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

Pursuant to the authorisation granted under Section 77 (3) *d)* of Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing, 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:

1. General provisions

Section 1 The scope of this Decree shall apply to service providers within the meaning of Section 1 (1) *a)* to *e)* and *m)* and Section 1 (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").

Section 2 This Decree shall apply to customer due diligence measures performed by the service provider or outsourced customer due diligence measures performed by way of an audited electronic means of communication.

Section 3 (1) For the purposes of this Decree:

1. '*audited electronic means of communication*' shall mean an audited electronic system with facilities for performing due diligence procedures via electronic channels, for making customer statements, for the reading and interpretation of customer statements, for the safe storage of such statements and for the retrieval and verification of the stored data;

2. *'biometric data'* shall mean a concept as defined in Article 4 (14) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

3. *'electronic customer identification and declaration system'* shall mean a personalised regime for electronic procedures designed for making a legal statement with facilities for the clear identification of the person making the statement and the time when it was made, and for retrieving the information contained in the legal statement in unaltered form;

4. *'electronic customer due diligence'* shall mean customer due diligence measures performed on a customer who is physically remote from the service provider, by way of an audited electronic means of communication;

5. *'strong customer authentication'* shall mean authentication based on the use of two or more elements categorised as:

a) knowledge (something only the customer knows),

b) possession (something only the customer possesses), and

c) inherence (something the customer is),

that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

6. *'ICT and security risk'* shall mean the risk of loss resulting from breaches of confidentiality, damage to the integrity of systems and data, the inadequacy or unavailability of systems and data, or the inability (lack of agility) to change information technology within a reasonable time and at a reasonable cost in response to changes in environmental or business requirements, including security risks resulting from inadequate or malfunctioning internal processes or external events, also including cyber-attacks or inadequate physical security;

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

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

9. *'fraudulent transaction'* shall mean any payment transaction specified in Act LXXXV of 2009 on the Provision of Payment Services, excluding card-based payment transactions, where there are reasonable grounds to suspect fraud, in that the payment transaction was not intended to be authorised by the customer or was authorised by a customer in error.

(2) The provisions of this Decree relating to the customer shall also apply to the customer's agent, nominee and representative interacting with the customer's service provider.

2. Assessment prior to the introduction of an audited electronic means of communication for electronic customer due diligence

Section 4 (1) Unless otherwise provided for by law, prior to the introduction of a new audited electronic means of communication, the service provider shall consider the justification for the introduction of the audited electronic means of communication and perform a preliminary assessment of the audited electronic means of communication.

(2) The preliminary assessment shall cover at least the following:

a) the completeness and accuracy of the data and documents to be collected through the audited electronic means of communication and the reliability and independence of the information sources used;

b) the impact of the use of the audited electronic means of communication on the risks to the service provider as a whole, including technological, operational, reputational and legal risks related to money laundering and terrorist financing;

c) the substantive risk mitigation measures for all risks identified in the assessment specified in paragraph *b)* and the identification of corrective actions, responsible parties and timelines;

d) tests to assess the risks of the fraudulent transaction, including those related to the misuse of identity or authentication data and other ICT and security risks, which

da) may be conducted by independent testers who have the knowledge, skills and expertise in testing information security measures as defined in Section 14 *f)* and who are not involved in the development of information security measures,

db) include vulnerability scans and penetration tests, including threat-based penetration tests where necessary and appropriate, commensurate with the identified level of risk to business processes and systems, and

e) end-to-end testing of its operation for customers, products and services as defined in the electronic customer due diligence policy.

Section 5 At the request of the Magyar Nemzeti Bank (hereinafter referred to as "MNB"), the service provider shall certify that it has performed a preliminary assessment prior to the introduction of the audited electronic means of communication. As part of this process, the service provider shall

present to the MNB the results of the assessment and whether the use of the solution is appropriate for the identified money laundering and terrorist financing risks in relation to the type of customer, service, geographical feature and product concerned.

