Pursuant to Article 18, paragraph 8, Article 19, paragraph 7 and Article 21, paragraph 7 of the Law on the Prevention of Money Laundering and Terrorism Financing (RS Official Gazette, Nos 113/2017, 91/2019, 153/2020, 92/2023, 94/2024 and 19/2025), and Article 15, paragraph 1 of the Law on the National Bank of Serbia (RS Official Gazette, Nos 72/2003, 55/2004, 85/2005 – other law, 44/2010, 76/2012, 106/2012, 14/2015, 40/2015 – CC decision, 44/2018 and 19/2025), the Executive Board of the National Bank of Serbia adopts the following

DECISION
ON CONDITIONS AND MANNER OF ESTABLISHING AND VERIFYING IDENTITY OF A NATURAL PERSON THROUGH MEANS OF ELECTRONIC COMMUNICATION

I INTRODUCTORY PROVISIONS

Subject matter

1. This Decision regulates the conditions and manner of establishing and verifying the identity of a customer who is a natural person, of a legal representative of that customer, of a customer who is an entrepreneur and of a natural person who is a representative of a customer that is a legal person – through means of electronic communication and without mandatory physical presence of the person who is being identified on the obliged entity's business premises (hereinafter: video identification).

Definitions

2. For the purposes of this Decision, the terms below shall mean as follows:

1) **obliged entity** means a person supervised by the National Bank of Serbia with regard to the implementation of the law governing the prevention of money laundering and terrorism financing, and includes a bank, voluntary pension fund management company, financial lessor, insurance undertaking, insurance brokerage undertaking, insurance agency undertaking and insurance agent with a licence to carry out life insurance business (except for agency undertakings and insurance agents for whose work the insurance undertaking is responsible in accordance with law), electronic money institution, payment institution, public postal operator and

digital asset service provider in the part of operations relating to virtual currencies;

2) **customer** means a natural person and entrepreneur who, in accordance with the law governing the prevention of money laundering and terrorism financing, carries out a transaction or establishes a business relationship with the obliged entity, a legal representative of a natural person who carries out a transaction or establishes a business relationship with the obliged entity on behalf of that person, and a natural person who is a representative of a legal person and who carries out a transaction or establishes a business relationship with the obliged entity on behalf of that legal person;

3) **means of electronic communication** are technical means and channels enabling the electronic transfer of data, image and/or sound between the customer and obliged entity in real time;

4) **personal document** means a valid document with a photo issued by the competent authority (e.g. an identity card or a passport);

5) **security elements** means elements of a personal document aimed at reducing the risk of counterfeiting or unauthorised changes to the document (e.g. microtext, optically variable ink, guilloche elements, diffractive optically variable element, relief elements, MLI zone).

Types of video identification

3. Video identification may be carried out as direct or indirect video identification.

Direct video identification means the procedure of establishing and verifying customer identity through means of electronic communication, with mandatory conversation between the employee at the obliged entity and the customer via video link, in real time.

Indirect video identification means the procedure of establishing and verifying customer identity through means of electronic communication, an integral part of which is a time-limited session in real time in which the customer participates using the obliged entity’s technical solution involving visual recording, but without conversation between the employee at the obliged entity and the customer in that procedure.

II CONDITIONS FOR CARRYING OUT THE VIDEO IDENTIFICATION PROCEDURE

Internal regulations

4. An obliged entity intending to offer customers the possibility of video identification shall regulate in more detail, by its internal regulations, the carrying out of the video identification procedure and the manner of implementing other provisions of this Decision, by the date of submission of the notification referred to in Section 30, paragraph 1 hereof.

The internal regulations referred to in paragraph 1 hereof shall define at least the following:

1) description of the video identification procedure, including all customer data collected in that procedure and the types of personal documents used to establish customer identity;
2) categories of customers whose identity is being established and/or verified in the video identification procedure, in accordance with this Decision and the obliged entity's risk assessment, as well as specific features of that procedure with regard to different customer categories and the obliged entity's products and services in relation to whose contracting the video identification procedure is carried out;
3) categories of customers whose identity may not be established and/or verified in the video identification procedure, in accordance with this Decision and the obliged entity's risk assessment;
4) parts of the video identification procedure which are fully automated and parts of the procedure requiring human intervention, and in particular the data obtained directly from the customer (orally and/or in writing), the data automatically retrieved from the personal document and/or other documentation submitted by the customer, as well as the data obtained in another manner (from internal or external sources);
5) manner in which the employee at the obliged entity supervises and verifies the indirect video identification procedure, including determination of the period from the completion of that procedure until notifying the customer about the establishment of the business relationship or the need to submit additional data and/or documents, as well as additional measures undertaken by the obliged entity towards the customer in accordance with Section 19, paragraphs 3 and 4 hereof;
6) allocation and segregation of duties, as well as duties and responsibilities relating to the carrying out of the video identification procedure;

