provider, intermediary crypto-asset service provider or crypto-asset beneficiary's crypto-asset service provider decides to reject a transfer or an intermediary crypto-asset service provider or crypto-asset beneficiary's crypto-asset service provider decides to return a transfer instead of requesting the missing information, they should inform the prior service provider in the transfer chain that the transfer has been rejected or returned because of missing information.

Crypto-asset transfers

47. Insofar as the rejection is technically not possible, the transfer should be returned to the originator. If returning the transfer to the original address is not possible, the crypto-asset service provider is expected to apply alternative methods. The MNB expects the crypto-asset service provider

[18] In accordance with Articles 8, 12, 17 and 21 of the Regulation
[19] In accordance with Article 8 (1), Article 12, Article 17 (1) and Article 21 (1) of the Regulation
[20] In accordance with Article 8 (1) (a), Article 12 (a), Article 17 (1) (a) and Article 21 (1) (a) of the Regulation

to set out the alternative methods in its rules, and these should include holding the returned assets in a secure, segregated account while taking all necessary measures vis-à-vis the originator to arrange a suitable return method to the originator.

III.6.3 Requesting required information[21]

Transfers of funds and crypto-asset transfers

48. If the Service Provider requests required information that is missing, it should set a reasonable deadline by which the information should be provided. This deadline should not exceed three working days for transfers taking place within the Member States of the EEA, and five working days for transfers received from outside of the Member States of the EEA, starting from the day the Service Provider identifies the missing information. Longer deadlines of up to seven days may be set if the transfer chains involve:

a) more than two parties in the transfer flow, including intermediaries and non-banks; or

b) at least one Service Provider from a non-EEA Member State.

49. Insofar as the Service Provider decides to request the required information from the prior Service Provider in the transfer chain, it should notify the prior Service Provider in the transfer chain of the technical actions taken in relation to the transfer, due to missing or incomplete information, as applicable.

50. Any request for information or clarification is expected to be sent through the same messaging system that was used for transmitting the required information or, where technical limitations exist as referred to in paragraph 16, through secure methods of contact in line with the provisions and obligations pursuant to Regulation (EU) 2016/679.[22]

Transfers of funds

51. If the requested information is not forthcoming, the payment service provider or intermediary payment service provider should send a reminder to the prior payment service provider or intermediary payment service provider in the transfer chain and advise the prior payment service provider or intermediary payment service provider in the transfer chain of the actions it may take in the event that the payment service provider or intermediary payment service provider fails to provide the requested information by the set deadline.

52. If the requested information is not provided by the set deadline, the payment service provider or intermediary payment service provider should make the decision on whether to reject, suspend or execute the transfer in line with its risk-based rules and procedures as specified in paragraphs 44 and 45. In addition to that decision it should, irrespective of whether the failure was repeated or not, consider the future treatment of the prior payment service provider or intermediary payment service provider in the transfer chain for anti-money laundering and terrorist financing compliance purposes, including rejecting any future transfers from or to the prior payment service provider or intermediary payment service provider in the transfer chain, or restricting or terminating its business relationship with that payment service provider or intermediary payment service provider.

[21] In accordance with Article 8 (1) (b), Article 12 (1) (b), Article 17 (1) (b) and Article 21 (1) (b) of the Regulation

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Crypto-asset transfers

53. If the requested information is not forthcoming, as part of actions to be taken in accordance with Articles 17 and 21 of the Regulation, crypto-asset service providers or intermediary crypto-asset service providers should consider sending a reminder to the prior crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain and advising the prior crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain of the actions they may take in the event that the crypto-asset service provider or intermediary crypto-asset service provider fails to provide the required information before the set deadline.

54. If the requested information is not provided by the set deadline, the crypto-asset service provider or intermediary crypto-asset service provider service provider should make the decision on whether to reject, return, suspend or execute the transfer in line with its risk-based rules and procedures as specified in paragraphs 44 and 45. In addition to that decision, the crypto-asset service provider or intermediary crypto-asset service provider should, irrespective of whether the failure was repeated or not, consider the future treatment of the prior crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain for anti-money laundering and terrorist financing compliance purposes, including rejecting any future transfers from or to the prior crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain or self-hosted address, or restricting or terminating business relationship with such.

55. Requests for missing information or clarification with respect to transfers from or to self-hosted addresses should be sent directly to the crypto-asset service provider's customer.