Section 6 The service provider may only use an audited electronic means of communication if, based on the prior assessment pursuant to Section 5, it is satisfied that said means can be integrated into its internal control system and that the service provider is able to adequately manage the risks arising from the use of the audited electronic means of communication in relation to money laundering and terrorist financing.

3. Electronic customer due diligence policy

Section 7 (1) In the case of electronic customer due diligence, the service provider shall draw up a risk-sensitive electronic customer due diligence policy and procedure (hereinafter jointly referred to as "electronic customer due diligence policy"), which shall contain the rules for the performance of electronic customer due diligence by means of all audited electronic means of communications used by the service provider, in order to identify the customer, verify the identity of the customer, and to perform an assessment and obtain information on the purpose and intended nature of the business relationship. The electronic customer due diligence policy may, at the service provider's discretion, also form part of its internal policy pursuant to Section 65 (1) of the AML Act.

(2) The electronic customer due diligence policy shall include at least the following:

1. a general description, characteristics and operation of the audited electronic means of communication implemented for the collection, verification and recording of information during the electronic customer due diligence procedure;

2. the situations in which the audited electronic means of communication may be used, including a description of the categories of customers, products and services that may be subject to customer due diligence via the audited electronic means of communication, taking into account the risk factors associated with customers, countries or geographical areas, products, services, transactions and delivery channels, as well as the risk factors identified and assessed in the service provider's risk assessment;

3. a description of which steps are fully automated, which steps require human intervention and to what extent, and the procedure for intervention;

4. control mechanisms to ensure that the first transaction with the customer is only executed by the service provider once all mandatory customer due diligence measures have been completed;

5. mandating induction and regular training programmes to ensure that the service provider's employees have up-to-date knowledge regarding the operation of the audited electronic means of communication, the associated risks and the measures to mitigate such risks;

6. the scope, frequency, steps and record keeping requirements for the assessment of the audited electronic means of communication;

7. the steps taken to continuously ensure the quality, completeness, accuracy and adequacy of the data collected through the audited electronic means of communication, which should be proportionate to the risks to the service provider related to money laundering and terrorist financing;

8. the scope and frequency of periodic reviews of the audited electronic means of communication;

9. the circumstances giving rise to ad hoc reviews, subject to the provisions of Section 9 (2);

10. corrective measures to eliminate any risk or error affecting the efficiency and effectiveness of the customer due diligence performed by means of the audited electronic means of communication, subject to the provisions of Section 10;

11. the scope of the information necessary to identify the customer, the types of documents, data or information which the service provider uses to verify the identity of the customer and the means of verifying that information;

12. the scope of information required to identify the customer, to verify their identity and to assess and obtain information on the purpose and intended nature of the business relationship;

13. the scope of information that the customer manually enters in the online interface, including its verification, and that is automatically recorded by the service provider on the basis of documents provided by the customer, as well as information that the service provider collects from other internal or external sources;

14. the rules on which categories of legal entities may be subject to customer due diligence via the audited electronic means of communication, taking into account the level of money laundering and terrorist financing risks associated with each category and the level of human intervention required to validate the identifying information;

15. the rules applied when establishing a business relationship that specify how they modify their own documentation templates, what documents they accept and what control mechanisms they have in place to verify those documents, and

16. the list and rules of the functions and activities of outsourced customer due diligence.

(3) The electronic customer due diligence policy shall be suitable to enable the service provider to comply with the requirements of this Decree.

Section 8 (1) The compliance manager of the service provider designated pursuant to Section 63 (5) of the AML Act shall, as part of his/her general responsibility for the development of policies and procedures for compliance with customer due diligence requirements, ensure that the service provider implements the electronic customer due diligence policy effectively, reviews and updates it regularly, in the event of a material change in the legal, internal regulatory or application environment, technology or workflow, but at least annually.

(2) The service provider's management body shall approve the electronic customer due diligence policy and, through the designated accountable manager, supervise its implementation.

4. Ongoing monitoring of electronic customer due diligence

Section 9 (1) The service provider shall continuously monitor – through regular and ad hoc reviews – all audited electronic means of communication used by it, in the interests of ensuring operation in accordance with its internal policy and the requirements of the legislation.

