NATIONAL BANK

DECISION No 281 of 7 November 2024

on the approval of the Regulation on the requirements for the identification and verification of customers' identities by electronic means

Published: 14.11.2024 in the OFFICIAL GAZETTE No 467-469 Article 886

Pursuant to Article 5^1, paragraph (3) of Law No 308/2017 on the prevention and combating of money laundering and terrorism financing (Official Gazette of the Republic of Moldova, 2018, No 58-66, Article 133), the Executive Board of the National Bank of Moldova

DECIDES:

1. The Regulation on the requirements for the identification and verification of customers' identities by electronic means, as set out in the Annex, is hereby approved.

2. This Decision shall enter into force on the date of its publication in the Official Gazette of the Republic of Moldova. The reporting entities that have implemented IT solutions for establishing the remote business relationship with clients as of the date when this decision comes into force shall comply with the new requirements within 6 months.

CHAIRMAN
OF THE EXECUTIVE BOARD **Anca-Dana DRAGU**

No 281 Chişinău, 7 November 2024

Appendix
To the Executive Board Decision
of the National Bank of Moldova
No. 281 of 07.11.2024

Regulation on the requirements for the identification and verification of customers' identities by electronic means

Chapter I. General Provisions

1. This Regulation on the requirements for the identification and verification of the customers' identity by electronic means (hereinafter - Regulation) aims to establish requirements for necessary policies and procedures, internal control system, risks and protection measures, as well as the minimum technical requirements for identification of customers and verification of their identity by the reporting entities mentioned in point 3 when establishing business relationships with customers without physical presence.

2. The requirements and standards for the identification and verification of customers with physical presence shall also apply to customers whose remote identification is carried out in accordance with the provisions of this Regulation, also the measures for the preventing and combating of money laundering and terrorist financing shall be applied in accordance with the provisions of Law no. 308/2017 on the preventing and combating money laundering and terrorist financing (hereinafter – Law no. 308/2017) as well as with the normative acts issued for its implementation.

3. The provisions of this Regulation shall apply to the reporting entities referred to in Article 4 paragraph (1), letters a), e), g) and i) of Law no. 308/2017.

4. The terms and expressions used in this Regulation shall have the meanings set out in Law no. 308/2017, Law no.124/2022 on Electronic Identification and Trust Services (hereinafter – Law no.124/2022) and in the normative acts issued for their implementation. In addition, for the purposes of this Regulation, the following terms and expressions shall apply:

Biometric data – means personal data resulting from specific processing techniques to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that person, such as facial images or fingerprint data;

Identification and verification of the customers' identity by electronic means – represent the process of identifying and remotely verifying the customer's identity based on

an appropriate risk assessment and according to the level of risk, through the use of one or more of the methods provided in article 5^1 paragraph (2) of Law no. 308/2017;

IT solution of establishing remote business relationships (IT solution) – means a set of technological components involved in the remote electronic identification process of a person, through which data are transmitted, images captured/uploaded and/or information is provided by the applicant;

Electronic means - represent tools that operate through innovative digital technologies using, inter alia, artificial intelligence and/or machine learning processes, such as applications performing person identification and/or identity document verification (e.g. digital image capture, facial biometric measurement, image matching), NFC (Near Field Communication) technology embedded in electronic identity documents.

Chapter II. Policies and procedures related to identification and verification of the customers' identity by the electronic means

Section 1
Policies and procedures

5. The reporting entity shall develop remote identification policies and procedures in order to comply with its obligations under Article 5(2)(a) of Law 308/2017 in cases where the customer is identified remotely. These policies and procedures shall be established based on the money laundering and terrorist financing risks identified and shall include, at a minimum, the following:

a) a general description of the IT solution used to collect, store, compare, verify, validate and update information throughout the process of establishing remote customer business relationships. This shall include an explanation of the components and functioning of the IT solution;

b) the circumstances under which the IT solution may be used taking into account the risk factors identified and assessed in accordance with article 6 paragraph (1) of Law no. 308/2017, within the framework of the entity's own risk assessment, including a description of the categories of customers, products and services eligible for remote identification;

c) the stages that are fully automated and those that require human intervention;

d) the controls established to ensure that the first transaction with a newly onboarded customer identified remotely is executed only after all customer due diligence measures, as required under Law 308/2017 have been applied;

e) a description of the induction and periodic training programs aimed at ensuring staff awareness, ongoing training and understanding of the functioning of the IT solution and the associated risks;

f) the requirements for the retention of data and information collected in the process of identification and verification of the customer's identity by electronic means.

