MNB Decree 14/2025 (VI. 16.)

on the detailed rules for the implementation of certain obligations of 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 Restrictive Measures ordered by the European Union and the UN Security Council

[1] The purpose of this Decree is to define the detailed rules for the implementation of certain obligations of service providers supervised by the Magyar Nemzeti Bank pursuant to the Act on Preventing and Combating Money Laundering and Terrorist Financing as well as 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 Restrictive Measures ordered by the European Union and the UN Security Council.

[2] Pursuant to the authorisation granted under Section 77 (3) *a)* to *c)* and *e)* to *l)* of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing,

in respect of sub-heading 9, pursuant to the authorisation granted by Section 17 (3) 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,

and acting within the scope of my duties specified in Section 4 (9) of Act CXXXIX of 2013 on the Magyar Nemzeti Bank, I hereby issue the following Decree:

CHAPTER I

GENERAL PROVISIONS

Section 1 With the exception specified in paragraph (2), the scope of this Decree shall apply to service providers within the meaning of Section 1 (1) *a)* to *e)* and *m)* and paragraph (1a) of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (hereinafter referred to as 'AML Act') (hereinafter jointly referred to as 'service provider').

(2) Sub-heading 9 of this Decree shall not cover service providers providing account information services exclusively pursuant to Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises.

Section 2 For the purposes of this Decree:

1. *'channel'* shall mean an electronic technical device – in particular a mobile telephone, computer, tablet – or intermediary, used for administration purposes at other than the premises where the service provider conducts its activities on a permanent basis,

2. *'inherent risk'* shall mean the level of risk before risk mitigation,

3. *'cash transaction'* shall mean cash payment to a customer and cash payment by a customer regardless of currency,

4. *'risk profile'* shall mean the general nature of the risk remaining after the mitigation of

identified money laundering and terrorist financing risks, including the type and level of risk,

5. *'threshold'* shall mean the cumulative limit of the amount that can be achieved through transactions conducted in the course of a business relationship, determined by the service provider on a risk-sensitive basis,

6. *'enhanced procedure'* shall mean enhanced monitoring involving a combination of risk-based measures to address the risk inherent in the customer, service, product, transaction, instrument used or geographical exposure,

7. *'monitoring'* shall mean the ongoing monitoring of the business relationship and the customer who regularly places orders,

8 '*payment service provider'* shall have the meaning defined in Section 2 item 22 of Act LXXXV of 2009 on the Provision of Payment Services,

9. *'money laundering and terrorist financing risk'* shall mean the likelihood and the likely effects of the occurrence of money laundering or terrorist financing,

10 '*self-hosted address'* shall mean the distributed ledger address specified in Article 3 (20) of Regulation (EU) 2023/1113 of the European Parliament and of the Council,

11. *'unusual transaction'* shall mean a transaction,

a) which is not consistent with the generally followed procedures for the service or product,

b) which has no clear economic purpose or legal basis, or

c) where there is an unjustified change in the frequency or size of transactions compared to the customer's previous activities,

12. *'management body'* shall mean the body of a service provider with a management function or a supervisory function.

CHAPTER II

SPECIFIC RULES ON CUSTOMER DUE DILIGENCE AND VERIFICATION OF THE IDENTITY OF THE BENEFICIAL OWNER

1. Measures to be taken to understand and establish the identity of the beneficial owner and the ownership and control structure of the customer

Section 3 In order to fulfil the obligation provided for in Section 8 (4) and Section 9 (1) and (1a) of the AML Act, the service provider shall take reasonable measures to understand the ownership and control structure of the customer, which are sufficient to enable the service provider to ensure that it has a clear understanding of the risk associated with the different levels of ownership and effective control of the customer and to determine the identity of the beneficial owners.

Section 4 (1) In order to determine the beneficial owner, the service provider shall, in accordance with the provisions of Section 3 (38) of the AML Act and taking into account the information made public by the Magyar Nemzeti Bank (hereinafter referred to as 'MNB'), examine whether there are any persons who otherwise exercise effective control over a customer which is a legal person or an unincorporated business association. To this end, in particular the service provider shall take into account:

a) control without direct ownership concerning the customer through a family relationship or contractual relationships,

b) the access to, use of or benefits from assets owned by the customer, and

c) responsibility for strategic decisions affecting the customer's business practices or operations.

(2) The service provider shall set out in its internal policy the method used to establish the identity of the beneficial owner.

(3) The service provider may base its determination of the ownership and control structure of the customer solely on the customer's statement if the customer is a low-risk customer and the service provider has no doubt as to the veracity of the statement, taking into account all of the circumstances. In all other cases, the service provider shall apply measures proportionate to the level of risk involved, based on a risk-sensitive approach, in order to identify the ownership and control structure of the customer.

Section 5 The service provider shall check the beneficial ownership register of the legal person customer on a risk-sensitive basis, if the data contained in the register are available to the service provider. In addition to assessing the data in the beneficial ownership register on a risk-sensitive basis for a legal person customer, the service provider shall obtain additional data if the business relationship is associated with a higher risk or if the service provider has doubts as to whether the person in the register is the beneficial owner.

Section 6 (1) The service provider may record the executive officer named by the customer as the beneficial owner of the customer only if it has exhausted all of the means possible in the given situation to identify the natural person who holds a share of ownership, voting rights or a dominant influence in respect of the customer pursuant to Section 3 (38) *a)* or *b)* of the AML Act, or who otherwise exercises effective control over the customer.

(2) In the case referred to in paragraph (1), the service provider shall record in its records, in a retrievable manner, the reason why the executive officer named by the customer was recorded as the beneficial owner of the customer.