(2) The service provider shall perform ad hoc reviews at least in the following cases:

a) changes in the service provider's exposure to money laundering and terrorist financing risks,

b) any deficiencies in the operation of the audited electronic means of communication identified by the monitoring, audit, external audit function or during supervisory activities,

c) a noticeable increase in attempts at fraud, and

d) changes in the legal or other regulatory framework.

Section 10 (1) The service provider shall have a corrective action plan in case a risk arises or an error is detected that affects the efficiency and effectiveness of the electronic customer due diligence performed by way of the audited electronic means of communication.

(2) The corrective measures shall include at least the following:

a) reviewing all relevant business relationships to assess whether the service provider has applied an appropriate level of customer due diligence to comply with the legal provisions on identity

verification, identification of the beneficial owner and disclosure of the purpose and nature of the business relationship, with particular attention to those where the risk of money laundering and terrorist financing is highest, and

b) taking into account the information obtained in the review specified in paragraph *(a)*, assessing whether the business relationship concerned requires

ba) additional customer due diligence measures,

bb) application of the restrictions set out in the internal regulations pursuant to Section 65 of the AML Act,

bc) termination of the business relationship,

bd) reporting to the Financial Intelligence Unit, and

be) a change to the customer's risk category classification.

Section 11 (1) The service provider shall ensure that the most effective method is used to monitor the ongoing compliance and reliability of the audited electronic means of communication.

(2) To comply with paragraph (1), the service provider shall, in addition to automated critical alerts and notifications, use at least one of the following methods:

a) quality assurance testing,

b) external audit function,

c) regular, automated quality reports,

d) sampling-based testing,

e) manual review.

Section 12 The service provider shall keep records of the review and corrective measures and, at the request of the MNB, shall demonstrate which reviews and corrective measures it has carried out to address the deficiencies identified during the entire period of use of the audited electronic means of communication used by it.

5. Minimum requirements for audited electronic means of communication and their operation, and means of auditing

Section 13 An electronic means of communication may be audited and operated if it meets at least the following IT security requirements:

a) its components can be identified and documented,

b) its operational procedures are regulated, documented and audited at the frequency prescribed in the rules of operation,

c) its change management processes ensure that changes to the system's parameterisation and software code are only carried out in a tested and documented manner,

d) its data backup and recovery regime ensures that the system is safely restored and that the backup–recovery sequence is tested with the frequency and documented in accordance with the rules of operation,

e) user access at both application and infrastructure level is controlled, documented and monitored at the frequency specified in the rules of operation,

f) end-user access authorisations are set up as a single, closed system, ensuring the identification process is carried out, and the activity of its users is logged, with automatic alerts generated for extraordinary events,

g) privileged access authorisations are controlled, documented and monitored at the frequency specified in the rules of operation, activities performed with privileged access rights are logged, the integrity of log files is ensured and automatic alerts are generated for critical extraordinary events,

h) remote access is controlled, documented and monitored at the frequency specified in the rules of operation,

i) protection against viruses and other malicious code and acts is provided,

j) its data communications and system connections are documented and controlled, and the confidentiality, integrity and authenticity of data communications are ensured,

k) the disaster recovery plan is regularly tested,

l) its maintenance is regulated,

m) the protection of its data media is regulated and it is ensured that access to data media is restricted to authorised persons and only for the purpose of the processing, and that this is regularly reviewed and verified,

n) its own control mechanisms and the rules of operation ensure the integrity and protection of the system components and the information processed, and

o) an appropriate level of physical protection, a segregated environment and the detection and management of individual security incidents is ensured.