Section 2
Pre-implementation of IT solution

6. When considering the implementation of an IT solution for the purpose of remote customer identification, the reporting entity shall conduct a pre-implementation assessment of that solution. Accordingly, the reporting entity shall define the scope, steps and requirements to be followed, including data recording and retention requirements, which shall include:

a) an assessment of the adequacy and security of the IT solution in terms of the accessibility, completeness, accuracy and integrity (non-repudiation) of the data and documents to be processed, as well as the reliability, authenticity and independence of the information sources used;

b) an assessment of the impact of the use of the IT solution on the specific risks of the entity, including money laundering and terrorist financing risks, as well as operational, reputational and legal risks, including the impact evaluation on the protection of personal data under the Law No 133/2011;

c) the identification of possible mitigating measures and remedial actions for each risk identified;

d) the identification of the IT solution's capability to mitigate the risk of using virtual private networks (VPNs) or proxy services aimed at concealing location or preventing the application of monitoring requirements;

e) an assessment of the compliance of the IT solution with the requirements for conducting the remote customer identification procedure using electronic means as established for the qualified trust service providers, under the provisions of Law no. 124/2022 and its subordinate normative acts;

f) an assessment of the compliance of the IT solution with the requirements of conducting remote customer identification and verification procedure using electronic means as laid down in international technical standards [1];

g) tests to assess fraud-related risks, including risks of the identity theft or impersonation;

h) an ICT and information security risk assessment;

i) an end-to-end functional testing of the IT solution, covering the customers, products and services for which the solution is applicable.

[1] See the provisions of pt. 29 of the Regulation.

7. In accordance with the provisions of point 49, the reporting entity shall submit to the NBM the supporting acts/documentation related to the assessments and tests referred to in point 6, their result, and the manner in which the application of the IT solution ensures the mitigation and remediation of money laundering and terrorist financing and other identified risks for the types of customers, services and products for which it is applicable. The assessments and tests referred to in point 6 may be performed/validated by an independent audit or through internationally recognized certifications, where the reporting entity does not possess the necessary internal resources in that purpose.

Section 3
Ongoing monitoring of the IT solution

8. The reporting entity shall monitor the IT solution on an ongoing basis to ensure that it operates in accordance with its intended purpose. In this regard, the reporting entity shall include in its remote customer identification policies and procedures, developed in accordance with point 5, at least the following:

a) the steps that the reporting entity shall take to ensure the quality, completeness, accuracy, adequacy and security of data collected during the remote customer identification process, which shall be proportionate to the money laundering and terrorist financing risks to which it is exposed to;

b) the scope and frequency of regular reviews of the IT solutions; and

c) the grounds for initiating and carrying out the ad hoc review of the IT solution, which shall include at least:

- changes in the entity's exposure to money laundering and terrorist financing risks;
- deficiencies in the functioning of the IT solution detected during monitoring, audit or supervisory activities;
- an estimated increase in attempts of customer identity fraud, including identity theft or impersonation, identified by the reporting entity;
- changes to the regulatory framework relevant to the remote customer identification process.

9. The reporting entity shall ensure that it has risk-based monitoring mechanisms in place, which shall take into account, as a minimum, the following factors:

a) lists of compromised or stolen identification data or credentials;
b) known fraud scenarios related to the establishing of remote business relationship;

c) indicators of compromised confidentiality, integrity or authenticity of the session resulting from the identification procedure;
d) a register of cases of regular or non-compliant use of the access device or IT solution provided to the person to be identified by the reporting entity;
e) abnormal/unusual geographical location of the person;
f) high risk geographical location (jurisdiction) of the person;
g) cases of identity theft, impersonation or unlawful processing of personal data identified.