7) description of the initial employee training programme at the obliged entity in accordance with this Decision, as well as regular training of employees, except for the training referred to in Section 5, paragraph 2, item 2) hereof;

8) guidelines referred to in Section 18, paragraph 5 hereof – if the obliged entity intends to carry out direct video identification;

9) manner of keeping the recorded material.

Within the meaning of the law governing the prevention of money laundering and terrorism financing, the authorised person at the obliged entity shall be responsible for the implementation and regular updating of the internal regulations referred to in this Section. The internal regulations referred to in this paragraph shall also be adopted by, and shall be the responsibility of, the obliged entity's senior management, which shall also supervise their implementation.

Employee training

5. Video identification may be carried out only by an employee at the obliged entity who has undergone special training for carrying out the video identification procedure (hereinafter: employee).

The obliged entity shall define the training programme referred to in paragraph 1 hereof, which shall include at least the following:

1) familiarisation with the provisions of the laws governing the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction, and the relevant secondary legislation adopted based on those laws, as well as with the provisions of the law governing personal data protection;

2) familiarisation with security elements and the manner of authenticating personal documents;

3) familiarisation with the manner of carrying out the video identification procedure in accordance with this Decision.

Video identification premises

6. The video identification procedure shall be carried out in a designated room at the obliged entity, physically separated from other premises. Access to the room where the video identification procedure is carried out shall be constantly controlled and restricted to employees with access permission, with mandatory video surveillance.

The room referred to in paragraph 1 hereof in the indirect video identification procedure means the room containing the technical and technological equipment and documentation enabling the carrying out of the video identification procedure.

Notwithstanding paragraph 2 hereof, if activities outsourced to a third party relate exclusively to the maintenance of the technical solution used by the obliged entity for carrying out the video identification procedure, without outsourcing activities relating to the carrying out of that procedure, the obliged entity shall ensure that the technical and technological equipment at that third party is used in a secure working environment and in compliance with the conditions from paragraph 1 hereof. The documentation generated in the video identification procedure referred to in this paragraph shall be maintained and kept electronically in accordance with regulations, and the obliged entity shall ensure that such documentation is protected against unauthorised access and available exclusively to authorised persons.

The outsourcing of implementation and maintenance of the technical solution used by the obliged entity for carrying out the video identification procedure shall also be subject to appropriate regulations governing operations of that obliged entity pertaining to outsourcing activities to third parties.

Technical solution

Characteristics of the technical solution

7. Video identification shall be carried out in real time and without interruption.

The obliged entity shall ensure a technical solution enabling real-time streaming of image and/or sound.

The technical solution referred to in paragraph 2 hereof shall also ensure a fully encrypted communication channel between the customer and obliged entity (end-to-end encryption), so that data during transmission cannot be intercepted, altered or made available to third parties in an unauthorised way. The technical solution referred to in this paragraph shall also use secure protocols and cryptographic algorithms in accordance with best practices, in order to ensure confidentiality, authenticity and integrity of exchanged data.

The technical solution referred to in paragraph 2 hereof shall also ensure high-quality image and sound streaming, connection to an accurate time source throughout the procedure, as well as uninterrupted recording of the entire video identification procedure. In the indirect video identification procedure, each obtained recording and/or photo shall contain data on the exact recording time, ensured through the use of a qualified electronic time stamp.

In the indirect video identification procedure, the obliged entity shall ensure reliable and verified technical solutions which, in addition to the conditions from paragraphs 1 to 4 hereof, also enable authentication of the customer's personal document, as well as liveness verification of the customer in real time.