Section 7 If there is doubt as to the identity of the beneficial owner, the service provider shall apply the following measures in respect of the beneficial owner named by the customer:

a) verification of the identity of the beneficial owner, and

b) a customer due diligence interview, documented in a retrievable manner and to be retained in accordance with Sections 56–58 of the AML Act, in order to verify the purpose and nature of the business relationship and the real economic link of the beneficial owner,

ba) with the customer,

bb) if the beneficial owner cooperates, on a risk-sensitive basis, with the beneficial owner as well.

Section 8 If, as a result of the measures carried out within the framework of customer due diligence, the service provider is unable to ascertain the ownership and control structure of the customer, and thus the identity of the beneficial owner, it shall proceed in accordance with the provisions of Section 13 (8) of the AML Act.

Section 9 The service provider shall document the risks incurred in relation to the customer and the results of the measures taken in respect of such risks in a retrievable manner and shall retain such records in accordance with Sections 56–58 of the AML Act. To this end, the service provider shall keep records that clearly show beyond doubt the source of the data relating to the customer and how the service provider verified them.

Section 10 In its internal policy pursuant to Section 65 (1) of the AML Act, the service provider shall set out the manner and the legal basis for accessing its records kept in connection with the measures to be taken to understand and determine the identity of the beneficial owner and the

ownership and control structure of the customer.

Section 11 The crypto-asset service provider shall verify that the self-hosted address is owned by the originator or beneficiary of the crypto-asset transfer or that it exercises ultimate control or oversight over it in any other way. For verification purposes, the crypto-asset service provider shall apply at least one of the following measures:

a) indirect electronic customer due diligence performed via an audited electronic means of communication as regulated in MNB Decree 29/2024 (VI. 24.) on the detailed rules for audited electronic means of communication and their operation, the minimum requirements for their internal regulation, the mode of their audit and the implementation of electronic customer due diligence performed by way of such means, used by service providers supervised by the Magyar Nemzeti Bank, indicating this title,

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

c) sending a predetermined amount – if possible 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, or

e) the use of reliable and secure technical means that enable the crypto-asset service provider to verify that the address is actually owned or under the ultimate control of the originator or the beneficiary.

2. Cases for enhanced customer due diligence and the threshold and time limit for simplified customer due diligence

Section 12 (1) The service provider shall apply enhanced customer due diligence in addition to that provided for in the AML Act at least in cases where its customer,

a) based on the service provider's internal risk assessment,

aa) is a non-profit organisation with a high risk of terrorist financing,

ab) is an organisation posing a high proliferation financing risk,

ac) is an organisation which is particularly significant for its operations in terms of cash distribution,

ad) is an organisation closely linked to a high geographical risk area,

b) is a legal person or unincorporated business association, the beneficial owner of which is from a high-risk third country with strategic deficiencies,

c) is a public limited liability company which holds bearer shares or whose shareholder is represented by a proxy,

d) is a legal person or unincorporated business association whose ownership and control structure appears to be unusual or excessively complex in relation to the nature of the business activity of the legal person or unincorporated business association, or

e) has a beneficial owner who does not cooperate in the customer due diligence interview referred to in Section 7 *b) bb)*.

(2) The provisions of paragraph (1) *d)* shall not apply if the service provider is of the opinion that the overly complex ownership structure of the legal person or unincorporated business association

is justified and this is supported by a detailed assessment of risk-mitigating and risk-enhancing factors in the service provider's internal risk assessment, or the customer's classification pursuant to Section 6/A of the AML Act is low risk.

Section 13 (1) The service provider may apply simplified customer due diligence if the customer's classification pursuant to Section 6/A of the AML Act is low risk.

(2) In the event of the application of simplified customer due diligence, the service provider shall set out in its internal risk assessment the reasonable threshold and time limit at which the measures specified in Section 15 (1b) of the AML Act are to be implemented.

(3) The determination of the threshold and the time limit of the measure shall be deemed reasonable if the implementation of the measures specified in Section 15 (1b) of the AML Act at a time other than the establishment of the customer relationship does not increase the risk of money laundering or terrorist financing and no data, facts or circumstances indicating money laundering or terrorist financing have been established.

(4) It is not necessary to set a threshold in the internal risk assessment for cases where, due to the persistently low risk of money laundering, measures are taken only in the course of fulfilling the verification obligations set out in Section 12 (1) and (2) of the AML Act.

CHAPTER III

SERVICE PROVIDER'S MEASURES TO BE TAKEN BASED ON THE CUSTOMER'S SPECIFIC RISK CLASSIFICATION

3.[1]

Sections 14 to 16[2]

4. Cases requiring a decision by the designated accountable manager to enter into a business relationship or to execute a transaction order under the risk-sensitive approach and the detailed rules for taking such decisions

Section 17 (1) In addition to the provisions of the AML Act, the designated accountable manager of the service provider shall decide at least in the following cases:

a) the establishment of a business relationship, if there are data, facts or circumstances indicating that the service is not actually used by the person who is indicated as the customer in the application for the conclusion of the contract,

b) the establishment of a private banking business relationship,

c) in relation to business practices related to the service or product provided by the service provider or new business practices, including new distribution solutions and the introduction of new or emerging technologies,

d) the establishment of a business relationship in the event of a significant risk of money laundering and terrorist financing resulting from evaluation of the customer due diligence questionnaire, in particular if the customer indicates cash transactions of HUF 100 million or more

[1] In force: 1 July 2025

[2] In force: 1 July 2025

per year in the questionnaire,

e) the establishment of a business relationship with a trustee or a customer engaged in a similar activity, and

f) the establishment of a business relationship, if the customer indicates the address of a domiciliation service provider as its registered office.

(2) The designated accountable manager of the service provider shall, in the cases specified in paragraph (1), take decisions in a documented form which ensures consistency, ongoing monitoring and verifiability.

