Instruction No 9/2017

Subject: Identification and establishment of the requirements applicable to the verification procedures to the opening of bank accounts at a distance provided for in Article 18(5) (c) of Notice of Banco de Portugal No 5/2013

Given the fast technological development and the emergence of alternatives to the means to verify the identification data in Article 17 of Notice of Banco de Portugal No 5/2013 of 18 December 2013, which show a degree of safety identical to the solutions currently provided for in this Notice, it was deemed necessary to revise it, in order to allow Banco de Portugal to define, through an Instruction, the procedures that may be adopted alternatively to those set forth in Article 18(5) (a) and (b).

In turn, given the increased risk of money laundering and terrorist financing associated with the use of means of distance communication, the possibility to use an alternative procedure shall be subject to compliance with a series of specific requirements ensuring the appropriate mitigation of these risks.

This Instruction allows for identification of the alternative procedures referred to in Article 18(5) (c) of Notice No 5/2013, as well as of the specific requirements that such procedures shall comply with. These procedures and the respective specific requirements are part of an Annex to this Instruction. At this moment, the non-face-to-face identification of the customer via videoconference is set out as an alternative procedure for verification, for the purposes of Article 18(5) (c) of Notice No 5/2013, and the specific requirements associated with the use of this procedure are defined. Taking into account the ongoing technological developments, in the future the Annex to this Instruction may include other alternative verification procedures proven to provide an identical degree of safety.

The alternative procedures identified in this Instruction shall also be admissible, mutatis mutandis, for the cases provided for in Article 23 of Notice No 5/2013, i.e. where financial institutions intend to establish other business relationships.

Adoption of the alternative procedures provided for in this Instruction shall not relieve financial institutions from full compliance with the customer identification obligation, whether or not they make use of outsourcing, as provided for in Notice No 5/2013.

Therefore, in the exercise of the powers conferred upon it by the provisions of Article 17 of its Organic Law, approved by Law No 5/98 of 31 January 1998, of Article 12(3), Article 23(1) and Article 39 of Law No 25/2008 of 5 June 2008, and of Article 18(5) (c) of Notice of Banco de Portugal No 5/2013 of 18 December 2013, Banco de Portugal determines the following:

Article 1

Subject matter

This Instruction identifies and establishes the requirements applicable to the verification procedures set forth in Article 18(5) (c) of Notice of Banco de Portugal No 5/2013, hereinafter simply referred to as 'Notice', for compliance with the customer identification obligation provided for in Article 7 of Law No 25/2008 of 5 June 2008, hereinafter simply referred to as 'Law No 25/2008'.

Article 2

Alternative procedures to verify identification data resorting to means of distance communication

1 – For the purposes of Article 18(5) (c) of the Notice, the alternative procedures specified in the Annex to this Instruction shall be admissible when opening accounts at a distance, within the meaning of Article 2(14) of the Notice.

2 – The alternative procedures specified in the Annex to this Instruction shall also be admissible, mutatis mutandis, where financial institutions intend to establish other business relationships, pursuant to the provisions of Article 23 of the Notice.

Article 3

Additional provisions

The procedures identified in this Instruction shall be an alternative mean for verifying the identification data referred to in Article 17 of Notice No 5/2013 and shall not relieve financial institutions from compliance with the obligations arising from the customer identification obligation, as well as with other obligations arising from Law No 25/2008 and the Notice.

Article 4

Entry into force

This Instruction shall enter into force on the day following that of its publication.

Annex to the Instruction

(referred to in Article 2(1) and (2))

A. Videoconference

Article 1

Videoconference

1 – For the purposes of this Annex, 'videoconference' means the non-face-to-face mean of communication for customer identification that consists of a form of interactive communication allowing the transmission and capture of sound, image and data in real time.

2 – The financial institutions referred to in Article 3 of the Notice may use videoconference as a procedure to verify the following identification data, as referred to in Article 18(1) (a) and (b) of the Notice: full name, date of birth, nationality contained in the identification document, and signature.

3 – In the cases provided for in the foregoing paragraph, the identification data set forth in Article 17(a) (vi) and (vii) of the Notice may be verified under the provisions of Article 18(1) (c).

