MNB Decree 26/2020. (VIII. 25.)

on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests

Acting under the authorisation conferred by Section 77 (3) of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing and

in respect of Subheading 10, by Section 17 (3) of Act LII of 2017 on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests, in my competence specified in Section 4 (9) of CXXXIX 2013 on the Magyar Nemzeti Bank, I decree the following:

CHAPTER I

GENERAL PROVISIONS

Section 1 The scope of this Decree applies to credit institutions, providers of financial services, occupational retirement institutions, voluntary mutual funds, international postal voucher acceptance and delivery service providers and trust managers (hereinafter collectively referred to as "the service provider") falling within the scope of Act LIII of 2017 on preventing and combating money laundering and terrorist financing (hereinafter: the "AML Act").

Section 2 For the purposes of this Decree:

1. *Audited electronic communications equipment:* an audited electronic system that is suitable for performing the customer due diligence, making customer declaration, the interpretation and safe storage of the declarations made by the customer and the retrieval and verification of the data stored remotely through an electronic data communications channel,

2. *Transfer related to an area outside the European Union:* service aimed to make a credit entry on the payee's payment account by means of a payment transaction or a series of payment transactions, which is launched from the payer's payment account managed by a payment service provides based on the order given by the payer, regardless of whether the payee and the payer are the same person and regardless of whether the payer's payment service provider and the payee's payment service provider are identical, if

a) the payee's or the payer's place of residence or establishment, or

b) the registered address of any payment service provider

is located outside the European Union,

3. *Electronic client identification and declaration system:* a system providing a personalised electronic process that facilitates making legal declarations in a form allowing for the clear identification of the declarant and the time when the declaration is made, as well as the unchanged retrieval of the content of the declaration,

4. *strong customer authentication:* authentication with the use of at least two elements that can be allocated to the category of

a) knowledge, i.e. something that only the user knows,

b) possession, i.e. something that only the user possesses, and

c) biological feature, i.e. something that is specific to the user,

which categories are independent of each other so that the breach of one does not compromise the reliability of the others, and the development of the procedure ensures the confidentiality of the personalised security credentials,

5. *Risk profile:* the general nature of the residual risk following the mitigation of the identified risks of money laundering and terrorist financing, including the type and level of the risk;

6. *Strengthened procedure:* increased monitoring involving a combination of risk-based measures for the management of the risk inherent in the customer, the product, the service, the transaction, the means employed, or the geographical exposure;

7. *monitoring:* continuous monitoring of the business relationship and the customer regularly submitting transaction orders,

8. *Money laundering and terrorist financing risk:* the likelihood and impact of money laundering and terrorist financing taking place;

9. *Unusual transaction:* Any transaction, which

a) is not consistent with the procedures generally followed in connection with the product or service;

b) lacks clearly understandable economic purpose or legal grounds;

c) indicates an unreasonable change in the frequency or volume of the transactions in comparison with the customer's previous activity.

CHAPTER II

RULES OF CUSTOMER DUE DILIGENCE PERFORMED THROUGH AUDITED ELECTRONIC COMMUNICATIONS EQUIPMENT

1. Minimum requirements for the operation of audited electronic communications equipment, audit method

Section 3 The provisions of this Section applicable to the customer shall be also applied to the proxies, associates with right of disposal and authorised representatives of the customer acting at the service provider.

Section 4 Electronic communications equipment may be audited and operated subject to compliance with at least the following IT security requirements:

a) its components are identifiable and documented;

b) its operating processes are regulated, documented, and controlled at the intervals specified in the operating policy;

c) its change management processes ensure that changes to the parameters and software code of the system may only be implemented in a tested and documented manner;

d) its data backup and recovery procedures provide for the safe recovery of the system, and backup and recovery are tested at the intervals specified in the operating policy, and documented;

e) user access is regulated, documented, and controlled at the intervals specified in the operating policy at both application and infrastructure level;

f) the end user access privileges assigned constitute a consistent and self-contained system and ensure implementation of the identification process, user activities are logged, and automated alerts are generated about incidents;

g) elevated access privileges are regulated, documented, and controlled at the intervals specified in the operating policy, activities carried out using elevated privileges are logged, the integrity of log files is provided, and automated alerts are generated about critical incidents;

h) remote access is regulated, documented, and controlled at the intervals specified in the operating policy;

i) protection is provided against viruses and other malware and malicious action;

j) its data communication and system connections are documented and controlled, and the confidentiality, integrity and authenticity of data communication is provided;

k) the disaster recovery plan is regularly tested, provided, that the service provider is prevented from performing the customer due diligence in other ways or the system used is classified as a business critical system in respect of the service provider,

l) its maintenance is regulated;

m) the protection of its data media is regulated and provided so that access to data media is only granted to authorised staff and only for the achievement of the purpose of data processing, which is reviewed and controlled at regular intervals;

n) its own controls and the operating policy provide for the integrity and protection of the system components and the information processed; and

o) arrangements have been made for an adequate level of physical protection, a segregated environment and the detection of specific security incidents.