Section 18 (1) On the basis of a risk-sensitive approach, the service provider may provide in its policy pursuant to Section 65 of the AML Act for the rules on the delegation of all or part of the cases specified in Section 10 (3), Section 14/A (4), Section 16 (2) a), and Section 16/A (1) b) of the AML Act, as well as in Section 17 of this Decree, requiring the decision of the designated accountable manager for the establishment of a business relationship or the execution of a transaction order, which may either be permanent delegation or delegation providing for the case-by-case substitution of the designated accountable manager.

(2) The service provider may delegate the decision-making powers pursuant to paragraph (1) in its policy pursuant to Section 65 of the AML Act only to a manager who has the professional knowledge required for the decision. In establishing the rules on delegation, the service provider shall also specify the criteria to be taken into account when considering the delegation of certain decision-making powers.

5. Cases and conditions of the enhanced procedure

Section 19 (1) The service provider shall, in addition to provisions set forth in the AML Act, use the enhanced procedure at least in the following cases:

a) in respect of the customer affected by the conversion of a non-registered savings deposit into a registered savings deposit pursuant to the Decree-Law on Savings Deposits, if the total value of the savings deposits to be converted into registered savings deposits reaches HUF 4.5 million, for one year from the date of the conversion,

b) if the customer is subject to due diligence by the service provider due to currency exchange amounting to or exceeding HUF 20 million, for a period of one year from the last currency exchange amounting to or exceeding HUF 20 million,

c) if a customer who regularly gives transaction orders is subject to due diligence by the service provider for a transaction order amounting to or exceeding HUF 50 million, for one year from the last transaction amounting to or exceeding HUF 50 million,

d) if the customer's cash turnover – i.e. the sum of its deposits and withdrawals – reaches or exceeds HUF 100 million per month, for one year after the last month with a cash turnover reaching or exceeding HUF 100 million,

e) if an STR report pursuant to Section 30 (1) of the AML Act has been made in relation to the customer of the service provider by the service provider or within the group to which the service provider belongs, for one year from the last report,

f) a non-Hungarian citizen natural person who has a permit or residence registration entitling to stay in Hungary for more than 90 days and who does not have a domicile or residence in Hungary, residing or staying outside the European Union,

g) if the service provider receives a notification from a correspondent bank or a public authority

in relation to a customer which, in the service provider's assessment, indicates an increased risk of money laundering associated with the customer, for a period of one year from the receipt of the notification,

h) if the service provider's customer has designated a domiciliation service provider as their registered office and has transferred money outside Hungary within three months of the establishment of the customer relationship, for one year from the date of the transfer, and

i) if the service provider's customer is a private investment fund whose ownership and management structure has not yet been disclosed, and the service provider has not yet determined the beneficial owner of the private investment fund customer pursuant to Section 3 (38) *g)* of the AML Act.

(2) The service provider shall record in its internal risk assessment any cases of enhanced procedures other than those specified in paragraph (1).

(3) A service provider may waive the enhanced procedure for a group of customers which it has identified, if it justifies this in its internal risk assessment in detail, in the cases referred to in paragraph (1), by a combined assessment of risk-mitigating and risk-enhancing factors.

Section 20 (1) The service provider shall screen, analyse and assess the transactions identified in the internal risk assessment for money laundering and terrorist financing for customers subject to the enhanced procedure in accordance with the provisions of Sections 35–42 on a risk basis, but in any case within 30 working days.

(2) In the risk assessment provided for in paragraph (1), the service provider shall also apply an aggregated limit per transaction and for several transactions over a given period to customers subject to the enhanced procedure.

(3) The limit set in the internal risk assessment shall be determined by the service provider on a risk basis, per transaction, by means of a combined assessment of risk-mitigating and risk-enhancing factors.

(4) In the case of a customer subject to the enhanced procedure, the service provider shall, after the condition giving rise to the enhanced procedure has been met, in respect of the customer's money laundering risk transactions

a) obtain information on the source of funds without delay and require the production of documents relating to the source of funds in order to verify this information,

b) verify whether any negative information has emerged from credible and reliable public sources concerning the customer or its significant counterparties, and

c) examine whether its customer's business activity is economically rational.

CHAPTER IV

SPECIFIC RULES ON PREVENTING AND COMBATING MONEY LAUNDERING AND TERRORIST FINANCING AND ON THE IMPLEMENTATION OF FINANICAL AND ASSET-RELATED RESTRICTIVE MEASURES ORDERED BY THE EUROPEAN UNION AND THE UN SECURITY COUNCIL

6. Rules for the preparation of an internal risk assessment

Section 21 (1) Within the framework of the internal risk assessment, the service provider shall, in respect of the known risks, identify those which have an impact on its money laundering and terrorist financing risks.

(2) Within the framework of the internal risk assessment, the service provider shall also perform an assessment of the risks at the individual customer level and for the activities of each of its business lines. The service provider shall also incorporate the risk assessment for business activities into the methodology for individual customer level risk assessments.

(3) In fulfilling its obligation specified in paragraph (1), the service provider shall determine the type and number of sources of information and the systems and control mechanisms to be implemented on a risk-sensitive basis, also taking into account the nature and complexity of its business.

(4) If the service provider is a member of a group that develops a group-level risk assessment, it shall consider whether the group-level risk assessment is sufficiently detailed and specific to reflect the service provider's business activities and the risks to which the service provider is exposed and, if necessary, supplement the group-level risk assessment on the basis of its internal risk assessment. If the parent company of the group is established in a third country with strategic deficiencies and a high risk, the service provider shall take this into account in its risk assessment even if it is not mentioned in the group-level risk assessment.

Section 22 (1) In order to identify the risk of money laundering and terrorist financing, the service provider shall use information from various sources, which may be accessed individually or through tools or databases aggregating information from several sources.