Section 14 In relation to the audited electronic means of communication, the service provider shall ensure that:

a) the transmission of data over the electronic transmission channel established with the customer is adequately secure, encrypted, confidential, intact and authentic,

b) the customer is informed of the terms and conditions of use of the service, including details on the customer-side responsibility for the security of the service and on data processing,

c) where human intervention is required, the service provider-side customer due diligence is performed only to the extent necessary and only by persons who, depending on the solution used by the service provider, have received the legal, technical and security training necessary to perform direct or indirect electronic customer due diligence,

d) it holds an audit report on the electronic means of communication and the electronic customer due diligence procedure which demonstrates that the IT protection of such is proportionate to the security risks and in particular meets the requirements set out in Section 13,

e) the audit report specified in point *d)* is revised in the event of a relevant change in legislation, the technology used or the business process that has an impact on the operation of the means of communication, but at least every two years,

f) the audit report specified in point *d)* is issued by an organisation registered in a Member State of the European Economic Area, where the person verifiably participating in the audit holds at least the following qualification and rating:

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

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

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

g) it makes available for, and transfers to, the data subject the personal data and data that do not qualify as personal data obtained by the service provider in the course of electronic customer due diligence during the period of processing, and

h) electronically stored data on the electronic customer due diligence procedure are recorded in a manner that can be used for subsequent verification of compliance with the customer due diligence provisions and the implementation of customer due diligence measures.

Section 15 Where the service provider uses functions suitable for automatic reading of information from documents, it shall ensure that these devices record information accurately and consistently.

Section 16 The service provider shall fully identify and manage the ICT and security risks related to the use of the electronic customer due diligence procedure, including in cases where the service provider outsources all or part of the electronic customer due diligence.

Section 17 If the service provider uses a multi-purpose device to perform the electronic customer due diligence procedure, the service provider shall ensure, in proportion to the risks, that the application or software code is run in a secure environment on the multi-purpose device. The service provider shall implement additional security measures to ensure the security and reliability of the application or software code and the data collected.

Section 18 The audited electronic means of communication must be capable of receiving all data, documentation and information concerning the customer pursuant to Sections 7-10 of the AML Act, and in the case of an automated solution, also of processing and verifying the information, except for documents that the customer may submit in the electronic customer identification and declaration system of the service provider.

6. Common rules for electronic customer due diligence

Section 19 (1) In the course of electronic customer due diligence, the service provider shall perform customer identification and identity verification pursuant to the AML Act, shall invite the customer to make the declarations and present the documents applicable to the customer pursuant to the AML Act, and shall furthermore assess the purpose and intended nature of the business relationship, and obtain supporting information for this purpose in justified cases.

(2) The service provider shall set up its electronic customer due diligence regime in accordance with the rights of disabled persons as set out in the Act on the Rights and Equal Opportunities of Persons with Disabilities.

(3) The service provider shall verify compliance with the requirements for electronic customer due diligence by the employee specified in the electronic customer due diligence policy, in the manner specified in the electronic customer due diligence policy. The verification and regulation shall also cover compliance with the requirements for recording the session.

Section 20 (1) The service provider may perform electronic customer due diligence by direct or indirect electronic means.

(2) In the case of the use of an audited electronic means of communication, if the service provider obtains beneficial owners' declarations and politically exposed persons' declarations, copies of documents, customer due diligence questionnaires and declarations on the source of funds or assets using its electronic customer identification and declaration system, no transaction may be executed until these declarations and copies of documents have been obtained and all customer due diligence measures to be performed on the basis of the customer's specific risk classification have been taken.

(3) The restriction specified in paragraph (2) shall not apply if the sending of a copy of the document is necessary for a customer who has already been fully vetted due to an exchange of documents or change of data.

Section 21 The service provider shall verify and ensure that

a) the information obtained through the audited electronic means of communication is up-to-date and complies with the requirements set out in Section 12 of the AML Act, and

b) the images, sound and video and audio recordings and data are recorded in a readable format and in sufficient quality to enable the customer to be clearly identified.

Section 22 The documents and information collected during the electronic customer due diligence shall be time-stamped and stored securely by the service provider. The service provider shall ensure that the content of the stored records is available in a readable format and allows for subsequent verification.

Section 23 (1) The service provider shall put in place appropriate mechanisms to ensure the reliability of the information collected automatically.