Section 5 In respect of the audited electronic communications equipment, the service provider shall ensure that

a) an adequate level of security, encryption, confidentiality, integrity and authenticity is provided for the remote data transmission through the electronic transmission channel with the customer,

b) the customer is informed about the conditions of using the service, including the customer's liability for the security of the service,

c) depending on the solution applied by the service provider, due diligence on the service provider's side only involves staff that has received legal, technical and security training as required for direct or indirect electronic customer due diligence, and only to the extent required;

d) an audit report has been issued on the electronic communications equipment and the customer due diligence process confirming that their IT protection is proportionate with the security risks, and complies in particular with the requirements in Section 4;

e) arrangements are made for the renewal of the audit report in the event of any relevant changes to the technology applied or the business process with an impact on operations, but at least every two years;

f) the audit report referred to in paragraph *d)* is issued by an entity registered in a Member State of the European Economic Area, engaging a person who has verifiably participated in the audit and holds at least one of the following qualifications and certifications, or higher:

fa) Certified Information Systems Auditor (CISA), issued by the Information Systems Audit and Control Association (ISACA);

fb) Certified Information Systems Manager (CISM), issued by the Information Systems Audit and Control Association (ISACA);

fc) Certified Information Systems Security Professional (CISSP), issued by International Information Systems Security Certification Consortium Inc. (CISSP), or

fd) Lead Auditor according to ISO/IEC 27001 Information Security Management Systems standard,

g) the personal data and the data not qualifying as personal data, obtained by the service provider during the customer due diligence and electronic identification prescribed by the AML Act, are made available to data subject during the period of data processing, and

h) the data stored electronically on the customer due diligence process are recorded in a way that later on makes them suitable for the subsequent assessment of compliance with the customer due diligence regulations and the implementation of the customer due diligence measures.

2. Common rules of the customer due diligence performed through audited electronic communication equipment

Section 6 (1) During the customer due diligence performed through audited electronic communication equipment, the service provider performs customer due diligence and verification of the customer's identity in accordance with the AML Act, and it shall also call upon the customer to make the declarations and present the instruments prescribed by the AML Act.

(2) The service provider shall develop the scheme of customer due diligence performed through audited electronic communication equipment taking into consideration the due rights of disabled persons, as stipulated in the Act on the Rights and Ensuring the Equal Opportunities of People with Disabilities.

(3) The service provider shall verify the fulfilment of the requirements applicable to customer due diligence performed through audited electronic communication equipment by the employee and in the manner stipulated in its internal policy. The verification and the related policy shall also cover the compliance with the requirements applicable to the recording of the workflow.

Section 7 (1) The service provider may perform the customer due diligence by means of audited electronic communications equipment in a direct or indirect electronic manner.

(2) When using audited electronic communications equipment, if the service provider obtains the beneficial owner and politically exposed person declarations as well as the copies of the instruments with the use of its electronic client identification and declaration system, no transaction shall be executed until such time as these declarations and copies of instruments are obtained and all customer due diligence measures to be performed based on the customer's

individual risk rating are completed.

(3) The restriction specified in paragraph (2) shall not apply if the submission of the copy of the instrument is necessary due to the replacement of the instrument or to data change in the case of a customer previously subjected to complete due diligence.

3. Forms and rules of indirect electronic customer due diligence

Section 8 (1) The service provider shall perform the indirect electronic customer due diligence executed through audited electronic communication equipment (hereinafter: indirect electronic customer due diligence) through an equipment that is able to

a) ascertain that the customer appearing at the remote location as the subject of the due diligence is a real, live person, uses the audited electronic communications equipment real time, personally and that the live picture is not manipulated, and

b) compare the photo taken of the customer during the customer due diligence and the image included in the instrument used for the due diligence in such a way that it can be established, beyond reasonable doubt, that the person specified in the official personal identity certificate is the same as the person on the photo.

(2) When using indirect electronic customer due diligence, the service provider provides the conditions related to customer due diligence in respect of the audited electronic communications equipment, if

a) the customer has learnt the detailed conditions of the indirect electronic customer due diligence and has specifically consented to it,

b) it uses strong customer authentication,

c) the resolution of the electronic communications equipment supporting picture transmission, and the lighting of the picture are suitable for the recognition of the gender, age and facial characteristics of the customer, for comparison with the photo identification card presented by the customer, and for identification of the security features of the presented official personal identity certificate, and

d) the customer due diligence process is regulated and controlled on a continuous basis.

Section 9 (1) The service provider shall record in a retrievable manner the entire workflow taking place in the course of indirect electronic customer due diligence between the service provider and the customer, the detailed information given to the customer about the indirect electronic customer due diligence, and the customer's specific consent to the due diligence.

(2) In order to perform the indirect electronic customer due diligence, the service provider shall

a) call upon the customer to look into the camera so as to allow his facial image to be recognised and recorded,

a) ascertain that the customer is a real, live person, uses the audited electronic communications equipment real time, personally and that the live picture is not manipulated, and

c) record the documents used for the customer due diligence in a way that the security features and data lines therein can be recognised and stored.

(3) The service provider performing the indirect customer due diligences shall ascertain that the used official personal identity certificate is suitable for the execution of the indirect electronic customer due diligence, and particularly

a) that certain elements of the official personal identity certificate and the position of those comply with the requirements of the authority issuing the official personal identity certificate, and

b) the specific security features, including in particular holograms, kinegrams and other equivalent security features are recognisable and intact,

(4) The service provider shall ensure that

a) the facial image of the customer is recognisable and can be identified with the facial image in the official personal identity certificate presented by him, and

b) the identification data required by the AML Act have been fully obtained and the data in the official personal identity certificate can be logically matched with the data held by the service provider about the customer.