10. The reporting entity shall establish within its remote customer identification policies and procedures developed in accordance with point 5 remedial measures to be applied where errors have been identified that affect the effectiveness of the IT solution. These measures shall include, at a minimum, at following:

a) a review of all affected business relationships to assess whether the reporting entity has properly applied customer due diligence (CDD) measures, with priority given to customers presenting an increased risk of money laundering and terrorist financing;

b) an assessment based on the information obtained during the review referred to in letter a) to determine whether an affected business relationship should be:

- reclassified into another risk category and made subject to the enhanced due diligence (EDD) measures;
- made subject to limitations, such as restrictions on transaction volume;
- terminated; or
- reported to the Service for the Prevention and Combating Money Laundering when suspicions of money laundering and/or terrorist financing have been identified.

11. The reporting entity shall determine the most effective means of monitoring the ongoing adequacy and reliability of the IT solution. In this end, it shall consider one or more, but not limited to, the following means:

- quality assurance testing;
- automated critical alerts and notifications;
- regular automated reports;
- sample testing;
- penetration testing;
- recognised expert reviews or reports issued by specialists in the field and/or supervisory authorities at national or international level,

including those in jurisdictions implementing similar standards for the prevention of money laundering and terrorist financing.

Chapter III. Requirements for the identification and verification of customers' identities by electronic means

12. The reporting entity shall carry out the identification and verification of the customer's identity by electronic means, with respect to potential new customers with whom the reporting entity intends to establish business relationships.

13. The reporting entity shall carry out the identification and verification of customers' identities by electronic means in relation to:

a) natural persons who are citizen of the Republic of Moldova;

b) resident legal entities whose representatives, founders, administrators and beneficial owners are citizens of the Republic of Moldova.

14. The reporting entity shall ensure that the IT solution includes components enabling the collection of the information necessary for customer due diligence (CDD), in accordance with the requirements of the remote customer identification policies and procedures developed by the reporting entity in accordance with point 5, it shall be capable of collecting:

a) all relevant data and documents necessary to identify and verify the identity of the natural and/or legal person;

b) all relevant data and documents necessary to verify that the natural person acting on behalf of the legal person is legally authorized to act in such capacity;

c) all relevant data and documents necessary to identify and verify the identity of the beneficial owner;

d) all relevant data and documents necessary to determine the purpose and intended nature of the business relationship.

15. The reporting entity shall ensure that regardless of the method applied for the remote identification and verification of customers' identities, the information that is normally required from customers identified in person is also collected and submitted by the customer. The method of information collection shall be determined by the reporting entity, which shall specify the type of information to be collected:

a) manually, entered by the customer or by an employee of the reporting entity;

b) automatically from documents submitted by the customer;

c) from other internal or external sources, collected either automatically or by an employee of the reporting entity;

16. The reporting entity shall implement and maintain mechanisms to ensure the integrity of the information captured in electronic format. It shall apply controls (at least on annual basis) over the process of establishing remote business relationship in order to address the risks associated with this process, including the concealment of Internet Protocol (IP) address locations and the use of services such as Virtual Private Networks (VPNs) or proxy servers.

17. In the case of the legal entity customer, the identification measures shall be applied to the natural person authorized to represent it, and the relevant registration documents of the legal entity shall be obtained. In such circumstances, for the natural person acting as the representative of the legal entity, the reporting entity shall apply the remote business relationship establishment process equivalent to that applied to a natural person customer. In the same context, measures shall be applied to verify that the natural person acting on behalf of the legal entity is legally entitled to do so.

18. The identification and verification of customers' identities by electronic means shall be performed either through automated verification mechanisms without the involvement of a human operator or, through verification processes assisted by a human operator (an employee of the reporting entity). The reporting entity may also use a computerised solution that combines both automated and human-assisted verification in the remote identification process of the individual.

19. Customer identification by electronic shall be preceded by the customer's explicit consent to the processing of personal data in accordance with the applicable legislation.

20. When identifying and verifying customers' identities by electronic means, the reporting entity shall ensure that the customer is informed of the terms and conditions under which electronic identification is carried out. The terms and conditions made available to the customer, including prior to the customer's access to the IT solution, shall include, but not be limited to, the following:

a) "Terms of use" (of the electronic platform, IT solution, or website) - shall contain the general conditions for accessing the IT solution used for the electronic identification of the customer;

b) „Information Notice on data processing and data protection" - shall contain information concerning the customer's right to be informed as a natural person or as a representative of a legal entity and shall describe the general, organizational and technical measures implemented, including details of the the information that will be processed in accordance with the requirements of the applicable legal acts;

c) „Anty-Money Laundering Policy" - shall contain a concise version of the policy regarding customer identification, prevention of money laundering, terrorist financing of politically exposed persons.