(2) In addition to information contained in the databases, the service provider may, when identifying money laundering and terrorist financing risk factors, take into account information from the following sources:

a) from civil society,

b) from an assessment of the adequacy and effectiveness of a third country's anti-money laundering and anti-terrorist financing system, of its anti-corruption and tax regimes,

c) from a credible and reliable public source,

d) from scientific and higher education institutions,

e) from professional self-regulatory organisations, and

f) from credible and reliable commercial organisations.

Section 23 (1) The service provider shall ensure that it has systems and control mechanisms in place to identify emerging money laundering and terrorist financing risks and to assess and, where appropriate, incorporate these risks in a timely manner into its business-wide and individual risk assessments.

(2) The systems and control mechanisms to be implemented by the service provider to identify emerging risks shall include at least the following:

a) procedures to ensure that information obtained in the course of the internal business operations of the service provider is regularly reviewed to identify trends and emerging risks, both in relation to individual business relationships and the service provider's business line activities,

b) procedures to ensure that the service provider regularly checks the relevant sources of information, including the sources of information referred to in Section 21, for both individual customer-level and business-wide risk assessments, including taking the necessary action on the basis of those sources,

ba) in respect of individual risk assessments at the customer level:

1. terrorism alerts and financial sanctions regimes and any changes thereunto immediately following the publication of such, and

2. media reports relevant to the sectors or jurisdictions in which the service operates,

bb) in respect of risk assessments covering business line activities:

1. law enforcement alerts and reports,

2. thematic assessments issued by the competent authorities, and

3. the procedures for collecting and reviewing information on risks, in particular new categories of customers, countries or geographical areas, new services and products, new tools used, new compliance systems and new control mechanisms, and

c) information obtained through cooperation with other representatives of the service provider's sector and with the competent authorities, and procedures for providing feedback to the service provider's employees on a finding.

Section 24 When identifying the risk factors of its business activities and determining the measures necessary for risk management, in addition to the provisions of Section 27 of the AML Act, the service provider shall also take into account the following:

a) the European Commission's supranational risk assessment,

b) the views of the European Supervisory Authorities on money laundering and terrorist financing risks affecting the EU financial sector,

c) the guidelines issued by the European Banking Authority or the Authority for Anti-Money Laundering and Countering the Financing of Terrorism, which are also addressed to the service provider,

d) recommendations issued by the MNB,

e) information made public by the MNB,

f) decisions taken and made public in the course of proceedings conducted by the MNB,

g) the European Commission's list of high-risk third countries,

h) the national risk assessment approved by the Government of Hungary,

i) the justification for legislation on money laundering and terrorist financing,

j) information from financial intelligence units and law enforcement authorities,

k) information obtained through the initial customer due diligence procedure and ongoing customer monitoring,

l) the nature and complexity of the services, products, activities and transactions it offers,

m) the solution it uses, including the free provision of services, the use of an agent or intermediary,

n) the types of customers served, and

o) the geographical areas of the business activity, in particular if it is conducted in a high-risk third country with strategic deficiencies or the country of origin of a significant proportion of its customers is a strategically deficient high-risk third country.

Section 25 (1) The service provider shall develop a comprehensive view of the money laundering and terrorist financing risk factors it has identified, which shall be taken together to determine the

level of money laundering and terrorist financing risk at the business line level and the customer level.

(2) In its risk assessment, the service provider shall take into account the inherent risks and the risk mitigation measures it has identified and shall categorise its business lines, business relationships and transaction orders in its internal risk assessment on the basis of the resulting level of money laundering and terrorist financing risk.

(3) The service provider shall classify risks into at least low, medium and high risk categories.

(4) The service provider shall classify the risks defined in accordance with paragraph (3) into at least customer, services, products, instrument used and geographical risk groups at the business line level and the customer level. The risk assessments of the service provider's business lines jointly form the basis of the service provider's individual customer-level risk assessment. The risk assessment performed at the business line level does not need to be repeated at the customer level; it is sufficient to refer to the business risk associated with the customer, if no other individual customer factors are taken into account for this by the service provider at the customer level.

(5) The service provider may weight the risk and its mitigating factors differently according to the relative importance of the risk factor for each business line.

(6) When weighting risk factors, the service provider shall ensure that:

a) the weighting is not unduly influenced by a single factor,

b) considerations based on business aspects do not influence the risk rating,

c) the weighting does not lead to a situation where no business relationship can be classified as high risk,

d) the risk classification of customers is recorded in the IT system and, depending on the risk assessment and the size of the service provider, its up-to-date status is supported by automated IT solutions built into the system,

e) the provisions relating to situations of high money laundering risk, as defined in the legislation, may not be overridden by the weighting of the service provider,

f) the service provider's risk assessment is not based exclusively on automatic mechanisms, and the service provider is able to override automatically determined risk values if necessary, and

g) the decision to override the risk values established in the risk assessment and the justification for it are recorded in a retrievable manner.

(7) The service provider shall determine, on a risk-sensitive basis, the frequency of the overall review of the methodology used for its internal risk assessment.

Section 26 (1) The service provider shall determine in its internal policy pursuant to Section 65 (1) of the AML Act, following the assessment of the identified risk, in proportion to the extent of the risk at the customer level, what measures are necessary to address the identified risks. The service provider shall also consider the related recommendations of the MNB when conducting individual customer-level risk assessments.

(2) The internal risk assessment report, including the business line and customer-level risk assessment, shall be approved by the body performing the control function of the service provider or, in its absence, by its executive officer.

Section 27 (1) The crypto-asset service provider shall identify and assess the money laundering and terrorist financing risks associated with crypto-asset transfers to or from self-hosted addresses, and shall include the identified risks in its risk assessment and the measures taken to mitigate and manage those risks in its internal procedures.