Section 10 (1) In the course of the indirect customer due diligence, the service provider shall compare the photo recorded of the customer with the facial image in the official personal identity certificate by using the audited electronic communications equipment.

(2) In the knowledge of the result of all customer due diligence measures prescribed by the AML Act, performed on the basis of the customer's individual risk rating, the service provider shall send a notification to the customer on the result of the customer due diligence within 2 banking days after recording.

Section 11 (1) The service provider shall interrupt the indirect electronic customer due diligence if:

a) the customer withdraws his consent to data recording during the customer due diligence,

b) the physical and data content requirements of the official personal identity certificate presented by the customer do not comply with the conditions specified in Section 9 (3),

c) the conditions of the visual identification of the official personal identity certificate presented by the customer are not fulfilled,

d) the service provider is unable to make the recording or cannot record the workflow defined in Section 9 (1), or

e) any contradiction or uncertainty occurs during the due diligence.

(2) The service provider shall immediately subject the customer to due diligence in his personal presence or to direct electronic customer due diligence, if in respect of the customer's activity the risk of money laundering or terrorist financing arises, and the customer cooperates in the execution of customer due diligence in the changed form, and thereby the service provider does not violate the prohibition of disclosure.

Section 12 The service provider shall perform the indirect electronic customer due diligence

a) using the Central Authentication Agent (hereinafter: CAA) service specified in Government Decree 451/2016 on the Detailed Rules of Electronic Administration,

b) by retrieving the authentic, natural identification data, suitable for the identification of the customer, from the official personal identity certificate containing the electronic storage element, or

c) in any other way, subject to the restrictions specified in Section 16.

Section 13 (1) The service provider performs the indirect electronic customer due diligence in accordance with Section 12 *a)*, if

a) it is performed by a service provider qualifying, within the meaning of sub-points *j)* and *l)* of point 17 of Section 1 of Act CCXXII of 2015 on the General Rules of Electronic Administration and Trust Services (hereinafter: Electronic Administration Act), and included in the database of transactions that can be administered electronically, or

b) by a market participant using the service specified in Section 42/A of the Electronic Administration Act

through an audited electronic communications equipment, and in the course of that the customer identifies himself through the electronic authentication service specified in the Electronic Administration Act.

(2) In order to implement the electronic authentication service specified in paragraph (1), the service provider shall

a) prescribe electronic authentication of "substantial" or "high" assurance level, as specified in Article 8(2) of Regulation 910/2014/EU of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,

b) connect to the CAA service through the audited electronic communication equipment and ensure through such equipment that during the customer due diligence the customer identifies himself, and

c) verify the customer's identity based on the information returned by CAA through the audited electronic communication equipment provided by it.

Section 14 (1) The service provider performs the indirect electronic customer due diligence in accordance with Section 12 *b)*, when

a) it retrieves – electronically through the audited communications equipment – the authentic, natural identification data, suitable for the identification of the customer and the photo taken of the customer by the authority that issued the official personal identity certificate, from the official personal identity certificate containing the electronic storage element presented by the customer, and compares them with the data provided by the customer and with the data and photo recorded during the identification, and

b) upon comparing the data and photos through the audited communications equipment it can be established beyond reasonable doubt that the person in the official personal identity certificate is the same as the person on the photo taken during the due diligence by the audited communications equipment, and that the official personal identity certificate was issued by the competent authority, and the data stored and retrieved electronically are unchanged and authentic.

(2) In addition to the cases specified in Section 11, the service provider does not execute the customer due diligence also in the case when during the due diligence it is unable to retrieve all relevant data from the electronic storage element of the electronic personal identity card, any doubt arises with regard to the authenticity of the official personal identity certificate or the data retrieved from the official personal identity certificate, or based on the retrieved data the service provider is unable to identify the customer beyond reasonable doubt.

Section 15 In the cases stipulated in Sections 13 and 14, the service provider shall

a) verify, with the use of the audited electronic communications equipment, the validity of the official personal identity certificate presented by the customer, including in particular that the official personal identity certificate is not invalid, in has not be withdrawn or annulled, and it has not been reported as lost, stolen, destroyed, damaged, found or has not been submitted to the authority, and

b) monitor the customer's business activity within the framework of strengthened procedure for one year after establishing the business relationship.

Section 16 When the service provider does not apply either of the solutions specified in Section 13 and 14, it may

perform indirect electronic customer due diligence, if

a) the customer involved in the customer due diligence or its beneficial owner involved in the due diligence is domiciled or headquartered in other than a third country involving strategic deficiencies and high risk,

b) the service provider ensures that the customer involved in the customer due diligence cannot execute cash transactions – with the exception of a monthly cash withdrawal in an amount not exceeding three hundred thousand forint – or credit transfers related to a region outside the territory of the European Union until such time as the customer appears in person or the direct electronic customer due diligence is performed, and

c) the service provider ensures that the customer involved in the customer due diligence cannot execute any transaction reaching or exceeding the amount of ten million forint until such time as the customer appears in person or the direct electronic customer due diligence is performed.