The liveness verification referred to in paragraph 5 hereof means the process of determining whether the customer's biometric data used to establish and/or verify customer identity (e.g. a recording of the customer's face) originates from a live person directly present in real time during the establishment and/or verification of his identity. The liveness verification referred to in this paragraph may include a request for the customer to perform certain actions before the camera recording the customer's face, which the customer cannot predict in advance – e.g. a request to read a sequence of characters and/or words, or a request to follow an area randomly selected on the screen by moving the head, or a request to move the head in a specific direction (active liveness verification), or analysis of the customer's facial biometric characteristics without requiring the customer to take any action – e.g. analysis of facial micro-movements, skin texture, facial structure, light reflections and the like (passive liveness verification).

The provisions of the decision governing minimum information-communication system management standards for financial institutions and/or other obliged entity shall also apply to the technical solution referred to in this Section.

Prior assessment of the technical solution

8. The obliged entity shall carry out prior assessment of adequacy of the technical solution referred to in Section 7 hereof and shall regulate, by its internal regulations, the manner of assessing that solution and maintaining records of that assessment, which shall contain at least the following:

1) assessment of adequacy of that solution in terms of completeness and accuracy of the data and documents collected, as well as reliability and authenticity of the data sources used;

2) assessment of the impact of using that solution on risks in the obliged entity's overall operations, including risks of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction, risk of opening payment accounts used for receiving and transferring funds obtained through fraud and abuse related to the execution of payment transactions, operational risk including legal risk, information and communication system risk and security risks in the use of this solution, as well as compliance risk including reputational risk;

3) identification of risk mitigation measures, as well as activities aimed at remedying deficiencies relating to the risks referred to in item 2) hereof;

4) results of tests assessing fraud risk, including impersonation fraud risks and other risks relating to the obliged entity's information-communication system and security risks, in accordance with the decision governing minimum standards of managing the information-communication system of a financial institution and/or other obliged entity and this Decision;

5) results of end-to-end testing of the functioning of the solution in connection with the customers, products and services for which this procedure may be used in accordance with the internal regulations.

Monitoring implementation of the technical solution and internal controls

9. The obliged entity shall regularly monitor and verify implementation of the technical solution referred to in Section 7 hereof, in order to ensure its functioning in accordance with this Decision.

The obliged entity shall consider and document the most efficient manner of monitoring adequacy and reliability of implementation of the technical solution referred to in paragraph 1 hereof, and shall apply at least the following measures:

1) testing of image and sound quality, recordings, liveness verification, personal documents, etc.;

2) automatic alerts and notifications on operation of the technical solution;

3) regular automatic quality reports (number of successfully completed video sessions, number of technical failures, number of performance drops, etc.);

4) sample-based testing;

5) manual controls (system and operational records, security checks, recording verification and the like);

6) other measures deemed appropriate.

By its internal regulations referred to in Section 4, paragraph 1 hereof, the obliged entity shall also define at least the following:

1) manner of carrying out regular internal control of the quality, completeness, accuracy and adequacy of data collected during the video identification procedure, proportionate to the risk of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction to which the obliged entity is exposed, as well as the scope and frequency of such controls;

2) circumstances under which extraordinary and/or ad hoc controls of the data referred to in item 1) hereof shall be mandatorily carried out, including at least the following:

– changes in the obliged entity's exposure to the risk of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction,

– deficiencies in the functioning of the technical solution referred to in Section 7 hereof identified during internal controls, internal audit or supervision by the National Bank of Serbia,

– observed increase in attempted frauds in the video identification procedure,

– changes in the legal framework directly or indirectly affecting the video identification procedure or the obliged entity's operations (e.g. changes to regulations governing personal data protection, video identification, the obliged entity's operations or the product or service provided based on the carried out video identification procedure).

An obliged entity carrying out indirect video identification shall regulate, by its internal regulation, regular internal control of the carrying out of the indirect video identification procedure at least once a year.

The internal control referred to in paragraph 4 hereof shall involve a review of recordings of the indirect video identification procedure, based on a random sample, by the authorised person at the obliged entity within the meaning of the law governing the prevention of money laundering and terrorism financing or the deputy of that person.

The obliged entity shall, by the internal regulation referred to in paragraph 4 hereof, also define the conduct of the persons referred to in paragraph 5 hereof if it identifies irregularities in carrying out the indirect

video identification procedure during the internal control procedure, as well as the measures undertaken in that case in order to ensure compliance with this Decision as soon as possible.