(2) The service provider shall ensure that control mechanisms are in place to manage the associated risks, including risks related to the automatic recording of data, including risks related to interference with the location of the customer's device or the use of fake IP addresses, virtual private networks (VPNs) or other similar services.

Section 24 (1) Where the service provider verifies the identity of a natural person customer using biometric data, it shall ensure that the biometric data are sufficiently unique to be unambiguously linked to a single natural person.

(2) The service provider shall use algorithms to verify whether the biometric data provided on the identity document submitted actually belong to the natural person customer concerned. The service provider shall also define additional control mechanisms to verify the biometric data provided on the identity document submitted, using a risk-sensitive approach.

Section 25 The service provider shall, on the basis of a risk-sensitive approach, apply at least one of the following control mechanisms or other similar measures to enhance the reliability of the control process:

a) the first payment is made to an account (whether solely or jointly owned) in the name of the customer held with a regulated credit or financial institution in the European Union or in a third country that applies requirements equivalent to or more stringent than those laid down in Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC;

b) sending of a one-time use and time-limited randomly generated identification code to the customer to confirm presence during the remote verification process, and returning of the code by the customer in the communication format chosen by the service provider;

c) collecting biometric data for comparison with data collected from other independent and reliable public sources;

d) maintaining contact with the customer by telephone;

e) sending of direct mail – electronic and postal – to the customer.

7. Rules for outsourcing electronic customer due diligence

Section 26 (1) Prior to outsourcing electronic customer due diligence or a part thereof, the service provider shall ensure that

a) the processes and procedures of the party performing the outsourced activities for electronic customer due diligence in relation to the audited electronic means of communication and the information and data collected in this context are sufficient and comply with the requirements laid down in the legislation,

b) the party performing the outsourced activities is able to ensure the continuity of business relationships between the customer and the service providers to protect against events that may reveal deficiencies in the electronic customer due diligence procedure using the outsourced electronic means of communication audited by the party performing the outsourced activities, and

c) the audited electronic means of communication operated by the party performing the outsourced activities complies with the requirements laid down in this Decree and there is a valid audit report in accordance with this Decree at all times.

(2) The service provider shall ensure that outsourcing does not result in the transfer of decision-making powers in relation to the establishment of the business relationship.

Section 27 (1) Before and during the outsourcing of the electronic customer due diligence procedure or a part thereof, on the basis of a risk-sensitivity approach, the service provider shall

a) ensure that the party performing the outsourced activities effectively implements and complies with the service provider's internal policy on electronic customer due diligence in accordance with the outsourcing agreement, by requiring regular reporting, ongoing monitoring, on-site inspections or sampling checks,

b) conduct assessments related to staff training, technological competence and data governance to ensure that the party performing the outsourced activities has the appropriate personnel and facilities to perform the electronic customer due diligence procedure or sub-process, and

c) ensure that the party performing the outsourced activities informs the service provider in advance of any proposed changes to the electronic customer due diligence procedure.

(2) The service provider shall ensure that the outsourcing agreement contains the arrangements for the execution of data protection requests relating to the exercise of the data subject's rights.

Section 28 In the event that the party performing the outsourced activities stores data relating to the customer, including image and sound recordings and documents, during the electronic customer due diligence procedure, the service provider shall ensure that

a) the party performing the outsourced activities collects and stores only the necessary customer data, in accordance with the data retention period set out in Sections 56-58 of the AML Act,

b) access to the data is strictly limited and recorded, and

c) the party performing the outsourced activities takes appropriate security measures to ensure the protection of the data stored.

8. Modes and rules for indirect electronic customer due diligence

Section 29 (1) The service provider shall perform indirect electronic customer due diligence by means of a device

a) that is capable of establishing that the customer to be vetted who appears at the remote location is a real, live person, is using the audited electronic means of communication in real time in person, and that the live feed is not manipulated, and

b) that is capable of comparing the photograph taken of the customer during the customer due diligence and the facial image in the document used for the due diligence in such a way that it can be established beyond doubt that the person portrayed in the official identity document is the same as the person featured in the photograph.