4. Rules of the direct electronic customer due diligence

Section 17 (1) During the direct electronic customer due diligence performed by using audited electronic communications equipment (hereinafter: direct electronic customer due diligence), the service provider compares – through the equipment complying with the provisions of Section 8(1) – the photo taken of the customer and the facial image in the official personal identity certificate. The customer due diligence is appropriate if it can be established beyond doubt that the person shown in the official personal identity certificate is the same as the person on the photo or in the video recording.

(2) The service provider shall perform direct electronic customer due diligence without using equipment complying with Section 8 in a room suitable for the purpose.

(3) Direct electronic customer due diligence may only be conducted by the managers and employees of the service provider, who previously completed the training arranged by the service provider on the conduct of such activities, and passed the subsequent test.

(4) In respect of the audited electronic communications equipment, the service provider shall provide the conditions for customer due diligence, to the extent that

a) has specifically consented to the conduct of such direct electronic customer due diligence,

b) the resolution of the electronic communications equipment enabling video real-time video and audio transmission, and the lighting of the image produced are suitable for the recognition of the gender, age and facial characteristics of the customer, and

c) the customer due diligence process is regulated and controlled on a continuous basis.

Section 18 (1) The service provider shall produce a retrievable video and audio recording of the entire communication taking place in the course of direct electronic customer due diligence between the service provider and the customer, the detailed information given to the customer about the direct electronic customer due diligence, and the customer's specific consent to the due diligence.

(2) In the course of direct electronic customer due diligence, it shall be ensured that the customer

a) looks into the camera so as to allow his facial image to be recognised and recorded,

b) clearly states the identification code of the official personal identity certificate used for the direct electronic customer due diligence, and

c) moves the official personal identity certificate used for the direct electronic customer due diligence in such a way that the security features and data series shown thereon can be recognised.

(3) The service provider performing the direct customer due diligence shall ascertain that the official personal identity certificate used for the direct electronic customer due diligence is suitable for the execution of the direct electronic customer due diligence, and thus

a) certain elements of the official personal identity certificate and the position of those comply with the requirements of the authority issuing the official personal identity certificate and with the relevant statutory provisions,

b) the specific security features, including in particular holograms, kinegrams and other equivalent security features are recognisable and intact, and

c) the document identifier of the official personal identity certificate corresponds to the document identifier stated by the customer, it is recognisable and intact.

(4) The service provider conducting direct electronic customer due diligence shall verify that

a) the facial image of the customer is recognisable and can be identified based on the facial image included in the official personal identity certificate presented by the customer, and

b) the data in the official personal identity certificate can be logically matched with the data held by the service provider about the customer.

(5) The service provider shall verify the validity of the official personal identity certificate presented by customer,

including in particular that the official personal identity certificate is not invalid, it has not be withdrawn or annulled, and it has not been reported as lost, stolen, destroyed, damaged, found or has not been submitted to the authority.

(6) The service provider shall send a centrally generated random identification code consisting of alphanumeric characters to the customer, by e-mail or text at the option of the service provider, to the customer's identifiable e-mail address or mobile phone, respectively. The customer shall return the code to the service provider before direct electronic customer due diligence is completed, through the communication channel specified by the service provider.

Section 19 The service provider shall interrupt the direct electronic customer due diligence, if

a) the customer withdraws his consent to data recording during the direct electronic customer due diligence,

b) the physical and data content requirements of the official personal identity certificate presented by the customer do not comply with the conditions specified in Section 18 (3),

c) the conditions of the visual identification of the official personal identity certificate presented by the customer are not fulfilled,

d) the service provider is prevented from producing the audio and video recording,

e) the customer fails to return the identification code, or returns an incomplete or incorrect code,

f) the customer does not make a declaration or noticeably makes a declaration under influence, or

g) any contradiction or uncertainty occurs during the due diligence.

CHAPTER III

CASES OF SIMPLIFIED AND ENHANCED CUSTOMER DUE DILIGENCE

Section 20 The service provider may apply simplified customer due diligence if its customer is of low risk based on the classification specified in Section 6/A of the AML Act.

Section 21 (1) In addition to the cases provided for in the AML Act, the service provider conducts enhanced customer due diligence where the customer

a) is a non-profit organisation complying with the criteria specified in the service provider's internal risk assessment,

b) a legal entity or unincorporated organisation, the beneficial owner of which comes from third country of strategic shortcomings, representing outstanding risk,

c) is a company that has bearer shares, or its shareholder is represented by a nominee, or

d) is a company with an ownership structure that appears unusual or overly complex relative to the nature of the company's business.

(2) The provisions of Section (1) *d)* shall not be applied, if in the opinion of the service provider the overly complex ownership structure of the company is justified, and proves this in detail in its risk assessment by evaluating the factors mitigating and increasing the risk simultaneously, or the customer is of low risk based on the classification specified in Section 6/A of the AML Act.