(2) The crypto-asset service provider shall apply risk mitigation measures commensurate with the identified risks associated with crypto-asset transfers to or from self-hosted addresses, including at least one of the following:

a) taking risk-based measures to identify and verify the identity of the originator or crypto-asset beneficiary of crypto-asset transfers to or from self-hosted addresses, or the beneficial owner of such originator or crypto-asset payee, including by relying on third parties,

b) requiring the provision of additional information on the origin and destination of the transferred crypto-assets,

c) monitoring the transactions in enhanced procedure, or

d) any other measures specified in the internal policy that mitigate and manage the risks of money laundering and terrorist financing, as well as the risks of non-compliance with and circumvention of targeted financial sanctions and targeted financial sanctions related to proliferation financing.

Section 28 The service provider shall keep its internal risk assessment up-to-date, setting a date for each calendar year when a business-wide risk assessment update is to be performed.

Section 29 The service provider shall perform an ad hoc review of its internal risk assessment, at least in cases where

a) an external effect changes the nature of the risk,

b) new information about the owners of the service provider, members of its management body, persons performing key functions or its organisation comes to light, and

c) in any other case where the service provider has reasonable grounds to believe that the information on which the risk assessment is based is no longer applicable.

7. Risk management system for determining the status of politically exposed persons in relation to the customer and the beneficial owner

Sections 14 to 16[3]

Section 32 (1) At the request of the supervisory authority, the service provider shall prepare an impact assessment on the applicability of the registers it uses, with the exception of publicly certified official registers, and, based on the results thereof, take further measures to ensure the reliable determination of politically exposed persons if the supervisory authority does not have information on the registers used by the service provider.

(2) In the impact assessment, the service provider shall specify:

a) IT and communication technology and security risks, in particular the risk that the innovative solution may be unsuitable, unreliable or susceptible to manipulation,

b) quality risks, in particular the risk that the information sources used for verification purposes do not meet the relevant legal requirements in terms of independence and reliability, and the risk that the scope of identity verification provided by the innovative solution is not proportionate to the level of money laundering or terrorist financing risk associated with the business relationship,

c) legal risks, in particular the risk that the external service provider providing the technological solution does not comply with the applicable data protection legislation, and

d) the nature of the relationship between the service provider and the third-party provider of the

innovative solution, and the legal basis for that relationship.

(3) The service provider shall specify in its internal policy what information and data it will assess in terms of reliability and independence from the registers it uses, taking into account

a) in the scope of assessing the reliability of information:

(aa) the publicly certified nature of the register based on legal provisions,

(ab) the results of the impact assessment, and

(ac) the legal status of the organisation maintaining the register and its responsibility for the reliability of the data,

b) in the scope of assessing the independence of information, regarding the person or institution that originally issued or made available the data or information

(ba) the extent to which the person or the institution is connected to the assessed customer or beneficial owner through direct personal, professional or family relationships, and

(bb) whether the person or the institution can be influenced by the customer or the beneficial owner.

8. Suspension of transactions

Section 33 (1) The service provider shall determine the information to be provided to the customer and shall establish in its internal policy the obligations and responsibilities of its organisational units in the event of the suspension of a transaction.

(2) The information referred to in paragraph (1) shall not refer to the fact of the suspension of the transaction and the reason for the suspension.

(3) The service provider shall ensure that

a) the manager and employee of the service provider who are aware of the fact of suspension, as defined in Section 31 (1) of the AML Act, shall act in accordance with the information set forth in paragraph (1),

b) it shall involve only the necessary organisational unit to execute the suspension,

c) it can notify the authority acting as a financial intelligence unit by telephone in the event of the emergence of any data, facts or circumstances that may give rise to an obligation to suspend, and in such case it shall act in accordance with the instructions received from them, and

d) during the period of suspension, telephone contact with the authority acting as the financial intelligence unit is maintained even if the designated person is unavailable.

(4) The service provider shall handle the document or a copy of the document certifying the suspension of the transaction separately in the records kept by it.

9. Operation of the internal control and information system

Section 34 For the purposes of this sub-heading:

1. *'automatic screening system'* shall mean an IT system for screening a customer and a transaction for money laundering and terrorist financing based on pre-established parameters, without the need for human intervention,

2. *'manual screening'* shall mean the screening of the customer and the transaction for money laundering and terrorist financing, requiring human intervention,

3. *'screening system'* shall mean a system supporting the execution of an STR report, which ensures that customers and unusual transactions that pose a risk for money laundering and terrorist financing are screened out and that the necessary data for reporting are made available.

Section 35 (1) As part of its internal control and information system, service providers with an automatic screening system as referred to in paragraph (3) shall have a screening system in place that also ensures real-time monitoring of transactions.

(2) The service provider may, with the exception provided for in paragraph (3), apply a screening system based on manual screening.

(3) The service provider shall operate an automatic screening system if

a) it performs payment service or crypto-asset service activities, or

b) it had more than 50,000 customers at the end of the year preceding the year under review.

Section 36 The screening system used by the service provider shall ensure at least the following:

a) the detection of unusual or suspicious transactions,

b) the monitoring of transactions relevant to suspicions of money laundering and terrorist financing,

c) the consistency of the risk profile of the customers in relation to the transactions referred to in point *b)* with the broader knowledge of the service provider in relation to the customer,

d) the consistency of the alerts stored by the screening system with documents, data or information held by the service provider to understand whether the risk associated with the business relationship has changed and to satisfy itself that the information on which the ongoing monitoring is based is accurate, and

e) if necessary to conclude the result of the screening, the obtaining of additional information, in particular documents relating to the source of funds or assets.

Section 37 At the request of the MNB, the service provider shall demonstrate that its transaction monitoring screening system is effective and adequate.

Section 38 (1) The service provider shall determine the conditions, intensity and frequency of screening based on its internal risk assessment, taking into account the unusual transaction alerts and the MNB's alerts based on the nature, scale and complexity of its business activity and the level of its risk exposure.