III.6.4 Executing a transfer[23]

Transfers of funds and crypto-asset transfers

56. The MNB expects that, insofar as a Service Provider becomes aware that required information is missing, incomplete or provided using inadmissible characters during the transfer and executes the transfer, it should document the reason for executing the transfer and, in line with its risk-based rules and procedures, consider the future treatment of the prior Service Provider or self-hosted address in the transfer chain for anti-money laundering and terrorist financing compliance purposes. However, where the payer, payee, originator or crypto-asset beneficiary cannot be unambiguously identified due to missing or incomplete information, or information provided using inadmissible characters, the Service Provider is expected not to execute the transfer.

III.6.5 Detecting missing or incomplete information after executing a transfer[24]

Transfers of funds

57. Where a payment service provider or intermediary payment service provider detects ex post that the required information was missing, incomplete or provided using inadmissible characters, it should ask the prior payment service provider or intermediary payment service provider in the transfer chain to provide the missing information, or to provide that information using admissible characters or inputs, applying Chapter III.6.3.

Crypto-asset transfers

[23] In accordance with Article 8 (1), Article 12 (1), Article 17 (1) and Article 21 (1) of the Regulation
[24] In accordance with Article 8 (1), Article 12 (1), Article 17 (1) and Article 21 (1) of the Regulation

58. Where a crypto-asset service provider or intermediary crypto-asset service provider executes the transfer and detects ex post that the required information is missing or incomplete, it should ask the prior crypto-asset service provider or intermediary crypto-asset service provider in the transfer chain to provide the missing information, applying Chapter III.6.3.

III.7 Repeated failure by a Service Provider[25]

III.7.1 Treatment of repeated failure by a Service Provider

Transfers of funds and crypto-asset transfers

59. In accordance with Article 8 (2), Article 12 (2), Article 17 (2) and Article 21 (2) of the Regulation, the MNB expects that Service Providers set out in their rules and procedures the quantitative and qualitative criteria they will use to determine whether a specific Service Provider has committed *'repeated failures'* and to document all transfers with missing or incomplete information.

60. The MNB expects quantitative criteria to include at least:

a) the percentage of transfers with missing or incomplete information sent by a specific Service Provider within a specific time frame; and

b) the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline.

61. Qualitative criteria are expected to include at least:

a) the level of cooperation of the requested Service Provider relating to previous requests for missing information;

b) the existence of an agreement with the Service Provider requiring more time to provide the information; and

c) the type of information missing or incomplete and the reason given by the Service Provider for not providing the information.

62. The warning in accordance with Article 8 (2) (a), Article 12 (2) (a), Article 17 (2) (a) and Article 21 (2) (a) of the Regulation should – in addition to setting a deadline – inform the prior Service Provider in the transfer chain of the steps that will be applied by the Service Provider, in the event that the former continues to fail to provide the required information.

63. The Service Provider should consider issuing a further warning to the prior Service Provider in the transfer chain that any future transfers will be rejected.

64. The MNB expects the Service Provider to consider how repeated failure by the prior Service Provider in the transfer chain to provide information and that Service Provider's attitude to responding to such requests affects the money laundering and terrorist financing risk associated with that Service Provider, and, where appropriate, the Service Provider should carry out real-time monitoring of all transactions received from it.

65. Before taking the decision to terminate a business relationship, in particular where the prior Service Provider in the transfer chain is a respondent counterparty from a third country, the Service Provider should consider whether or not the risk can be managed in other ways, including ex ante by the application of enhanced due diligence measures.

[25] In accordance with Article 8 (2), Article 12 (2), Article 17 (2) and Article 21 (2) of the Regulation

III.7.2 Reporting repeated failure by a Service Provider to the competent authority[26]

Transfers of funds and crypto-asset transfers

66. The report is expected to be submitted to the MNB by the Service Provider without undue delay, and no later than three months after identifying the repeated failure by the Service Provider. Reporting should take place regardless of the reasons given by the Service Provider committing *'repeated failures*', if any, to justify that breach, or their registration in or outside an EEA Member State.

67. The report should include:

a) the name of the Service Provider identified as committing repeated failures to provide the required information;

b) the country in which the Service Provider is authorised;

c) the nature of the breach, including:

i) the frequency of transfers with missing information;

ii) the period of time during which the breaches were identified; and any reasons the Service Provider may have given to justify its repeated failure to provide the required information;

d) details of the steps the reporting Service Provider took.

68. The reporting obligation detailed in the previous paragraph does not affect the reporting obligation to be fulfilled to the financial information unit pursuant to Sections 30 to 31 of the AML Act.

III.8 Transfers of crypto-assets made from or to self-hosted addresses[27]

III.8.1 Individually identifying transfers made from or to self-hosted addresses

69. The MNB expects crypto-asset service providers and intermediary crypto-asset service providers to consider a transfer of a crypto-asset as individually identified when:

a) a unique identifier for each transfer is used, such as a transfer hash or a reference number; or

b) additional information is included in the transfer to help identify the transfer.