(2) In the case of the use of indirect electronic customer due diligence, the service provider shall ensure the conditions for customer due diligence for the audited electronic means of communication, provided

a) the customer has been made fully aware of the terms and conditions of the indirect electronic customer due diligence and has given his or her explicit consent thereunto,

b) strong customer authentication is used,

c) the image resolution and the illumination of the electronic means of communication enabling transmission of the image make it possible to recognise the gender, age and facial features of the customer and to compare them with the photo identification document presented by the customer, to identify the security features of the identity document presented, and

d) the customer due diligence procedure is regulated and continuously monitored as set out in the service provider's internal policy.

Section 30 (1) The service provider shall record the entire workflow between the service provider and the customer during the indirect electronic customer due diligence, the customer's provision with detailed information on the indirect electronic customer due diligence and the customer's explicit consent to the indirect electronic customer due diligence in a retrievable manner.

(2) For the purposes of indirect electronic customer due diligence, the service provider shall

a) ensure that a photograph of the customer is taken in which his or her face can be recognised and recorded,

b) ascertain that the customer is a real, live person, is using the audited electronic means of communication in real time in person and that the live feed is not manipulated, and

c) record the documents used for customer due diligence in such a way that the security elements and data series contained therein can be identified and stored.

(3) The service provider performing the indirect electronic customer due diligence shall ensure that the official identity document used is suitable for performing the indirect electronic customer due diligence, such that

a) the various elements of the official document suitable for identification purposes and their respective positions comply with the requirements of the authority issuing the official document suitable for identification purposes, and

b) the individual security elements, in particular the hologram, kinegram or equivalent security elements, are recognisable and uncompromised.

(4) The service provider shall ensure that

a) the customer's facial image is recognisable and identifiable with the facial image featured in the official document suitable for identification purposes presented by the customer, and

b) the identification data required by the AML Act have been fully obtained and the data contained in the official documents suitable for identification can be logically matched with the data on the customer held by the service provider.

Section 31 (1) During the indirect electronic customer due diligence procedure, the service provider shall compare the photograph taken of the customer and the facial image contained in the official document suitable for identification purposes using the audited electronic means of communication.

(2) In light of the result of all customer due diligence measures required by the AML Act, taken based on the customer's specific risk classification, the service provider shall send the customer a notification of the result of the customer due diligence within 2 banking days of the recording of the data.

Section 32 (1) The service provider shall not perform indirect electronic customer due diligence if

a) the customer withdraws his or her consent to the recording of data or to the performance of indirect electronic customer due diligence during the customer due diligence,

b) the physical and data content requirements applying to the official document suitable for identification purposes presented by the customer do not meet the conditions set out in Section 30 (3),

c) the conditions for visual identification of the official document suitable for identification purposes presented by the customer are not met,

d) the service provider is unable to take the photograph or to record the session specified in Section 30 (1),

e) a discrepancy or uncertainty is encountered during the course of the customer due diligence, or

f) the identification process cannot be continued because technical failures or unexpected connection disruptions are detected.

(2) The service provider shall immediately perform customer due diligence in the customer's physical presence or shall perform direct electronic customer due diligence where there is a risk of money laundering or terrorist financing occurring in relation to the customer's activities, and the customer cooperates in the implementation of the customer due diligence in the changed manner, and the service provider does not thereby breach the prohibition of disclosure.

Section 33 (1) The service provider shall perform indirect electronic customer due diligence

a) by using the Central Authentication Agent (hereinafter referred to as "CAA service"),

b) by way of reading the authentic natural identification data enabling customer identification from the official document suitable for identification purposes containing an electronic storage module,

c) by using eIdentification pursuant to Section 46 (1) *a)* of Act CIII of 2023 on the Digital Government and Certain Rules for the Provision of Digital Services (hereinafter referred to as "Digital Services Act"), or

d) by other means, subject to the limitation specified in Section 38.

(2) The service provider shall perform indirect electronic customer due diligence by means of eIdentification pursuant to paragraph (1) *c)*, if the customer identifies him or herself by means of the electronic identification service pursuant to the Digital Services Act.