Chapter IV. Methods for the identification and verification of customers' identities by electronic means

21. When identifying and verifying customers' identities by electronic means, the reporting entity shall, depending on the level of money laundering and terrorist financing or other associated risks, use one or more of the following remote identification methods:

a) means of electronic identification providing an adequate level of security and complying with the standards established under Law no.124/2022 (qualified electronic signature);
b) electronic means ensuring the simultaneous live transmission of video and audio including elements verifying the customer's physical presence, as well as the recording of the original identity document and the capturing of the customer's facial image during the live session;
c) electronic means ensuring the live transmission of a photograph including elements verifying the customer's physical presence, together with the recording of the original identity document;
d) other electronic means provided by a qualified trust service provider, accredited under Law 124/2022.

22. When identifying and verifying customers' identities using video/photo identification means, with the involvement of a human operator, the reporting entity shall ensure that the identification process is recorded and that it meets the following requirements:

a) it shall be of a reasonable duration (as established under the entity's internal regulations), and shall contain, at a minimum, the following relevant information/data:
   - hour, day, year of the recording;
   - the exact time at which the natural person subject to video verification presents their identification data from the identity document (name and surname, personal identification number, date/month/year of birth, domicile and/or residence address), as well as the time/date/month/year of the recording and the customer's mobile phone contact number;
   - the time at which the employee of the reporting entity contacts the customer during the video verification and/or the time at which the customer receives or enters the unique code or accesses the link sent via Short Message Service (SMS) or email;

- the time when the customer brings the identity document close to the camera and displays both sides of it;

b) shall comply with the following conditions:

- the identification process shall be carried out in a quiet environment with adequate lightning conditions and no third person shall be involved in the process, so as to allow clear identification of the individual, otherwise, the process shall be interrupted;
- the video/photo verification process shall be conducted in real time and without interruptions, through a continuous live stream. If the verification process is interrupted, regardless of the reason, it shall be restarted from the beginning;
- the identification process shall ensure a free and clear interaction between the employee of the reporting entity and the customer, as well as the visual verification by the employee of the documents presented by the customer, including the applicable security features of the document concerned;
- the identification process shall ensure that the original documents are used and that no reproductions of original document, such as a photographs, copies or scans are accepted;
- the identification process shall ensure that the quality of the video and audio during the live transmission is high, with a resolution of minimum 8 megapixels or at least FullHD (1920x1080), to enable accurate and unconditional identification of the individual;
- the identification process shall ensure that the live video transmission is recorded in color and synchronized with sound;
- the identification process shall ensure the automatic capture of the customer's facial image and identity document;
- the identification process shall ensure that the IT solution does not permit the uploading of pre-recorded photos/videos during the live interview or photo identification process;
- the identification process shall ensure the use of appropriate technologies to maintain the integrity and security of video/photo recordings used for identity verifications.

23. When identifying and verifying customers' identities using electronic video/photo identification means that operate without the involvement of a human operator, where the customer does not interact with an employee, the reporting entity shall ensure that the process is recorded and complies with the following:

a) It shall be of a reasonable duration (as established under the entity's internal regulations), and shall include, at a minimum, the following relevant information and data:

- the hour, day and year of the recording;
- the exact time at which the natural person subject to video verification presents their identification data from the identity document (surname, given name, personal identification number, date/month/year of birth, domicile and/or residence address), as well as the time/date/month/year of the recording and the customer's mobile phone contact number;
- the time at which the customer presents the identity document, recorded by the camera on both sides;

b) it shall comply with the following conditions:

- the photograph (s) or video recording (s) shall be made under adequate lighting conditions, ensuring that the necessary features are captured with sufficient clarity to enable proper verification of the customer's identity;
- the IT solution shall include motion detection controls, which may involve procedures requiring a specific action from the customer to verify their presence during the communication session, or may rely on the analysis of received data without requiring explicit action from the customer;
- the IT solution shall use technologies employing algorithms to verify the authenticity of the identity document presented, including verification of its design and security features, comparison of the data registered in the submitted document with the data contained in the machine-readable zone (MRZ), authenticity assessment based on the colors profile of the submitted document, and the use of biometric algorithms to estimate the person's age and gender for validation against the information contained in the document;
- the IT solution used for remote identification shall employ algorithms capable of determining that the identity document used is original and not presented based on a reproduction of the original document, such as a photograph, copy or scan;
- the quality of the image and sound during the video transmission shall be high quality, with a resolution of at least 8 megapixels or at least Full HD (1920x1080), to enable accurate and reliable identification and recognition of the person;
- the IT solution shall use reliable algorithms capable of verifying whether the photograph(s) or video recording(s) correspond to the photograph(s)

extracted from the customer's official document(s) or photograph(s) obtained from secure and independent sources;

- the IT solution shall not permit the uploading of pre-recorded photos or videos during the session or photo identification process;
- the IT solution shall employ technologies ensuring the integrity and security of the video/photo recordings used identity verification.

c) It shall use electronic means.

24. When establishing a remote business relationship by electronic means, the reporting entity shall identify, verify and retain the technical data of the computer/device used by the customer (for example, model, name, hardware parameters, user-agent, cookies, installed fonts, time zone, language settings, screen dimensions, network connection data), the IP address and its location, as well as any other available data that and possibly collected data.

25. During the process of establishing a remote business relationship by electronic means, the reporting entity shall verify the telephone number and/or email address to be used for further communication with the customer, by sending to the individual undergoing the remote identification procedure a One-Time Password (OTP) or a time-limited link, specifically created for this purpose and generated individually (via email or SMS).

26. The procedure for establishing a remote business relationship by electronic means may be concluded only after One-Time Password (OTP) has been transmitted and successfully validated, or after the link has been transmitted and accessed.

27. In the context of establishing a remote business relationship by electronic means, the reporting entity shall verify the customer's identity documents under the following aspects:

a) detection of damage pr forgery of the document, in particular by identifying cases where a falsified photograph has been affixed over the original, as well as verifying the correspondence of the document's shape, security features (for example: holograms, optically variable elements, special fonts, etc.), letters and spacing with the standards applicable to the respective type of the identity document, including by tilting the document horizontally and vertically;

b) verification that the customer's appearance corresponds to the photograph on the identity document;

c) verification of the validity of the identity document;

d) confirmation of the existence and correspondence of the security features that must be present on the identity document presented by the customer, in line with the standards applicable to the respective type of document;

e) where there are suspicions regarding the identity of the person or the authenticity of the documents presented, additional questions shall be asked to verify the person's identity or the authenticity of the documents or a manual verification of the information shall be carried out by an employee;

f) comparison of the data from the identity documents presented with the data contained in the State Register of Population.

28. For the purpose of verifying and validating the data/information obtained from the customer during the video verification process , the reporting entity shall:

a) to obliged to verify the customer with regard to the following aspects:

- involvement in terrorist activities or in the proliferation of weapons of mass destruction;
- the application of international sanctions;
- the application of European Union financial sanctions;
- status as a politically exposed person (PEP) or other high risk factors;
- the existence of information that could affect the customer's reputation, by accessing credible information sources and/or publicly available databases and/or the internet, including those held by other public institutions and entities;

b) to obliged to request the customer's physical presence at its office where there are suspicions and/or doubts concerning the customer's free consent (due to physical or psychological pressure or influence) by third parties or any other suspicions regarding the customer;

c) have the right to require the use of an electronic signature on a copy of the identity document, as an additional measure to video identification, where there are doubts regarding the accuracy or authenticity of the information provided by the customer;

d) to obliged to verify the data/information received through electronic communication in accordance with the applicable regulations on the prevention and combating money laundering and terrorist financing.

29. When establishing remote business relationships by electronic means, the reporting entity shall use IT solutions certified in accordance with the applicable international standards[2].

30. The reporting entity may use the IT solution for establishing remote business relationship by electronic means for the purpose of updating the information or data of existing customer.