Determining measures taken by the obliged entity to remedy deficiencies

10. The obliged entity shall define, by the internal regulations referred to in Section 4, paragraph 1 hereof, measures for remedying deficiencies if any of the risks materialised or if errors affecting the efficiency and effectiveness of the technical solution referred to in Section 7 hereof have been identified. These measures shall include at least the following:

1) verification of all business relationships affected by such risks and errors, in order to assess whether the obliged entity applied the necessary customer due diligence actions and measures upon establishing the business relationship, priority being given to those business relationships carrying the highest risk of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction;

2) taking into account the data and conclusions from the verification referred to in item 1) hereof, assessment of whether the business relationship referred to in that item should be:

– subject to additional customer due diligence actions and measures,

– subject to restrictions, such as restrictions on the transaction volume or the service provided (e.g. provision of service of payment account with basic features), until a final decision on the business relationship is made,

– terminated,

– reported to the Administration for the Prevention of Money Laundering,

– reclassified into another risk category.

Personal documents

11. Only personal documents containing security elements and a machine-readable zone may be used in the video identification procedure.

Customer risk category

12. An obliged entity may not establish and verify the identity of a customer and/or person in the video identification procedure in the following cases:

1) if the obliged entity previously classified the natural person, entrepreneur or legal person into the category of high risk of money laundering, terrorism financing or financing of the proliferation of weapons of mass destruction, based on the risk analysis developed in accordance with the regulations governing the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction;

2) if the legal person establishing a business relationship or carrying out a transaction is an off-shore legal person;

3) if there is an off-shore legal person in the ownership structure of a legal person establishing a business relationship or carrying out a transaction;

4) if a person establishing a business relationship or carrying out a transaction comes from a country with strategic deficiencies in its system for the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction;

5) if the customer belongs to a category of customers whose identity the obliged entity may not establish and verify in the video identification procedure and is not the customer referred to in items 1) to 4) hereof, which the obliged entity shall determine by its internal regulation, based on the risk assessment.

Customer consent

13. Prior to initiating the video identification procedure, the obliged entity shall obtain the customer's express consent to the entire video identification procedure, particularly to the processing of personal data in that procedure, as well as to the recording of image and/or sound and keeping the recorded material in accordance with law.

The consent referred to in paragraph 1 hereof shall relate to a specifically determined type of video identification referred to in Section 3 hereof and shall be recorded.

The obliged entity shall inform the customer in advance about the manner of carrying out the video identification procedure, the personal data processed in that procedure, the purpose and legal basis for processing such data, as well as the fact that the granting of consent referred to in paragraph 1 hereof will be recorded and kept.

III VIDEO IDENTIFICATION PROCEDURE

Authentication of the personal document

Verification of security elements and personal document data

14. In the video identification procedure, the obliged entity shall authenticate the personal document by verifying the security elements of that document and the data that such type of personal document should contain, namely:

1) customer data: name, surname, date and place of birth and unique master citizen number for nationals of the Republic of Serbia;
2) biometric customer data: a photo, fingerprint and/or signature;
3) personal document data: the number of the personal document, date of issuance with the validity period, place of issuance and the name of the issuer of the personal document;
4) data on permanent and/or temporary residence of the customer, unless such data can be established by an immediate (visual) inspection of the personal document, in which case such data shall be established in accordance with Section 24 hereof.

The obliged entity shall establish whether the layout of the data referred to in paragraph 1 hereof in the personal document, as well as the number, size and font of the characters correspond to that type of personal document. In particular, it shall verify whether the personal document number is correct (type, number and layout of characters, as well as the positioning in the personal document).

The validity period of the personal document shall correspond to the date of issuance and shall be determined in accordance with regulations.

The obliged entity shall also verify whether the personal document has been damaged and/or altered and whether the photo has been subsequently added (e.g. glued or fastened).

Authentication of the personal document in direct video identification

15. In the direct video identification procedure, verification of security elements of the personal document which may be visually recognised under light and/or when moving the document (e.g. optically variable ink, diffractive optically variable element, MLI zone) and which such type of personal document should contain, as well as the data referred to in

Section 14 hereof, shall be carried out by the employee trained in accordance with Section 5 hereof. For that purpose, the employee may ask the customer to show the personal document before the camera in a certain direction, to move the personal document and/or to cover a specific part of it by hand.