Section 34 In order to implement the electronic identification service provided for in Section 33 (1) *a)*, the service provider shall

a) connect to the CAA service via the audited electronic means of communication and use it to ensure that the customer identifies him or herself during the customer due diligence, and

b) verify the identity of the customer on the basis of the information received back from the CAA via its audited electronic means of communication.

Section 35 (1) The service provider shall perform indirect electronic customer due diligence in accordance with Section 33 (1) *b)*, if

a) from the official document suitable for identification purposes containing an electronic storage module presented by the customer, the service provider is able to electronically read, by means of the audited electronic means of communication, the authentic natural identity data of the customer, which are suitable for personal identification, and the photograph of the customer taken by the authority issuing the official document suitable for identification purposes, and compare them with the data provided by the customer and/or the data recorded and the photograph taken during the identification process, and

b) a comparison of the data and photographic images by an audited electronic means of communication establishes beyond reasonable doubt that the person identified in the official document suitable for identification purposes is the same person as the person identified in the photographic image taken during due diligence by the audited electronic means of communication,

and that the official document suitable for identification purposes was issued by a competent authority and that the data electronically stored and read are unaltered and authentic.

(2) In addition to the cases specified in Section 32, the service provider shall not perform customer due diligence, if during the due diligence process it is not possible to read all relevant data from the electronic storage module of the electronic personal identification document, there is doubt as to the authenticity of the official document suitable for identification purposes or the data read from the official document suitable for identification purposes, or the service provider is unable to establish the customer's identity beyond reasonable doubt on the basis of the data read.

Section 36 In the case of the application of indirect electronic customer due diligence as defined in Section 33 (1) *c)*, the requirements set out in the Digital Services Act and in legislation issued on the basis of the authorisation contained in the Digital Services Act shall prevail.

Section 37 In the cases specified in Sections 34 and 35, the service provider shall verify the validity of the official document suitable for identification purposes presented by the customer using the audited electronic means of communication, including in particular whether the official document suitable for identification purposes is invalid, has been withdrawn or invalidated, and whether it has been reported lost, stolen, destroyed, damaged, found or submitted to the competent authority.

Section 38 The service provider may perform indirect electronic customer due diligence pursuant to Section 33 (1) *d)*, if it monitors the customer's activity in an enhanced procedure for one year from the date of the establishment of the business relationship.

9. Rules for direct electronic customer due diligence

Section 39 (1) During direct electronic customer due diligence, by means of a device complying with the provisions of Section 29 (1), the service provider shall compare the photograph taken of the customer and the facial image contained in the official document suitable for identification purposes used for due diligence. Customer due diligence is appropriate, if it can be established beyond reasonable doubt that the person portrayed in the official document suitable for identification purposes is the same as the person featured in the photograph or video recording.

(2) The service provider shall perform direct electronic customer due diligence in a room that is suitable for this purpose.

(3) Direct electronic customer due diligence may only be performed by a manager and employee of the service provider who has attended a training course previously organised by the service provider for the performance of this activity, who has acquired during the training adequate knowledge of the recognition and prevention of the use of deception techniques related to customer due diligence by means of audited electronic means of communication and who has passed an examination following the training.

(4) In order to avoid collusion between the customer and the service provider's employee, the service provider shall ensure the random assignment of the participating employee for direct electronic customer due diligence processes.

Section 40 (1) The service provider shall prepare a question-and-answer guide delineating the successive steps of the direct electronic customer due diligence process and the actions expected of the employee. The guidelines provide guidance on how to observe and identify psychological factors and other characteristics that may indicate suspicious behaviour during direct electronic customer due diligence.

(2) The service provider shall ensure the conditions for customer due diligence in relation to the audited electronic means of communication, where

a) the customer has been made fully aware of the terms and conditions of the direct electronic customer due diligence and expressly consented to such, and has been informed of the data processing and acknowledged such,

b) the image resolution and the illumination of the electronic means of communication enabling the real-time transmission of images and sounds is suitable for the recognition of the gender, age, facial features of the customer, and

c) the customer due diligence procedure is regulated and continuously monitored.