4 – Verification pursuant to the provisions of the foregoing paragraphs shall not prevent use of the means set forth in Article 18(5) (b) of the Notice, notably the electronic use of the *Cartão de Cidadão* (Citizen's Card) through the authentication service or the *Chave Móvel Digital* (digital mobile key) provided by the Portuguese State.

Article 2

Prerequisites to the adoption of videoconference as an identification data verification procedure

1 – Prior to adoption of videoconferencing as an identification data verification procedure, financial institutions shall:

(a) conduct a risk analysis specifically identifying the money laundering and terrorist financing risks associated with the procedure in question;
(b) conduct effectiveness and safety tests to the procedure;
(c) obtain prior opinion from the compliance officer, assessing in particular the adequateness of the mechanisms to mitigate the risks identified in the analysis provided for in sub-paragraph (a).

2 – The analyses, tests and opinions for the purposes of the foregoing paragraph shall be included in a written document and be subject to the obligation to keep documents and records under the terms of Article 49 of the Notice.

Article 3

Requirements associated with customers

1 – The identification data verification procedure via videoconference shall only be applicable to natural persons holding a public document that complies with the requirements of Article 14(1) of the Notice.

2 – The financial institution shall request the customer to indicate a contact data so that the requirements in Article 5(2) and (3) are complied with.

3 – Prior to the opening of the account, the institution shall verify whether the customer is identified in restrictive measures, notably stemming from a United Nations Security Council resolution or a European Union regulation.

4 – The financial institution shall require that the first deposit or transaction is carried out by the customer in a traceable form, making it possible to identify the payer, from an account opened at a financial entity or a legally authorised entity that, not being located in a high-risk third country, is proven to apply equivalent identification and due diligence measures.

Article 4

Requirements regarding human and material resources

1 – The videoconference shall be ensured by duly trained staff in the field of prevention of money laundering and terrorist financing, in compliance with the provisions of Article 46(1) of the Notice.

2 – Staff verifying identification data via videoconference shall include in the internal records of these actions a note clearly identifying them and the date when verification was carried out.

3 – The financial institution shall hold the videoconference in an autonomous physical space allowing adequate videoconference recording and quality, inter alia.

4 – The technical means used shall ensure that:

(a) the videoconference is held in real time without interruption;
(b) sound and image are recorded with sufficient quality to permit subsequent verification of the identification data collected and checked;
(c) the videoconference is recorded with the respective date and time stamp, subject to the consent of the customer.

5 – All the data collected during the videoconference, including its recording, shall be subject to the record-keeping obligation pursuant to Article 49 of the Notice.

Article 5

Requirements to be observed during the videoconference

1 – During the videoconference, the financial institution shall capture the front and back of the identification document referred to in Article 3(1), with the respective date and time stamp and sufficient quality for all identification data in the document to be perceptible, including the customer's photograph and signature.

2 – During the videoconference, the customer shall be sent a limited-duration one-time password (OTP), generated specifically for that purpose, ensuring full traceability of the identification procedure and the holding of the videoconference in real time and without interruption, pursuant to the provisions of Article 4(4) (a).

3 – The identification verification procedure shall only be considered complete when the customer introduces the one-time password referred to in the foregoing paragraph in the platform supporting the opening of the account and the respective confirmation of this password by the system.

4 – If the technical conditions necessary for completion of the identification verification procedure are not in place, including poor image quality, weak light and sound conditions, or interruptions in the video transmission, the videoconference shall be interrupted and considered invalid.

5 – Where the identification document presented during the videoconference raises doubts about its content, eligibility, authenticity, validity date, accuracy, or sufficiency, the videoconference shall not produce the intended effects regarding verification of the identification data.

6 – Where, during the videoconference, there are suspicions as to the accuracy of the identification data that may be related to money laundering or terrorist financing crimes, financial institutions shall:

(a) report this as laid down in Article 16 of Law No 25/2008;
(b) consider that the videoconference does not produce the intended effects regarding verification of the identification data.

7 – For the purposes of the foregoing paragraph, when financial institutions have reason to consider that their actions are liable to compromise an investigation by the competent judicial authorities, they shall, where possible, act in liaison with said authorities, by previously consulting them.