In the direct video identification procedure, the obliged entity may also use tested and verified technical solutions intended to assist the employee in authenticating the personal document, without prejudice to the obligations of the employee referred to in paragraph 1 hereof, as well as technical solutions enabling NFC (Near Field Communication) reading of personal documents if the customer's personal document contains an NFC chip.

Authentication of the personal document in indirect video identification

16. In the indirect video identification procedure, the authentication of the personal document shall be carried out using the technical solution referred to in Section 7 hereof, by means of which the security elements of that document and the data referred to in Section 14 hereof are verified, with mandatory supervision and verification by the employee in accordance with Section 19 hereof.

Establishing customer identity

Comparison with the photo from the personal document

17. Customer identity shall be established by comparing the customer's physical appearance with the photo from the personal document.

Comparison, conversation and assessment in direct video identification

18. In the direct video identification procedure, the employee shall compare the data from the personal document with the information provided by the customer during conversation. For that purpose, the employee may ask the customer to disclose some of the data contained in the personal document, which the customer would undoubtedly be expected to know (e.g. his date of birth).

The employee shall assess whether the customer's responses to the questions posed are convincing, sensible and consistent.

The conversation between the employee and the customer in the direct video identification procedure shall be conducted in Serbian. By way of exception, the conversation may also be conducted in English, provided that the employee holds a certificate proving knowledge of English at an advanced level (at least C1 level according to the Common European Framework of Reference for Languages), namely a certificate issued by an authorised foreign language teaching institution, a certificate of an accredited faculty of philology or an internationally recognised certificate.

Notwithstanding paragraph 3 hereof, the conversation between the employee and a deaf or hard-of-hearing customer may be conducted using sign language if the employee holds an appropriate certificate for the use of such language.

The obliged entity shall define, by its internal regulations, employee guidelines for customer conversation, in accordance with this Decision.

Comparison, assessment and verification in indirect video identification

19. In the indirect video identification procedure, for the purpose of establishing customer identity, the obliged entity shall ensure the following:

1) that all photos and/or video recordings in that procedure are taken under appropriate lighting conditions and with necessary clarity, in order to enable proper establishment of customer identity;
2) that all photos and/or video recordings are taken in real time, i.e. at the time of carrying out the customer identity establishment procedure, which shall be confirmed by data on the exact recording time through the use of a qualified electronic time stamp;
3) that the liveness verification referred to in Section 7, paragraph 5 hereof is carried out;
4) that the recorded photos and/or video recordings obtained during the verification referred to in item 3) hereof are compared with the photo from the customer’s personal document.

The establishment of customer identity referred to in paragraph 1 hereof shall be carried out with mandatory supervision and verification by an employee trained in accordance with Section 5 hereof. The supervision and verification referred to in this paragraph shall be carried out prior to establishing a business relationship with the customer and/or carrying out a transaction.

Notwithstanding paragraph 2 hereof, the supervision and verification by the employee referred to in that paragraph may also be carried out within 72 hours following the completion of the indirect video identification procedure and/or establishment of the business relationship with the customer, subject to the application of additional enhanced customer due diligence actions and measures during that period, including monitoring of the customer's transactions and limitation of the total amount of transactions that the customer may carry out during that period.

In order to prevent fraud and abuse, and in addition to all measures applied in accordance with this Decision and the regulations governing the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction, irrespective of the risk category assigned to the customer, the obliged entity shall undertake special additional measures towards the customer referred to in this Section also during the period of 30 days following the establishment of the business relationship, including monitoring of the customer's transactions and limitation of the total amount of transactions that the customer may carry out during that period.

Comparison with already obtained data

20. If the obliged entity already possesses certain customer data (e.g. the customer already uses certain services of the obliged entity), it shall compare such data with the data obtained during the video identification procedure.

Establishing the identity of the legal representative of a natural person

21. If a business relationship is established or a transaction carried out on behalf of a natural person by a legal representative, the identity of that legal representative may be established only in the direct video identification procedure.

In the procedure referred to in paragraph 1 hereof, the employee shall also establish the identity of the represented person in accordance with the regulations governing the prevention of money laundering and terrorism financing.

The employee shall request the customer – legal representative of the natural person to also show before the camera the personal document of the represented person and/or another official document used to

establish the identity of that person, as well as a public document proving the status of his legal representative.

The personal document referred to in paragraph 3 hereof shall meet the conditions from Section 11 hereof, and the employee shall authenticate it in accordance with Sections 14 and 15 hereof.