CHAPTER IV

MEASURES TO BE PERFORMED BY THE SERVICE PROVIDER BASED ON THE CUSTOMER'S INDIVIDUAL RISK CLASSIFICATION

5. Cases where the risk sensitivity approach requires a management decision for the establishment of a business relationship or the execution of a transaction order

Section 22 (1) In addition to the cases stipulated in the AML Act, the decision shall be made by the manager specified in the service provider's internal policy, as a minimum, on

a) the establishment of the business relationship, if any data, fact or circumstance arise that imply that the service in fact is used not by the person that is indicated in the contract application,

b) the establishment of the business relationship, if the customer indicates that the monthly volume of cash transactions would reach or exceed one hundred million forint per year,

c) the execution of the transaction order, if the value thereof reaches or exceeds fifty million forints,

d) the establishment of private banking business relationship,

e) the execution of transaction orders related to new products, or involving new business practices, among other things, new execution solution or the application of new or developing technologies, carrying additional risk elements specified in the internal risk assessment,

f) the execution of unusual transaction.

(2) If the service provider operates a separate organisational unit for the prevention of money laundering and terrorist financing, and for the implementation of the financial restrictive measures ordered by the European Union and the United Nations Security Council (hereinafter: UNSC), in the cases specified in paragraph (1) *a)* and *b)* the decision shall be made by the head of this organisational unit or his appointed deputy.

(3) In respect of certain groups of customers, specified by the service provider, the service provider may omit the management decision, if in respect of the cases specified in paragraph (1) it supports such decision in detail in its internal risks assessment, simultaneously evaluating the factors that mitigate and increase the risks.

(4) The manager of the service provider specified in paragraphs (1) and (2) shall make his decision in such documented form that ensures consistency, the possibility of continuous monitoring and verifiability.

6. Strengthened procedure – cases and criteria

Section 23 (1) In addition to the cases provided for in the AML Act, the service provider may conduct a strengthened procedure at least in the following cases:

a) in respect of customers involved in the registration of anonymous savings deposits as specified in the Law Decree on Savings Deposits, to the extent that the aggregate amount of the savings deposits to be registered is at least four million, five hundred thousand forint, for one year from the registration,

b) if the service provider performs the customer due diligence due to a currency exchange reaching or exceeding ten million forints, for one year after last the currency exchange reaching or exceeding ten million forints,

c) if the service provider performs the customer due diligence of a customer regularly submitting transaction orders due to a transaction order reaching or exceeding fifty million forints, for one year after the last transaction order reaching or exceeding fifty million forints,

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

e) if any notification is made under Section 30 (1) of the AML Act in connection with the customer of the service provider by the service provider or by an entity in the group that the service provider belongs to, for one year from the last notification,

f) for non-Hungarian citizen natural persons not holding a residence permit or registration of stay providing the right to stay in Hungary for more than ninety days, nor having residence or abode Hungary, with place of residence or abode outside the European Union or the European Economic Area.

(2) The service provider shall stipulate the cases of its strengthened procedures other than those specified in paragraph (1), in its internal risk assessment.

(3) In respect of certain groups of customers, specified by the service provider, the service provider may omit the strengthened procedure, if in respect of the cases specified in paragraph (1) it supports such decision in detail in its internal risks assessment, simultaneously evaluating the factors that mitigate and increase the risks.

Section 24 (1) As regards of customers falling under the strengthened procedure, the service provider shall screen, and analyse and evaluate from the perspective of money laundering and terrorist financing, the transactions specified in its internal risk assessment in accordance with the provisions of Sections 34-37.

(2) In the course of the risk assessment specified in paragraph (1), the service provider shall apply a limit by transaction.

(3) The limit specified in the internal risk assessment shall be determined by the service provider subject to the simultaneous assessment of the risk mitigating and risk increasing factors, and it may not exceed one hundred million forints.

(4) If customers falling under the strengthened procedure perform cash payments or currency exchange reaching or exceeding ten million forints, the service provider shall obtain information on the sources of funds and require the submission of documents on the sources of funds in order to verify that information.

CHAPTER V

CERTAIN RULES APPLICABLE TO THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING, AND TO THE IMPLEMENTATION OF FINANCIAL RESTRICTIVE MEASURES ORDERED BY THE EUROPEAN UNION AND UNSC

7. Rules for internal risk assessment

Section 25 (1) As part of its internal risk assessment, the service provider shall identify from its known risks those affecting its money laundering and terrorist financing risks.

(2) For the purpose of the identification under Subsection (1), the service provider shall take into account the available risk profile.

Section 26 (1) In addition to the factors provided for in the AML Act, for the identification of risk factors, the service provider shall take into account the following:

a) the European Commission's supranational risk assessment,

b) the opinions of European supervisory authorities on risks of money laundering and terrorist financing to the EU's financial sector,

c) the recommendation issued by the Magyar Nemzeti Bank (hereinafter: the MNB),

d) information disclosed by the MNB, and

e) documents generated and disclosed in the course of proceedings conducted by the MNB.

(2) For the identification of risk factors, the service provider may take into account information obtained, in particular, from

a) the civil society,

b) the assessment of the adequacy and effectiveness of the system implemented by the state specified in Section 27 (1) to combat money laundering and terrorist financing, and its anticorruption and taxation regimes,

c) public sources, and

d) information from scientific institutions.

Section 27 (1) Where a service provider is exposed to risks of money laundering and terrorist financing from another Member State or a third country, the service provider shall also identify those risks.