Section 41 (1) The service provider shall record all communications between the service provider and the customer during direct electronic customer due diligence, the customer's provision with detailed information on direct electronic customer due diligence and the customer's explicit consent thereunto in a retrievable manner in video and audio recordings.

(2) During direct electronic customer due diligence, the service provider shall ensure that the customer

a) looks into the camera so that his or her facial image can be recognised and recorded,

b) clearly indicates the identifier of the official document suitable for identification purposes used for direct electronic customer due diligence, and

c) positions the official identity card used for direct electronic customer due diligence in such a way that the security elements and data sequences on the document can be recognised and recorded.

(3) The service provider performing direct electronic customer due diligence shall ensure that the official document suitable for identification purposes used for direct electronic customer due diligence is suitable for performing direct electronic customer due diligence, insofar as

a) the various elements of the official document suitable for identification purposes and their respective positions comply with the requirements of the authority issuing the official document suitable for identification purposes, and the relevant legal requirements,

b) the individual security elements, in particular the hologram, kinegram or equivalent security elements, are recognisable and uncompromised, and

c) the document identifier of the official document suitable for identification purposes is the same as the document identifier provided by the customer, is recognisable and uncompromised.

(4) The service provider performing direct electronic customer due diligence shall ensure that

a) the customer's facial image is recognisable and identifiable based on the facial image featured in the official document suitable for identification purposes presented by the customer, and

b) the data contained in the official document suitable for identification purposes can be logically matched with the data on the customer held by the service provider.

(5) The service provider shall verify the validity of the official document suitable for identification purposes presented by the customer, including in particular whether the official document suitable for identification purposes is invalid, has been withdrawn or invalidated, and whether it has been reported lost, stolen, destroyed, damaged, found or submitted to the competent authority.

(6) The service provider shall send the customer a randomly generated identification code consisting of an alphanumeric code, centrally generated, to an e-mail address or SMS mobile phone number suitable for customer identification, at the option of the service provider, which shall be returned by the customer to the service provider in the communication format chosen by the service provider before completion of the direct electronic customer due diligence.

Section 42 The service provider shall discontinue direct electronic customer due diligence if

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

b) the physical and data content requirements applying to the official document suitable for identification purposes presented by the customer do not meet the conditions set out in Section 41 (3),

c) the conditions for visual identification of the official document suitable for identification purposes presented by the customer are not met,

d) the service provider is unable to create the audio and video recording,

e) the customer does not return the identification code, returns it incomplete or returns it incorrectly,

f) the customer fails to make a declaration or the service provider notices that the customer is making the declaration under some influence, or

g) a discrepancy or uncertainty is encountered during customer due diligence.

10. Closing provisions

Section 43 (1) With the exception stated in paragraph (2), this Decree shall enter into force on 1 July 2024.

(2) Sub-heading 3 shall enter into force on 1 January 2025.

Section 44 (1) The service provider shall assess the extent to which its audited electronic means of communication already in use at the time of the entry into force of this Decree complies with the provisions of this Decree and shall apply measures to mitigate the relevant risks arising from the use of the audited electronic means of communication until full compliance is achieved.

(2) In performing the assessment specified in paragraph (1), the service provider shall take into account in particular whether the audited electronic means of communication used by it covers the following risks:

a) the risks associated with authentication and specific risk mitigation measures set out in the electronic customer due diligence policy, in particular with regard to risks related to identity theft,

b) the risk that the customer is not the same person as the person he or she claims to be, and

c) the risk of using lost, stolen, suspended, withdrawn or expired identity documents, including, where appropriate, means to detect and prevent identity fraud.

(3) In respect of an audited electronic means of communication already in use on the date of entry into force of this Decree, the service provider shall perform the assessment specified in paragraph (1) by 31 October 2024 and comply with the requirements of this Decree by 1 May 2025 at the latest.

TABLE OF CONTENTS