31. The reporting entity shall not initiate a business relationship with a customer by electronic means where it is unable to apply the standard customer due diligence measures, provided for in Law no. 308/ 2017, or where the technical requirements are not met, or the entity is unable to verify the customer's identity in accordance with the requirements of this Regulation.

Chapter V. Requirements for internal control system

32. When establishing a remote business relationship by electronic means using video/photo identification of the customer with the involvement of human operator, the reporting entity shall implement, at least, the following requirements:

a) for the employee of the reporting entity responsible for identifying customers by electronic means:
   - shall possess an adequate level of professional qualification in customer identification;
   - shall have at least one year of experience in applying customer due diligence measures ;
   - shall have received specialized training for the purpose of customer identification by electronic means;
   - shall have sufficient knowledge of the applicable regulations on the prevention and combating of money laundering and terrorist financing;
   - shall have sufficient knowledge of the security aspects of remote verification and shall be adequately trained to anticipate and prevent the intentional or deliberate use of deceptive techniques related to remote verification, as well as to detect and respond to their occurrence.

b) for the special area designated for the electronic identification of customers:

[2]
1. ISO/IEC 30107: Information technology - Biometric presentation attack detection;
2. ISO/IEC 24745: Information technology – Security techniques – Biometric information protection;
3. ISO/IEC 27034: Information technology – Security techniques – Application security;
4. ISO/IEC 15408: Information security, cybersecurity and privacy protection;
5. NIST SP 800-63: Digital Identity Guidelines;
6. NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management.

- shall be under constant control and video surveillance during the process of establishing the remote relationship with customers by electronic means;
- shall ensure that no other persons and/or objects are in front of the camera and that there is no noise that could compromise the quality of the recording or the information.

33. Senior management shall ensure that the entity's policies and procedures for establishing remote business relationship with customers developed in accordance with paragraph 5 are effectively implemented, regularly reviewed and amended where necessary.

34. Depending on the money laundering or terrorist financing risk associated with the business relationship or other associated risks, the reporting entity shall apply one or more of the following verification measures in high risk situations:

a) ensuring that the customer executes a transaction, from a payment account held with another reporting entity, including by using a payment instrument;
b) ensuring that the customer executes a transaction from a payment account held with a foreign financial institution located in a jurisdiction where anti-money laundering and counter-terrorist financing requirements are at least equivalent to those of the Republic of Moldova;
c) collecting biometric data for comparison with data obtained from other independent and reliable sources;
d) contacting the customer by telephone;
e) sending direct correspondence to the customer (both electronical and postal).

35. Where the reporting entity uses tools for the automatic reading information from documents, such as optical character recognition (OCR) algorithms or machine-readable zone (MRZ) checks, it shall take the necessary measures to ensure that those tools capture the information accurately and consistently and shall ensure that the integrity of the algorithm used to generate the unique identification number of the original document is maintained.

36. The reporting entity shall immediately inform, in accordance with the requirements of Law no. 308/2017, the Service for the Prevention and Combating of Money Laundering upon identifying any act or circumstances that give rise to suspicions, regarding customers suspected of money laundering, related predicate offences and/or terrorist financing, whether such transactions are being prepared, attempted, carried out, or have already been completed.

Chapter VI. Risks and protection measures

37. In the case of customer identification by electronic means, the risk-based approach shall be applied as established in:

a) Law 308/2017 on preventing and combating money laundering and terrorist financing;

b) the normative acts issued by the NBM in the field of preventing and combating money laundering and terrorist financing;

c) the normative acts issued by the Service for Prevention and Combating Money Laundering in the field of preventing and combating money laundering and terrorist financing;

d) this Regulation;

e) the additional enhanced due diligence measures established in the reporting entity's internal documents.

38. When identifying customers by electronic means, the reporting entity shall apply enhanced due diligence measures, in addition to those provided in article 8, paragraph (3) of Law no. 308/2017, in the following cases:

a) the person is a former customer with whom the business relationship was terminated due the inability to apply due diligence measures in accordance with the article 5, paragraph (3) of Law no. 308/2017;

b) the person is a resident, including a temporary resident of a high risk jurisdiction;

c) the person is managing assets under fiduciary administration (trust, investment fund).