(2) The service provider shall identify the risks under Subsection (1) particularly where the service provider

a) is a member of a financial group formed in another Member State or in a third country,

b) is the owner of a service provider registered in another Member State or third country

c) its beneficial owner comes from another Member State or from a third country, or

d) maintains a relationship with a body or organisation in another Member State or in a third country that implies that the service provider is exposed to the money laundering and terrorist financing risks of the respective country.

(3) The service provider shall collect information pertaining to risks of money laundering and terrorist financing associated with the Member State or third country under Subsection (1) that could affect its activities.

(4) Within three business days of becoming aware, following the identification of the risks under Subsection (1) and the collection of the information under Subsection (3), of any deficiencies that threaten the financial system of the European Union, the service provider shall report such deficiencies to the MNB.

Section 28 The service provider shall take into account the following considerations for the purpose of its internal risk assessment:

a) its ownership and corporate structure, with regard to the status of the service provider as an international, non-resident or resident institution, parent undertaking, subsidiary, branch office or other entity,

b) the complexity and transparency of its organisation and structure,

c) the nature and complexity of the product or service offered, the activity performed, and the transaction executed,

d) the means employed, including services rendered free of charge, and the engagement of agents or brokers,

e) the types of customers serviced,

f) the geographical scope of its business, particularly where it is conducted in a third country involving strategic

deficiencies and high risk, or a significant proportion of the service provider's customers originate in a third country involving strategic deficiencies and high risk,

g) the quality of its internal control arrangements and structure, including the effectiveness of the internal audit and compliance functions, compliance with the legal requirement for the prevention and combating of money laundering and terrorist financing, and the effectiveness of its previous internal risk assessments,

h) the prevailing corporate culture, in particular the culture of compliance and transparency,

Section 29 (1) The service provider's risk assessment shall be based on the factors in Sections 26-28 collectively.

(2) In order to mitigate the risk of money laundering and terrorist financing, the service provider shall assess the impact of the risk factors under Sections 26-28 on the service provider, and the adequacy of the risk-based control system and process that the service provider has in place.

(3) Based on the relative significance of each risk factor, the service provider may apply various weights to risks and the factors mitigating the risks.

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

(5) The service provider shall classify risks at least into the risk groups of customer, product, service, means employed, and geographical.

Section 30 (1) Based on the assessment of the risk identified, the service provider shall determine – in its internal policy, specified in Section 65 (1) of the AML Act – the measures needed to manage the identified risk.

(2) The internal risk assessment report shall be approved by the service provider's executive officer or management body.

Section 31 (1) The service provider shall update its internal risk assessment by conducting periodic and ad-hoc reviews of the underlying information.

(2) The schedule of the review conducted by the service provider according to Subsection (1) shall be commensurate with the risk of money laundering and terrorist financing to the service provider.

(3) The service provider shall urgently review its internal risk assessment where

a) the nature of the risk is changed by an external effect,

b) a new type of risk of money laundering and terrorist financing arises,

c) such measure is required by a finding made by the MNB, in its capacity as public authority,

d) this follows from the service provider's own measure adopted for the mitigation of the risk,

e) new information emerges relating to the shareholders of the service provider, the members of its management body, the persons holding its key functions, or its organisation, and

f) in any other case, where the service provider has reasonable grounds to assume that the information underlying the risk assessment is no longer applicable.

8. Suspension of transactions

Section 32 (1) The service provider shall specify the information to be provided, and in its internal policy it shall lay down the duties and responsibilities of its organisational units in the event of a transaction being suspended.

(2) The information under Subsection (1) shall not imply either the fact of the transaction being suspended or the reason for the suspension.

(3) The service provider shall ensure that

a) the service provider's managers and employees who are aware of the fact of the suspension, proceed in accordance with the information under Subsection (1),

b) only the required organisational unit is involved in the implementation of the suspension,

c) in the event of any data, fact or circumstance emerging to imply the need to comply with the suspension obligation, the service provider has the means to notify by telephone the authority acting as the financial intelligence unit, and that in such an event, it would follow the instructions received from that authority, and

d) during the suspension, telephone contact with the authority acting as the financial intelligence unit is continuous even if the event of the designated person being prevented.

(4) Within the records maintained by it, the service provider shall handle the document, or its duplicate, that certifies the suspension of a transaction.

9. Operation of the internal control and information system

Section 33 For the purposes of this subheading:

1. *Automatic screening system:* information technology system that is capable of collating by applying money

laundering and terrorist financing criteria and based on pre-set parameters, without any human intervention required to screen customers and transactions

2. Manual screening: the application of money laundering and terrorist financing criteria to screen customers and transactions with human intervention required.

Section 34 (1) As part of the internal audit and information system, the service provider shall have a screening system, supporting the fulfilment of reporting, which ensures the identification of the customers and unusual transactions representing money laundering and terrorist financing risk and the provision of the data necessary for making the report (hereinafter: screening system).

(2) Service provider – with the exception specified in paragraph (3) – may apply a screening system based on manual screening.

(3) The service providers that

a) perform payment services, or

b) whose number of customers exceeded fifty thousand at the end of the year preceding the current year

shall operate an automatic screening system.

Section 35 (1) The service provider shall prepare an internal policy on the operation of the screening system, and the procedure of assessing customers and transactions included in the hit list.

(2) The internal rules of procedure under Subsection (1) shall be put down in writing, kept up-to-date and made available to the competent supervisory authorities by the service provider.