Customer identity verification

Manner of identity verification

22. The obliged entity shall ensure the verification of customer identity during the video identification procedure by using a one-time password (OTP) or by generating a security code within the obliged entity's application solution, if the customer already uses that solution, or by electronic signature or other methods of secure authentication.

The obliged entity shall submit the one-time password or security code referred to in paragraph 1 hereof to the customer using the phone number which the customer will use for communication with the obliged entity in connection with the business relationship established with that entity and/or the transaction performed in accordance with this Decision. The obliged entity shall submit the one-time password or security code to the customer – representative of a legal person using the phone number which that representative will use for communication with the obliged entity in connection with the business relationship established with that entity on behalf of the represented legal person and/or the transaction performed in accordance with this Decision. The obliged entity shall ensure that the validity period of the one-time password is limited to the period required for authentication of customer identity, and shall also determine the number of unsuccessful attempts to enter the one-time password or security code after which such code and/or password shall cease to be valid.

In addition to identity verification referred to in paragraphs 1 and 2 hereof, in the indirect video identification procedure the obliged entity may also undertake additional measures, such as making a phone or video call with the customer or delivering appropriate data directly to the customer's address specified in the personal document or to a verified email address.

The obliged entity shall ensure the existence and keeping of records on customer identity verification referred to in this Section, in accordance with the decision governing minimum information-communication system

management standards for financial institutions and/or other obliged entity and this Decision.

Condition for completion of the video identification procedure

23. The video identification procedure may be completed only if customer identity has been verified in accordance with Section 22 of this Decision.

Obtaining documents

24. Prior to establishing a business relationship and/or carrying out a transaction with a customer whose identity was established in accordance with this Decision, the obliged entity shall also obtain a copy of the personal document used by the customer in the procedure, as well as copies of the documents referred to in Section 21, paragraph 3 hereof, which it shall keep in accordance with law.

If it is not possible, based on the copy of the customer's personal document referred to in paragraph 1 hereof, to obtain data on the customer's permanent and/or temporary residence or other data prescribed by the law governing the prevention of money laundering and terrorism financing, the obliged entity shall also obtain a scan reading of the customer's personal document and/or a copy of another official document containing such data (e.g. a vehicle registration certificate or a property tax assessment decision), and if for objective reasons the missing data cannot be obtained in that manner either, such data shall be obtained directly from the customer.

Direct obtaining referred to in paragraph 2 hereof shall mean obtaining the data referred to in that paragraph orally during the direct video identification procedure and/or obtaining such data in writing during the indirect video identification procedure, together with the submission of a copy of the document or other proof confirming such data (e.g. a telephone or utility bill containing such data or a statement given by the customer under full financial and criminal liability) prior to establishing the business relationship and/or carrying out the transaction referred to in paragraph 1 hereof.

A copy and/or scan reading referred to in paragraphs 1 to 3 hereof shall also mean a digitised (e.g. scanned or photographed) document referred to in those paragraphs.

Recording the procedure and keeping the recording

25. The obliged entity shall ensure uninterrupted recording of the entire video identification procedure, including the customer's consent referred to in Section 13 of this Decision. The date and time of recording shall be visible throughout the recording.

The direct video identification procedure shall be recorded in the form of a video sound recording and, in addition to the date and time of recording, the faces of both the customer and the employee carrying out the video identification procedure shall be fully visible throughout the recording.

The recording referred to in paragraph 1 hereof shall form an integral part of the customer file and the obliged entity shall keep it in its system in the manner and within the deadlines prescribed by the laws governing the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction, and personal data protection, in the format enabling subsequent verification of that recording.

Procedure termination

26. The video identification procedure must be terminated in the following cases:

1) if it is not possible to ensure uninterrupted streaming of image and/or sound (e.g. due to a brief loss of image and/or sound or freezing of image) or high-quality streaming (e.g. the image is not sharp and clear, lighting is poor, colours are missing, lines and/or noise appear on the screen);
2) if the room in which the customer stays during the procedure is poorly lit or noisy, preventing the authentication of the personal document or identification of the customer, or if the voices of the customer and the employee during the direct video identification procedure cannot be clearly heard;
3) if, during the procedure, any doubt arises as to the authenticity of the personal document and/or identity of the customer;
4) if, due to other barriers in communication, image and/or sound streaming or due to other circumstances, the employee is unable to authenticate the personal document or identify the customer.