39. Depending on the risk, the reporting entity may use one or more of the methods set out in point 21 to manage and mitigate the risks of money laundering and terrorist financing, including by obtaining additional information from the customer. In such situations, the additional methods used shall not be considered a remote customer identification method, but rather a measure applied by the entity for the effective management of money laundering or terrorist financing.

40. The reporting entity shall adequately identify and manage the information and communication technology and security risks associated with the use of the remote customer identification process, including in cases where third parties are used or where the process is outsourced.

41. The reporting entity shall use secure communication channels to interact with the customer during the remote identification process and associated exchange of information. The remote customer identification IT solution shall use secure protocols and cryptographic algorithms in line with industry best practices to ensure the confidentiality, authenticity, integrity and availability of the data exchanged, as applicable.

42. The reporting entity shall provide the customer with information on the applicable security measures that must be taken to ensure the secure use of the IT solution.

43. When establishing business relationships through other methods of remote customer identification using digital means accepted under Law no. 124/2022, and regulated by the Government, the reporting entity shall assess the extent to which such methods comply with the provisions of this Regulation and shall apply the necessary measures to mitigate the relevant risks arising from their use. The reporting entity shall, in particular, consider whether at least the following risks are addressed:

a) the risk of impersonation fraud, including the aleration of the applicant's appearance through physical and/or electronic means;

b) the risk that the customer's identity is not claimed or does not correspond to that recorded in the State Population Register;

c) the risk of counterfeiting and forgery of identity documents through physical or electronic means;

d) the risk of loss, theft, suspension, revocation or expiry of proof of identity, including, where applicable, tools for detecting and preventing identity fraud;

e) the risk of personal data breaches.

Chapter VII. Data processing and retention

44. When processing personal data, the reporting entity shall comply with the data confidentiality procedure, to undertake the necessary organizational and technical measures to protect personal data against unlawful or accidental access, destruction, alteration, blocking, copying, unlawful or unauthorized dissemination, and other unlawful actions.

45. For the purpose of electronic customer identification, the reporting entity shall process the data and ensure the protection and confidentiality of personal data obtained in the process of implementing the provisions and requirements of this Regulation, in accordance with the normative acts on personal data protection and this Regulation.

46. The reporting entity shall retain all documents and information obtained from customers, including video, audio, photo, screenshots, including copies of identification documents, the electronic fingerprint of the computer/device used, the IP address, and any other documents or information obtained, throughout the active period of the business relationship and for a period of 5 years after its termination.

47. The reporting entity shall ensure that, upon request, the documents and information on the identification and verification of customers, beneficial owners, as well the monitoring of customer transactions, including supporting documents related to such transactions, are made available to the National Bank of Moldova, the Office for Prevention and Combating Money Laundering and law enforcement authorities.

Chapter VIII. Responsibilities

48. In implementing this Regulation, the reporting entity shall inform the National Bank of Moldova of any suspicious activities and fraud incidents that pose risks to the safety, proper functioning or reputation of the reporting entity.

49. The reporting entity shall notify the National Bank of Moldova, at least 30 days prior to the initiating the customer identification procedure by electronic means, regarding its compliance with the following requirements:

a) evidence that the reporting entity has appropriate remote identification policies and procedures in place, implementing the requirements of this Regulation;

b) evidence that the reporting entity has carried out the pre-implementation assessment of the IT solution in accordance with point 6;

c) evidence that the employees of the reporting entity responsible for video identification using human-assisted verification means have been trained in accordance with point 32 letter (a);

d) evidence that the reporting entity has adequate premises for conducting video identification using human-assisted verification means, in accordance with point 32 letter (b);

e) evidence that the reporting entity has appropriate remote identification methods in place, in accordance with the requirements of Chapter IV.

50. The notification referred to in point 49 of this Regulation shall be submitted only once, prior to the reporting entity commencing the customer identification procedure by electronic means and implementing the provisions of this Regulation.

51. The outsourcing of the process of customer identification and verification of customer identity by electronic means shall be carried out by the reporting entity in accordance with the provisions of the applicable normative acts.

52. The reporting entity shall immediately cease the use of IT solution for establishing remote business relationship by electronic means upon the request of the National Bank of Moldova, if it is determined that the solution poses significant risks to the security or integrity of the customer identification and verification process.