(3) The internal rules procedures of the screening system shall meet the following minimum requirements:

a) It shall be based on the institution's internal risk assessment;

b) It shall comply with the related internal policies of the service provider;

c) It documents the scenarios used by the service provider, including the underlying logic, parameters and thresholds and ensures the traceability of changes;

d) It ensures the integrity and quality of the data, so that accurate and complete data pass through the screening system;

e) it records the data sources containing the relevant data;

f) It ensures the availability of qualified employees or external consultants responsible for the design, operation, testing, putting into service and continued supervision of the screening system, as well as case management, supervision and the decisions adopted with respect to positive hits and potential reports;

g) it sets the time limits applied in the analysis and evaluation process;

h) It includes test protocols that describe in detail how the warnings generated by the screening system should be investigated and how to decide which of the positive hits should be reported, who is responsible for taking such decisions and how the decision-making process should be documented;

i) It provides for the review of the scenarios in line with the underlying logic, parameters and thresholds, and include who is responsible for the review, and

j) in the case of the automatic screening system, it provides for testing to monitor the complete process of the screening system and before and after its introduction, as well as for the performance of periodic testing related to control, data mapping, identification of transactions, search scenarios and logic, the screening modelling and the assessment of the data entered and the results.

Section 36 (1) The service provider shall perform screening for at least the following customer or transaction types and ensure it in its internal risk assessment:

a) cash deposited for a natural person customer in an amount reaching or exceeding twenty-five million forints,

b) cash deposited in an amount reaching or exceeding fifty million forints for a customer that is a legal person or an entity without legal personality,

c) cash paid to a natural person customer in an amount reaching or exceeding twenty-five million forints,

d) cash payment in an amount reaching or exceeding fifty million forints for a customer that is a legal person or an entity without legal personality,

e) transactions reaching or exceeding twenty-five million forints originated in or forwarded to a third country involving strategic deficiencies and high risk,

f)-g)[1]

(2) In addition to the provisions of Subsection (1), the service provider shall specify its screening criteria based on its own internal risk assessment.

(3) Based on its internal risk assessment, the service provider may replace the mandatory screening criteria specified in paragraph (1) by other screening, if it can prove to the supervisory authority that the screenings introduced by it are

[1] Effective from: 1 January 2021.

fully suitable for the management of the risks underlying the screenings specified in paragraph (1).

Section 37 (1) The service provider shall screen customers and transactions on a continuous basis. The service provider shall forthwith notify the MNB – in electronic form through the MNB's Electronic System for the Receipt of Authenticated Data (hereinafter: ERA System) – on obtaining knowledge of any circumstance hindering the continuity of the screening for more than twenty-four hours and on the measures it implemented or plans to implement to eliminate the problem.

In the case referred to in Section 24 (1) and Section 36 (1), the service provider shall analyse and evaluate the filtered client or transaction for money laundering and terrorist financing within twenty working days of screening, and in all other cases within thirty working days after screening. The date of screening shall not be counted in the above time limit.

(3) During the screening the service provider shall take into consideration the signals implying unusual transactions, developed based on its internal risk assessment.

(4) The analysis and assessment process for customers and transactions screened positive shall be documented by the service provider so that the result of the measure taken by the service provider, as well as the decision adopted on grounds of that result, may subsequently be reconstructed.

Section 38 (1) As part of the internal control and information system, the service provider shall operate an anonymous system for reporting abuse (hereinafter: "whistleblowing system").

(2) Persons may submit report on whistleblowing through the whistleblowing system, who are aware of that any provision of the AML Act is or has been violated at the service provider.

(3) The service provider shall investigate each report on whistleblowing within thirty days. The date of the report on whistleblowing shall not be counted within the above time limit.

(4) A person affected by the report shall be prohibited from participating in the investigation of the report on whistleblowing.

(5) Where the service provider finds that any data, fact or circumstance has emerged to imply the occurrence of money laundering, terrorist financing or that a thing has been derived from criminal activities, the designated person shall immediately submit a report to the financial intelligence unit.

(6) Where the service provider finds that reasonable grounds exist to suspect criminal activity, it shall immediately file a report with the investigating authority with the relevant powers and competence.

(7) Where in any case other than those provided for in Subsections (5) and (6), the service provider finds evidence of any violation of the provisions of the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests, or the provisions of this Decree, the designated person shall immediately notify the MNB of this fact.

(8) Following submission of the report, the service provider shall ensure that the report may not be accessed by anyone other than the person reporting and those involved in the investigation of the report.

Section 39 The service provider shall ensure that the internal control and information system is capable of screening business relationships by

a) personal data, prescribed by the AML Act
b) account number,
c) customer number,
d) a type of transaction, or
e) amount limit.

Section 40 The service provider shall ensure that the internal control and information system is capable of recording the data registered in it so that the data may be retrieved during the period provided for in the AML Act.