The identity of the customer who participated in the procedure terminated pursuant to paragraph 1 hereof shall be established by inspection of the customer's personal document, with the mandatory

physical presence of the customer at the obliged entity, in accordance with the law governing the prevention of money laundering and terrorism financing.

Notwithstanding paragraph 2 hereof, the identity of the customer referred to in that paragraph may also be established in a new video identification procedure, except in the case referred to in paragraph 1, item 3) hereof, but only if the previous procedure was terminated due to a circumstance which may be removed (e.g. technical issues) and only after such circumstance has been removed. A new procedure shall be carried out as if the previous procedure had not taken place, and the obliged entity shall again obtain the customer's consent in accordance with Section 13 of this Decision.

In accordance with the assessment of the risk of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction, the obliged entity shall determine by its internal regulations the maximum possible number of unsuccessful attempts to carry out the video identification procedure after which customer identity must be established in accordance with paragraph 2 hereof.

IV OUTSOURCING VIDEO IDENTIFICATION ACTIVITIES

Special conditions for outsourcing

27. If the obliged entity outsourced the establishment and verification of customer identity to a third party, in accordance with the provisions of the law governing the prevention of money laundering and terrorism financing relating to the outsourcing of certain customer due diligence actions and measures to a third party, such third party may establish and verify customer identity in the video identification procedure in accordance with this Decision, but only provided that such third party may also be subsumed under the definition of the obliged entity referred to in Section 2, item 1) of this Decision and that it is included in the list of obliged entities referred to in Section 30, paragraph 7 hereof.

The obliged entity referred to in paragraph 1 hereof shall, before and during the business relationship with the third party referred to in that paragraph, ensure the following in accordance with the risk assessment:

1) application by and conduct of the third party in accordance with the obliged entity's internal regulations relating to the implementation of the video identification procedure, as well as in accordance with the

outsourcing agreement, achieved through regular reporting, continuous monitoring, on-site inspections at the premises of the third party or sample testing;

2) carrying out an assessment to ensure that the third party is adequately equipped and capable of implementing the video identification procedure, which may include assessment of employee training, technological suitability and data management at the third party;

3) notification to the obliged entity of all proposed changes to the video identification procedure at the third party or of any modification to the technical solution.

Keeping data at the third party

28. If the third party referred to in Section 27 hereof keeps customer data, including photos, video recordings and/or documents obtained during the video identification procedure, the obliged entity shall also ensure the following:

1) that only the necessary customer data are collected and kept in a legible format in accordance with law;

2) that access to customer data is strictly restricted and that records exist of granted and revoked access rights to such data;

3) that appropriate security measures are applied to ensure the protection of customer data;

4) that the retention period for customer data is clearly determined;

5) that the conditions and manner of returning customer data to the obliged entity and securely deleting such data from the information-communication system of the third party are determined.

Relevant application of primary legislation on outsourcing

29. The outsourcing referred to in Section 27, paragraph 1 hereof shall also be subject to the relevant regulations governing the operations of the obliged entities referred to in that paragraph, insofar as such regulations relate to the outsourcing of activities to third parties.

V REPORTING TO AND SUPERVISION BY THE NATIONAL BANK OF SERBIA

Reporting to the National Bank of Serbia

30. An obliged entity intending to offer customers the possibility of video identification in accordance with this Decision shall notify the National Bank of Serbia thereof at least 30 days before the date of commencement

of offering such possibility and shall submit, along with that notification, documentation proving that the conditions for carrying out the video identification procedure laid down by this Decision are met, as follows:

1) internal regulations referred to in Section 4 hereof;
2) evidence that the obliged entity's employees who will carry out the video identification procedure are trained in accordance with Section 5 hereof;
3) the list of all countries (including the Republic of Serbia) – issuers of personal documents for whose authentication the obliged entity's employees underwent special training, together with the appropriate proof thereof issued by the ministry in charge of internal affairs or another acceptable training organiser (for personal documents of the Republic of Serbia), and/or the competent foreign authority;
4) evidence that the obliged entity has appropriate premises for carrying out the video identification procedure, in accordance with Section 6 hereof;
5) evidence that the obliged entity has the technical solution referred to in Section 7 hereof, containing a description of the characteristics and manner of functioning of that solution, including the prior assessment of that technical solution referred to in Section 8 hereof.