III.8.2 Identification of a transfer made from or to a self-hosted address

70. To determine whether or not a self-hosted address is used on the other end of a transfer, the originator's crypto-asset service provider and the crypto-asset beneficiary's crypto-asset service provider should rely on available technical means including but not limited to blockchain analytics, third-party data providers and identifiers used by messaging systems.

71. If the information specified in paragraph 70 cannot be retrieved via technical means, the originator's crypto-asset service provider and the crypto-asset beneficiary's crypto-asset service provider should obtain that information directly from its customer. In this case, if the originator's crypto-asset service provider and the crypto-asset beneficiary's crypto-asset service provider establish that the transfer is made to or from another crypto-asset service provider, it is expected that the originator's crypto-asset service provider and the crypto-asset beneficiary's crypto-asset service

[26] In accordance with Article 8 (2), Article 12 (2), Article 17 (2) and Article 21 (2) of the Regulation
[27] In accordance with Article 14 (5) and Article 16 (2) of the Regulation

provider take the necessary steps to accurately identify the counterparty crypto-asset service provider.

72. The originator's crypto-asset service provider should undertake this assessment before the transfer is initiated and the information is transmitted in accordance with Article 14 (5) of the Regulation. The crypto-asset beneficiary's crypto-asset service provider should undertake this assessment before the crypto-assets are made available to the crypto-asset beneficiary in accordance with Article 16 (2) of the Regulation.

III.8.3 Identification of the originator and the crypto-asset beneficiary in a transfer made from or to a self-hosted address

73. Insofar as a self-hosted address is used on the other end of the transfer, the MNB expects crypto-asset service providers to obtain the information on the originator or crypto-asset beneficiary from their customer.

III.8.4 Transfers above EUR 1,000 and proof of ownership or control of a self-hosted address

74. Crypto-asset providers are expected to determine whether a transfer involving a self-hosted address amounts to or exceeds EUR 1,000:

a) at the moment the transfer was ordered or initiated, in the case of the originator's crypto-asset service provider; or

b) at the time of the receipt, in the case of the crypto-asset beneficiary's crypto-asset service provider.

75. To determine whether the value of transfers made from or to self-hosted addresses is above EUR 1,000, the MNB expects crypto-asset service providers to use the exchange rate of the crypto-asset being transferred to determine its value in euros at the time of the transfer, and regardless of any transaction fees.

76. In order to assess whether the self-hosted address is owned or controlled by the originator or crypto-asset beneficiary, respectively, crypto-asset service providers should use at least one of the following verification methods:

a) indirect electronic customer due diligence performed by means of an audited electronic communication device specified in the MNB Decree[28] (hereinafter referred to as 'Customer due diligence decree'), displaying the address;

b) direct electronic customer due diligence carried out by means of an audited electronic communication device as specified in the Customer due diligence decree;

c) sending an amount predetermined by the crypto-asset service provider – preferably the smallest denomination of the crypto-asset – from the self-hosted address to the crypto-asset service provider's account;

d) requesting the customer to digitally sign a given message in the account and wallet software using the key corresponding to the given address;

e) other suitable technical means as long as they allow for reliable and secure assessment and the

[28] MNB Decree 29/2024 (VI. 24.) on the detailed rules of the audited electronic communications devices, and the minimum requirements for their operation, internal regulation, the method of auditing, and the implementation of the electronic customer due diligence process by means of such devices used by the service providers supervised by the Magyar Nemzeti Bank

crypto-asset service provider is fully satisfied that it knows who owns or controls the address.

77. The MNB holds as a good practice when the decision on which method(s) to choose depends on:

a) the technical capabilities of the self-hosted address;

b) the robustness of the assessment each method can deliver; and

c) the money laundering and terrorist financing risk.

78. Where one method on its own is not sufficiently reliable to reasonably ascertain the ownership or control of a self-hosted address, the crypto-asset service provider should use a combination of methods.

79. Insofar as the crypto-asset service provider is fully satisfied that the self-hosted address is owned or controlled by its customer, the crypto-asset service provider should document this in its systems and may not need to re-apply the measures above to subsequent transactions from/to the same address ('whitelisting'). A crypto-asset service provider making use of whitelisting should have controls in place to identify changes in the money laundering terrorist financing risk of the self-hosted address and its ownership or control. If the crypto-asset service provider establishes that the money laundering terrorist financing risk of the self-hosted address has changed or that there are indications that its customer no longer owns or controls the self-hosted address, it should remove this address from its whitelist.