(2) The service provider shall perform the analysis and assessment of the screened customer or transaction for money laundering and terrorist financing on a risk basis, but no later than within 60 working days after the day on which the screening is performed.

(3) The service provider shall promptly incorporate into its internal risk assessment the information provided by the MNB, subject to public disclosure restrictions to safeguard criminal investigation interests, on screening criteria that require real-time transaction monitoring, or require a faster assessment than the 60 working days specified in paragraph (2).

(4) The service provider shall regularly monitor the effectiveness of the assessment and analysis work performed pursuant to paragraph (2) and the effective functioning of its screening system on a risk basis, taking into account its operating model, by involving an external audit function or, in its absence, additional lines of defence.

(5) The service provider shall document the process of analysis and evaluation of the screened customer or transaction, as well as the verification thereof, in such a way that the result of the action taken by the service provider and the decision taken on the basis of that action can be subsequently

reconstructed.

Section 39 (1) The service provider shall draw up an internal procedure for the operation of the screening system, the procedure for the analysis and assessment of the screened customer and the transaction.

(2) The service provider shall record the internal procedures referred to in paragraph (1) in writing, keep them up-to-date and make them available to the MNB upon request.

(3) The internal procedures for the screening system shall comply with at least the following conditions:

a) they are based on the service provider's internal risk assessment,

b) they comply with the relevant internal policies of the service provider,

c) they document the scenarios used by the service provider, with their underlying logic, parameters and thresholds, and ensure the traceability of changes,

d) they ensure the integrity and quality of the data to ensure that accurate and complete data are transferred through the screening system,

e) they record all data sources containing relevant data,

f) they ensure the availability of qualified staff or external consultants responsible for the design, operation, testing, commissioning and ongoing monitoring of the screening system, as well as for case management, review and decisions on findings and possible STR reports,

g) they record the deadlines used in the analysis and evaluation process,

h) they include investigation protocols that detail how alerts generated by the screening system are to be investigated, how decisions are to be made about which hits should be reported, who is responsible for making such decisions, and how the decision-making process is to be documented,

i) they ensure that the scenarios and the underlying logic, parameters and thresholds are reviewed in accordance with the risks and include who is responsible for their review,

j) they specify which transactions are monitored in real time and which transactions are monitored ex post, including at least the following:

ja) the high-risk factors or combinations of high-risk factors that require real-time transaction monitoring in all cases, and

jb) the higher money laundering and terrorist financing risks associated with real-time tracked transactions, in particular those transactions where there is an increased risk associated with the business relationship, and

k) in the case of an automated screening system, they provide for the testing of the screening system throughout the process, before and after its implementation, as well as periodic testing of control, data mapping, transaction identification, search scenarios and logic, screening modelling, and in relation to the examination of data inputs and results.

Section 40 The service provider shall perform the screening on an ongoing basis. The service provider shall immediately inform the MNB in electronic form, via the MNB's Electronic System for Receiving Authenticated Data (hereinafter referred to as "ERA system") upon becoming aware of any circumstance that has prevented the continuity of the screening for more than 24 hours and of the measures taken or planned to be taken to remedy such circumstance.

Section 41 Within the scope of their data reporting obligations relating to the transfer of funds and certain crypto-asset transfers, payment service providers and crypto-asset service providers shall use infrastructure and services for the transmission and receipt of information that are

technically capable of transmitting and receiving information without deficiencies or errors.

Section 42 The payment service provider and the crypto-asset service provider shall have a screening system capable of screening out any deficiencies or errors in the display of information referred to in Section 41, as well as related transactions below the threshold value.

Section 43 (1) The service provider shall operate an anonymous whistleblowing system as part of its internal control and information system.

(2) Any person who has knowledge that a provision of the AML Act is being or has been violated at the service provider may report such cases of abuse through the whistleblowing system referred to in paragraph (1).

(3) The whistleblowing report shall be investigated by the service provider within 30 days of receipt.

(4) The person affected by such notification shall not participate in the investigation of the report of abuse.

(5) If the service provider establishes that there are data, facts or circumstances indicating money laundering, terrorist financing or the origin of property from a criminal offence, the designated person shall immediately report those to the financial intelligence unit.

(6) If the service provider establishes that a criminal offence is suspected, it shall immediately report the offence to the investigating authority with jurisdiction and competence.

(7) If, in addition to the cases provided for in paragraph (5) and (6), the service provider establishes a violation of the AML Act, the Act on the Implementation of Financial or Asset-related Restrictive Measures ordered by the European Union and the UN Security Council (hereinafter referred to as "UNSC") or this Decree, the designated person shall immediately report this fact to the MNB.

(8) After the case has been reported, the service provider shall ensure that no person other than the person who made the notification or the employee of the service provider as the person investigating the notification has access to the notification.

Section 44 The service provider shall ensure that the internal control and information system is capable of screening the business relationship on the basis of the following:

a) the personal data required by the AML Act,

b) the payment account financial account identified or IBAN,

c) the customer number,

d) the type of transaction, or

e) the amount limit.

Section 45 The service provider shall ensure that the internal control and information system is capable of keeping records of the data recorded in it in a retrievable manner during the period of time specified in the AML Act.

10. Minimum requirements for the development and operation of a screening system to implement financial and asset-related restrictive measures ordered by the European Union and the UNSC

Section 46 For the purposes of this sub-heading:

1. *'automatic screening system'* shall mean an IT system for the continuous comparison, without

human intervention, of the personal data of the customer, beneficial owner, authorised signatory, authorised representative and representative with the data of persons referred to in European Union legal acts and in the United Nations Security Council Resolution (hereinafter referred to as 'UNSC Resolution'),

2. *'manual screening'* shall mean a procedure requiring human intervention to compare the personal data of the customer, beneficial owner, authorised signatory, authorised representative and representative with the data of persons referred to in European Union legal acts and the UNSC Resolution,

3. '*sanctions screening system'* shall mean a screening system that ensures the immediate and complete implementation of EU legal acts and UNSC resolutions ordering financial and asset restrictions.