If the obliged entity intends to offer customers the possibility of direct video identification, it shall also submit to the National Bank of Serbia, together with the notification referred to in paragraph 1 hereof and in addition to the documentation referred to in that paragraph, the certificate referred to in Section 18, paragraph 3 hereof – if the direct video identification procedure at the obliged entity is to be carried out in English as well, and/or the certificate referred to in Section 18, paragraph 4 hereof – if the direct video identification procedure at the obliged entity is to be carried out in sign language as well.

If the obliged entity outsources direct video identification activities in accordance with Section 27 of this Decision, it shall also submit to the National Bank of Serbia the decision on outsourcing such activities, containing data on the business name and head office of the obliged entity to which such activities are outsourced.

In the notification referred to in paragraph 1 hereof, the obliged entity shall specify the type of video identification it intends to offer to customers, as well as whether it intends to offer the possibility of video identification to all customers within the meaning of this Decision or only to a specific category of persons (e.g. to offer the possibility of video identification to a

customer who is a natural person, but not to entrepreneurs and legal persons).

The obliged entity referred to in paragraph 1 hereof shall, following submission of the notification referred to in that paragraph and prior to the expiry of the deadline referred to therein, provide employees of the National Bank of Serbia with a presentation, i.e. demonstration, of the entire video identification procedure in real time, for all categories of persons to whom it intends to offer the possibility of video identification.

The deadline referred to in paragraph 1 hereof shall run from the date of submission of the duly completed documentation referred to in that paragraph.

The National Bank of Serbia shall publish on its website the list of obliged entities that submitted the notification and duly completed documentation referred to in paragraphs 1 to 3 hereof.

Change in circumstances after notifying the National Bank of Serbia

31. The obliged entity shall notify the National Bank of Serbia without delay of any change to the regulations, documentation, data, technical solution and other circumstances referred to in Section 30, paragraph 1 hereof which occurred during the period from submission of the notification referred to in that paragraph until the expiry of the deadline referred to therein.

Following the expiry of the deadline referred to in Section 30, paragraph 1 hereof, the obliged entity shall notify the National Bank of Serbia in advance of any intended change to internal regulations which may materially affect the video identification procedure, as well as of all other circumstances resulting in a different manner of carrying out that procedure compared to the video identification procedure previously notified to the National Bank of Serbia, and shall also submit the documentation referred to in Section 30 hereof which is amended due to such changes.

Supervision by the National Bank of Serbia

32. Following the commencement of carrying out the video identification procedure, the obliged entity shall, at the request of the National Bank of Serbia, submit all regulations, other documents and data relating to the implementation of that procedure, including evidence of

verifications and internal controls carried out in accordance with this Decision and measures undertaken to remedy identified deficiencies.

If it identifies irregularities in the carrying out of the video identification procedure at the obliged entity, the National Bank of Serbia may – in addition to other measures laid down by the laws governing the prevention of money laundering, terrorism financing and financing of the proliferation of weapons of mass destruction and other regulations – order the obliged entity to discontinue carrying out video identification procedures.

VI TRANSITIONAL AND FINAL PROVISIONS

33. Obliged entities carrying out the video identification procedure in accordance with the Decision on Conditions and Manner of Establishing and Verifying the Identity of a Natural Person through Means of Electronic Communication (RS Official Gazette, Nos 15/2019, 84/2020 and 49/2021 – hereinafter: the Decision) shall harmonise their operations and internal regulations with the provisions of this Decision within six months from the effective date hereof.

Technical solutions used for carrying out the video identification procedure in accordance with the Decision shall, if necessary, be aligned with the provisions of this Decision within one year from the effective date hereof.

34. The procedures initiated in accordance with the Decision based on notifications submitted until the effective date of this Decision shall be completed in accordance with the provisions of the Decision.

35. On the day this Decision comes into effect, the Decision on Conditions and Manner of Establishing and Verifying the Identity of a Natural Person through Means of Electronic Communication (RS Official Gazette, Nos 15/2019, 84/2020 and 49/2021) shall cease to apply.

36. This Decision comes into effect on the eighth day following its publication in the RS Official Gazette.

NBS EB 14
7 May 2026
Belgrade

Chairperson
NBS Executive Board
Governor
National Bank of Serbia

Dr Jorgovanka Tabaković, sign.