10. Development of a screening system for the implementation of restrictive measures imposed by the European Union and the United Nations Security Council (hereinafter: UNSC) relating to liquid assets and other financial interests, and the minimum requirements for the operation of the system

Section 41 For the purposes of this subheading:

1. *Automatic screening system:* information technology system that is capable of comparing the personal data of customers, beneficial owners, associates having the right of disposal, authorised representatives and proxies against the data of the persons specified in the legal acts of the EU and the resolutions of the UNSC on a continuous basis,

without any human intervention required,

2. *Manual screening:* procedure suitable for comparing the personal data of customers, beneficial owners, associates having the right of disposal, authorised representatives and proxies against the data of the persons specified in the legal acts of the EU and the resolutions of the UNSC, with human intervention required,

Section 42 The service provider shall possess and apply a screening system that ensures the immediate and comprehensive implementation of the legal acts and UNSC resolutions ordering financial restrictive measures (hereinafter: sanction-based screening system).

Section 43 Within the framework of the sanction-based screening system, the service provider shall apply automatic screening, if at the end of the year preceding the current year the number of its customers exceeded one thousand; in other cases the service providers may ensure the immediate and comprehensive implementation of the legal acts and UNSC resolutions ordering financial restrictive measures also by means of manual screening.

Section 44 (1) The service provider shall draw up internal rules of procedure on the operation of the sanction screening system and the analysis and evaluation of customers screened positive, beneficial owners, agents, proxies and representatives, as well as the transactions.

(2) The internal rules of procedure defined in Subsection (1) shall be documented, kept up-to-date and made available by the service provider to the competent authorities in exercising their licensing and regulatory activities.

(3) The internal rules of procedures of the sanction screening system shall meet the following minimum conditions:

a) it documents the search logic used by the service provider and the underlying assumptions and parameters,

b) it ensures the integrity and quality of the data, so that accurate and complete data pass through the screening system,

c) it records the data sources containing the relevant data,

d) it ensures the availability of qualified employees or external consultants responsible for the design, operation, testing, putting into service and continued supervision of the sanction screening system, as well as case management, supervision and the decisions adopted with respect to positive hits and potential reports,

e) it sets the time limits applied in the analysis and evaluation process,

f) It includes test protocols that describe in detail how the warnings generated by the sanction screening system should be investigated and how to decide which of the positive hits should be reported, who is responsible for taking such decisions and how the decision-making process should be documented,

g) it ensures the continuous monitoring of the screening logic and the underlying rules and parameters, and

h) the automatic screening system provides for testing to monitor the complete process of the sanction screening system and before and after its introduction, as well as for the performance of periodic testing related to control, data mapping, identification of transactions, search scenarios and logic, the screening modelling and the assessment of the data entered and the results,

Section 45 (1) The service provider shall continuously screen customers and transactions for restrictive measures imposed by the EU and the UNSC relating to liquid assets and other financial interests. The service provider shall forthwith notify the MNB – in electronic form through the ERA System – on obtaining knowledge of any circumstances hindering the continuity of the screening for more than twenty-four hours and on the measures it implemented or plans to implement to eliminate the problem.

(2) The service provider shall analyse and assess the screening hits.

(3) The analysis and assessment process for screened positive hits shall be documented by the service provider so that the result of the measure taken by the service provider, as well as the decision adopted on grounds of that result, may subsequently be reconstructed.

11. Training programme

Section 46 (1) Before employing him in that job or within 30 days of employment, the service provider shall provide general administrator training, and shall subsequently provide further training at least annually after the year of hiring (hereinafter collectively: general administrator training) to its managers and employees engaged in any activity associated with the prevention and combating of money laundering and terrorist financing and with the financial restrictive measures imposed by the European Union and the UNSC. A written exam organised by the service provider, including the exam carried out in its electronic systems, shall form part of the training.

(2) Any employee may participate in the fulfilment of the activity related to the prevention and combating money laundering and terrorist financing, and to the financial restrictive measures ordered by the European Union and the UNSC only under the supervision of a staff member who has successfully passed the exam related to the training specified in paragraph (1) until such time as he successfully passes the exam organised by the service provider on the curriculum of the prevention training.

(3) The service provider may engage only persons to hold the training, who

a) are holding relevant higher qualification, in particular, in law, economics, finance or IT, and

b) at least three years' experience

ba) gained in an area attending to internal audit or compliance duties at service providers falling within the scope of the AML Act, or

bb) in the area of attending to supervisory functions falling within the scope of the AML Act at supervisory bodies defined by the AML Act.

(4) The service provider shall compile a training programme of the depth necessary for filling certain positions; the training programme shall contain the topics necessary for filling the individual positions.

(5) The service provider shall retain the training curriculum and the material of the related exams, the dates and the participants of the trainings, the solutions of the exams, the list of examinees, and the exam results by examinees in a retrievable manner for 5 years from the date of the exam.

(6) The manager of the service provider, specified by Section 63(5) of the AML Act, shall be responsible for elaborating the training programme, the organisation of the prevention training in due course, ensuring the participation of the employees in the training, the recording of the data specified in paragraph (5) in a retrievable manner and for the verification of compliance with the provisions of paragraph (2).

(7) Upon elaborating the group policies and procedures, the service provider shall take into consideration the provisions of paragraphs (1)-(6).

CHAPTER VI

FINAL PROVISIONS

Section 47 (1) With the exception stated in Subsection (2), this Decree shall enter into force on 1 October 2020.

(2) Points *f) and g)* of Section 36 (1) shall enter into force on 1 January 2021.

(3) MNB Decree 45/2018. (IV. 17.) on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid Assets and Other Financial Interests shall be repealed.

---->>----->>--<<-----<<----