Section 47 The service provider shall have a sanctions screening system.

Section 48 The service provider shall apply automatic screening within the framework of the sanctions screening system if the service provider had more than 1,000 customers at the end of the year preceding the year under review; otherwise, the service provider may also use manual screening to ensure the immediate implementation of European Union legal acts and the UNSC resolutions ordering financial and asset-related restrictive measures.

Section 49 (1) The service provider shall draw up internal procedures for the operation of the sanctions screening system and the analysis and evaluation of the screened customer, beneficial owner, authorised signatory, authorised representative and representative, as well as the transaction.

(2) The service provider shall record and keep up-to-date the internal procedures specified in paragraph (1) in writing and make them available to the MNB acting in its supervisory capacity.

(3) The internal procedures of the sanctions screening system shall comply with at least the following conditions:

a) they document the search logics used by the service provider, with the assumptions and parameters on which they are based,

b) they ensure the integrity, accuracy and quality of the data to ensure that accurate and complete data are transferred through the sanctions screening system,

c) they record all data sources containing relevant data,

d) they ensure the availability of qualified staff or external consultants responsible for the design, operation, testing, commissioning and ongoing monitoring of the sanctions screening system, as well as for case management, review and decisions on findings and possible reports,

e) they record the deadlines used in the analysis and evaluation process,

f) they include investigation protocols that detail how alerts generated by the sanctions screening system are to be investigated, how decisions are to be made about which hits should be reported, who is responsible for making such decisions, and how the decision-making process is to be documented,

g) they ensure the continuous testing of the screening logics and the underlying rules and parameters, and

h) in the case of an automated screening system, they enable the testing of the sanctions screening system throughout the process, before and after its implementation, as well as periodic testing of control, data mapping, transaction identification, search and logics, screening modelling, and through the examination of data inputs and results.

Section 50 (1) The service provider shall continuously perform screening regarding financial and

asset-related restrictive measures ordered by the European Union and the UNSC. The service provider shall immediately inform the MNB in electronic form, via the ERA system upon becoming aware of any circumstance that has prevented the continuity of the screening for more than 24 hours and of the measures taken or planned to be taken to remedy such circumstance.

(2) The service provider shall analyse and evaluate the screened results.

(3) The service provider shall regularly monitor the effectiveness of the assessment and analysis work performed pursuant to paragraph (2) and the effective functioning of its screening system on a risk basis, taking into account its operating model, with the involvement of all lines of defence of the service provider.

(4) The service provider shall document the process of analysis and evaluation of the screened hits, as well as the verification thereof, in such a way that the result of the action taken by the service provider and the decision taken on the basis of that action can be subsequently reconstructed.

11. Training programme

Section 51 (1) The service provider shall provide its compliance officer and employee involved in the performance of activities related to the prevention and combating of money laundering and terrorist financing and to financial and asset-related restrictive measures ordered by the European Union and the UN Security Council (hereinafter jointly referred to as "employee") with training prior to their employment in this position or within 30 days of their entry into this position (hereinafter referred to as "prevention training") and shall organise refresher training sessions for them at least once annually after the year of their entry into this position (hereinafter jointly referred to as "training"). The training includes a written examination organised by the service provider, including an examination conducted via the service provider's electronic systems.

(2) The employee may only participate in the performance of activities related to the prevention and combating of money laundering and terrorist financing, and to financial and asset-related restrictive measures ordered by the European Union and the UN Security Council under the supervision of a staff member who has successfully passed an examination related to the training specified in paragraph (1) until he/she has successfully passed an examination organised by the service provider on the knowledge acquired in the prevention training.

(3) For the provision of training, the service provider may only use a person who

a) holds a higher education degree in a specialised field, in particular law, economics, finance or information technology, and

b) has at least three years of

ba) professional experience in an internal audit or compliance function at a service provider covered by the AML Act, or

bb) professional experience obtained at the supervisory body specified in Section 5 of the AML Act in the field of the supervisory activity covered by the AML Act.

(4) The service provider shall elaborate a training programme with a level of detail necessary to fill each job role; the training programme shall include the topics necessary to fill each job role.

(5) The service provider shall keep retrievable records of the material of the training courses and the examinations related thereunto, the dates of the training courses and the names of the participants, the examination answer key, the names of the examinees and the examination results per examinee, and shall retain such records for five years from the date of the examination.

(6) The service provider's compliance manager shall be responsible for developing the training programme of the service provider, organising the prevention training in a timely manner, ensuring that employees have the opportunity to participate in the training, recording the data specified in paragraph (5) in a retrievable manner and monitoring compliance with paragraph (2).

(7) When developing group-level policies and procedures, the service provider shall take into account the provisions of paragraphs (1) to (6).

CHAPTER V

PROFESSIONAL REQUIREMENTS FOR THE PERSON PERFORMING THE EXTERNAL AUDIT FUNCTION AND THE MANDATORY CASES OF ENGAGEMENT

12. Rules on the appointment and engagement of the person performing the external audit function

Section 52 (1) The external audit function as defined in Section 3 point 21a of the AML Act may be performed by a person who has at least five years of proven professional experience in auditing or advising on the services provided by the service provider.

(2) The service provider shall, at the request of the MNB, demonstrate that the party appointed by it to perform the external audit function and its employee who actually performs the external audit function (hereinafter jointly referred to as "external auditor") have adequate knowledge of:

a) the legal requirements applicable to the service provider's sector,

b) the systems used by the service provider,

c) the policies and procedures implemented by the service provider, and

d) the services and products provided by the service provider.