III.8.5 Mitigating measures to put in place regarding transfers made from or to a self-hosted address

80. The MNB expects crypto-asset service providers to assess the risk associated with transfers made from or to a self-hosted address as set out in Chapter III.5.3 and in accordance with the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures, using all of the information related to originators and crypto-asset beneficiaries, patterns and geographies, and information from regulators, law enforcement and third parties.

81. The MNB expects crypto-asset service providers to apply at least one of the risk-mitigating measures as defined in Section 26 of the MNB Decree on Money laundering[29] that are commensurate with the risks identified including where the crypto-asset service provider:

a) is or becomes aware that the information on the originator or crypto-asset beneficiary using the self-hosted address is inaccurate; or

b) encounters unusual or suspicious patterns of transactions or situations of higher money laundering and terrorist financing risk associated with transfers involving self-hosted addresses, in accordance with the MNB Recommendation on the assessment of money laundering and terrorist financing risks and the determination of related measures.

82. Where, as a result of the assessment in Chapter III.8.4, it is established that the self-hosted address is owned or controlled by a third person instead of the crypto-asset service provider's customer, the MNB expects that the verification referred to in the MNB Decree on money laundering is deemed to have taken place if:

[29] MNB Decree 14/2025 (VI. 16.) on the detailed rules for the implementation of certain obligations of the service providers supervised by the Magyar Nemzeti Bank pursuant to the Act on Preventing and Combating Money Laundering and Terrorist Financing, and on the minimum requirements for the development and operation of a screening system of such service providers pursuant to the Act on the Implementation of Financial and Asset-related Restriction Measures ordered by the European Union and the UN Security Council (MNB Decree on money laundering)

a) the crypto-asset service provider collects additional data from other sources to verify the submitted information, including but not limited to blockchain analytical data, third-party data, recognised authorities' data and publicly available information, as long as these are reliable and independent; or

b) the crypto-asset service provider uses other suitable means as long as the crypto-asset service provider is fully satisfied that it knows the identity of the originator or crypto-asset beneficiary and can demonstrate this to its competent authority.

83. Insofar as such transfers raise suspicions of money laundering and terrorist financing, crypto-asset service providers are expected by the MNB to report that to the financial information unit in accordance with the provisions of sub-heading 11 of the AML Act.

III.9 Obligations of the payer's payment service provider, the payee's payment service provider and the intermediary payment service provider insofar as a transfer is a direct debit

Transfers of funds

84. Where a transfer of funds is a direct debit, the payee's payment service provider should send the required information on the payer and on the payee to the payer's payment service provider as part of the direct debit collection. Upon receipt of this information by the payer's payment service provider, the payee's payment service provider and the intermediary payment service provider may consider the information requirements in Article 4 (2) and (4) and Article 5 (1) to (2) of the Regulation to have been satisfied.

85. For the purposes of paragraph 84:

a) the obligations set out in Articles 4, 5 and 6 of the Regulation should be applied to the payee's payment service provider;

b) verification pursuant to Article 4 (4) of the Regulation should be performed by the payee's payment service provider on the information of the payee, before sending the direct debit collection;

c) the obligations set out in Articles 7, 8 and 9 of the Regulation should be applied to the payer's payment service provider (debtor payment service provider);

d) verification pursuant to Article 7 (3) to (4) of the Regulation should be performed by the payer's payment service provider (debtor PSP) on the information of the payer before debiting the payer's account.

86. Insofar as the payer's payment service provider becomes aware, when receiving the direct debit collections, that the information referred to in Articles 4, 5 and 6 of the Regulation is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7 (1) of the Regulation, the payer's payment service provider is expected to apply the options set out in Article 8 (1), second subparagraph of the Regulation. The payer's payment service provider should choose to request the required information on the payer and the payee before or after debiting the payer's account, in a risk-based approach. In particular, it should assess whether the payment should still be credited where information is missing or whether funds should be made available to the payee relying on the information obtained from the payer and verified as part of the customer's due diligence process, in accordance with Chapter III.4.

87. The payer's payment service provider should leverage available communication channels to engage with any payee's payment service provider committing repeated failures, prior to taking

further actions to restrict or reject payments. Where payment service providers rely on information obtained prior to the transactions, their rules and procedures should take into consideration possible changes to information over time, in particular including name and address.

IV. Closing provisions

88. 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 for 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.

89. 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.

90. 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 wishes 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.

91. The MNB expects the Service Providers concerned to apply this Recommendation from 1 July 2025.

92. On 30 June 2025, MNB Recommendation 1/2020 (III.4.) on procedures for the handling of transfers of funds with missing data by payment service providers shall be repealed.