(3) When appointing an external auditor, the service provider shall take into account that the external auditor may not be identical with

a) the statutory auditor or audit firm that has performed the statutory audit of the service provider in the three years preceding the date of the external audit, nor the legal adviser or legal representative engaged by the service provider in the three years preceding the date of the external audit to ensure compliance with the provisions containing the statutory requirements relating to the prevention of money laundering and terrorist financing,

b) the service provider supplying or operating the systems used by the service provider, the external service provider drawing up the service provider's internal procedures in force, or the service provider acting as consultant for the procurement of such systems or the drawing up of such procedures, or

c) an undertaking owned by the service provider, a subsidiary of the service provider or a person listed in paragraph (4).

(4) A person who has held the following functions with the service provider in the three years preceding the engagement may not hold an external audit function:

a) an employee of the audited service provider,

b) an employee of the audited service provider in a managerial position,

c) a member of the audit committee of the audited service provider or, in the absence of such a committee, a member of a body performing functions equivalent to those of an audit committee, or

d) a member of the management body of the audited service provider.

(5) The external auditor's mandate may be ad hoc or for a fixed term. The fixed-term mandate for the external audit function shall be for a maximum of two years. After the expiry of the mandate, the service provider may not grant the external auditor a new external audit mandate for a period of up to twice the duration of the original mandate. For the purposes of this paragraph, regularly recurring ad hoc engagements shall be regarded as a single, continuous engagement of limited duration.

(6) Taking into account the provisions of Section 60 (2) *e)* of the AML Act, the procedure for the selection of the external auditor shall be defined in the internal policy of the service provider.

(7) In the case of using the external audit function, the service provider shall, on the basis of the internal risk assessment specified in Section 27 (1) of the AML Act, update the internal policy set forth in Section 65 of the AML Act to specify all issues to be examined, which the audit report prepared by the external auditor shall cover in order to reduce and manage the risks of the service provider. In the case of a fixed-term mandate, the areas to be examined, as set out in the internal policy, shall include at least the compliance of the systems used by the service provider to prevent and combat money laundering and terrorist financing, including the screening, reporting and support systems for the risk classification of customers.

Section 53 (1) The service provider shall use the external audit function at least in the following cases:

a) if the service provider decides to use an external control function based on the findings of its internal risk assessment,

b) if the MNB requires the service provider to engage an external auditor, taking into account the findings of its internal risk assessment, and

c) if the service provider has at least 100,000 customers doing business with the service provider on average per year and the annual number of alerts generated by the service provider's screening system requiring risk action is at least 10,000 or where the service provider uses an artificial intelligence solution for its screening processes; and where the screening, reporting and customer risk classification support systems used or employed by the service provider to prevent and combat money laundering and terrorist financing have not been audited by an external audit function within five years.

(2) At the request of the MNB, the service provider shall commission an external audit to assess the aspects set out in the relevant notice.

13. Rules on the operation of the external auditor

Section 54 (1) The external auditor may not be instructed or influenced by anyone in the performance of his/her duties.

(2) The external auditor shall draw up an audit report on the inspection at the service provider at the end of the ad hoc mandate, or at least every calendar year in the case of a fixed-term mandate, in which he/she shall make findings and observations, supported by practical examples, in order to assess whether the service provider is able to fulfil the obligations laid down in the AML Act and its delegated legislation, and whether the procedures required for this, the systems used by it, and its internal and external resources are appropriate and sufficient. The external auditor may also prepare an unscheduled report, if necessary.

(3) The audit report drawn up by the external auditor shall also contain proposals for measures to be taken to ensure the legal compliance of the service provider and measures deemed necessary on the basis of the examination of the aspects specified in paragraph (2).

(4) The external auditor shall send the audit report directly to the management body of the service provider. The management body of the service provider shall discuss the external auditor's audit report at a meeting of the management body, at which the external auditor may be present as an invitee.

(5) The service provider shall make the external auditor's audit report available to the MNB and the service provider's compliance manager without delay.

Section 55 The external auditor shall have liability insurance to cover any damage caused by him/her to the service provider, guaranteeing that he/she will be able to comply with any liability arising from his/her activities.

Section 56 (1) The contract of engagement between the service provider and the external auditor shall include at least the following:

a) a professional description of the external auditor's qualifications and a statement of compliance with the qualification requirements, including the qualifications of all of his/her collaborators, as set out in sub-heading 12,

b) the definition of the material conditions and system access rights necessary for the external auditor to perform his/her tasks,

c) the definition of the conditions relating to the external auditor's liability insurance pursuant to Section 55,

d) the obligation for the external auditor or any collaborator engaged by the external auditor to attend professional training organised by the MNB or recognised as appropriate by the MNB and published on its website,

e) the recording under the terms of immediate termination of the engagement contract of the circumstance where facts are discovered during the performance of the engagement which substantiate the external auditor’s lack of competence, and

f) a statement of the facts justifying the engagement of the external auditor, as provided for in Section 53.

(2) At the request of the MNB, the service provider shall demonstrate the measures taken to ensure that the obligations of the external auditor under the engagement contract are fulfilled in accordance with the contract.

CHAPTER VI

CLOSING PROVISIONS

14. Provisions on entering into force

Section 57 (1) This decree shall enter into force on 1 July 2025, with the exceptions specified in paragraphs (2) and (3).

(2) Sections 14 to 16 shall enter into force on 1 September 2025.

(3) Sections 30 to 31 shall enter into force on 31 December 2025.

15.[4]

Section 58[5]

[4]Repealed: Based on Sections 12–12/B. of Act CXXX of 2010. Effective: From 2 July 2025.
[5]Repealed: Based on Sections 12–12/B. of Act CXXX of 2010. Effective: From 2 July 2025.