BANK OF GREECE

EUROSYSTEM

EXECUTIVE COMMITTEE

Meeting 172/29.5.2020

Agenda item 1: Terms and conditions for remote electronic identification of natural persons in the initiation of a business relationship with credit and financial institutions supervised by the Bank of Greece

---

THE EXECUTIVE COMMITTEE OF THE BANK OF GREECE, having regard to:

(a) Articles 2, 28 and 55A of the Statute of the Bank of Greece;

(b) the provisions of Law 4557/2018 "Prevention and suppression of money laundering and terrorist financing (transposition of Directive 2015/849/EU), and other provisions" (Government Gazette A 139), in particular Articles 3, 5, 6, 13 and 30 thereof;

(c) Banking and Credit Committee Decision no. 281/5/17.3.2009 "Prevention of the use of credit and financial institutions supervised by the Bank of Greece for money laundering and terrorist financing" (Government Gazette B 650), in particular para. 5.5.1 thereof;

(d) Bank of Greece Governor's Act 2577/9.3.2006 "Framework of operational principles and criteria for the evaluation of the organisation of Internal Control Systems of credit and financial institutions and relevant powers of their management bodies" (Government Gazette A 59), in particular Annex 1 thereof ("Outsourcing");

(e) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1/4.5.2016);

(f) the provisions of Law 4624/2019 "Data Protection Authority, measures implementing Regulation (EU) 2016/679 of the European Parliament and of the

Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, transposition to domestic law of Regulation (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions" (Government Gazette A 137);

(g) the Legislative Act of 13 April 2020 on measures to address the ongoing consequences of the COVID-19 pandemic, and other emergency provisions (Government Gazette A 84), in particular Article 39 thereof;

(h) the European Council and the Council of the EU Public Register of Authentic travel and identity Documents Online (PRADO);

(i) the Opinion of 23 January 2018 of the Joint Committee of the European Supervisory Authorities on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC/2017/81);

(j) the Draft Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines"), amending Guidelines JC/2017/37, of 4 January 2018; and

(k) the fact that no expenditure shall be incurred by the Government Budget as a result of the provisions of this Act,

HEREBY DECIDES AS FOLLOWS:

A. Subject matter and scope

1. This Act lays down the terms and conditions for the remote electronic identification of natural persons in the initiation of a business relationship with credit and financial institutions, as defined in Article 3(2) and (3) respectively of Law 4557/2018, supervised by the Bank of Greece, in accordance with Article 6(1)(a) of the said law (hereinafter referred to as "obliged entities"), in the context of the application of the institutional framework on the prevention of money laundering (hereinafter "ML") and terrorist financing (hereinafter "TF"). These terms and conditions concern the reliable verification of identification data nos. 1-4 of the table in para. 5.5.1 of Banking and Credit Committee Decision no. 281/5/17.3.2009, on the basis of the identity documents that are specified in the above paragraph and meet the conditions of this Act.

2. The provisions of this Act shall also apply to the remote electronic identification of the beneficial owners of legal persons, as defined in Article 3(17) of Law 4557/2018, or the legal representatives of a legal person or other natural persons whose identity must be verified due to their relation with the legal person under para. 5.5.2 of Banking and Credit Committee Decision no. 281/5/17.3.2009.

3. The terms and conditions laid down in this Act aim at mitigating the risk from the non-face-to-face verification and validation of the identity of natural persons.

B. Assessment and management of the risks of remote electronic identification

4. Obliged entities shall ensure that the remote electronic identification process and the technological solution adopted are adequate and appropriate for the validation and verification of the identity of natural persons on the basis of documents, data or information obtained from a reliable and independent source, as provided for by Article 13 of Law 4557/2018.

5. Obliged entities shall thoroughly assess the risks arising from the remote electronic identification of natural persons in respect of the natural persons themselves, the reliability and independence of the sources used for identity verification, the products or services to be provided to customers, as well as geographical and other factors. Obliged entities shall adopt, on the basis of the above risk assessment, the appropriate remote electronic identification process and technological solution in line with the provisions of this Act and shall ensure its effective implementation. When assessing the risks and establishing the applicable remote electronic identification process, obliged entities shall have regard to the Opinion of 23 January 2018 of the Joint Committee of the European Supervisory Authorities on the use of innovative solutions by credit and financial institutions in the customer due diligence process (JC/2017/81).

6. Obliged entities shall examine carefully the validity and authenticity of the data, documentation and information obtained in respect of natural persons as part of the remote electronic identification process, using an adequate range of data from different, reliable and independent sources, and bearing in mind that the data obtained electronically from the identity document of a natural person not physically present are not enough to verify his/her identity unless accompanied by the necessary control measures and mechanisms provided for in this Act.

7. Before adopting a remote electronic identification process and the relevant technological solution, obliged entities shall conduct an informed assessment of:

(a) the possibility of fully integrating the adopted technological solution into their existing systems and processes, and the relevant technical and operational risks, in particular the risk that the technological solution may be unreliable or could be tampered with or suffer irreparable failure;

(b) qualitative risks, in particular the risk that the sources of information used for verification purposes are not sufficiently independent and reliable, as well as the risk that the extent of identity verification provided by the technological solution is not commensurate with the level of ML/TF risk associated with the natural person;

(c) impersonation fraud risks, i.e. the risk that a natural person is not who they claim to be or that the person is not a real person; and

(d) the risk that the technological solution does not comply with the applicable data protection legislation.

8. With respect to technical and operational risks, obliged entities shall have sufficient in-house expertise, in addition to any external expert advice, to guarantee the proper implementation and use of the technological solution as well as to ensure the continuation of services should the technological solution suffer irreparable system failure or in case of termination of the business relationship between the obliged entity and an external provider of the solution (where it is not developed in-house). To this end, proper contingency plans shall be put in place to ensure continuity of services.

9. Obliged entities shall conduct appropriate tests in order to establish whether or not the remote electronic identification process and the technological solution are adequate and reliable and allow the application of CDD measures in line with the obliged entities' AML/CFT policies and processes and the applicable AML/CFT legislation. To this end, the AML/CFT Officer referred to in Article 38 of Law 4557/2018 must have a deep understanding of the workings of the technological solution and participate actively in its evaluation.

10. The above risk assessment and the remote electronic identification process shall be approved by the board of directors of the obliged entity, or by its senior management, as defined in Chapter IVA, para. 3 of Bank of Greece Governor's Act 2577/2006, on a detailed recommendation from the relevant key function holders and the AML/CFT Officer referred to in Article 38 of Law 4557/2018. Even if the process

has been approved by the board of directors, senior management must have a deep understanding of these risks, the remote electronic identification process and the function of the technological solution.

11. The approved remote electronic identification process shall include at least:

(a) a step-by-step description of the remote electronic identification process by method applied under Chapter C, and the organisational, technical and procedural safeguards that ensure the reliable identification and validation of the identity of natural persons and the management of the above relevant risks, as well as compliance with the provisions of this Act;

(b) a procedure whereby additional measures and safeguards are triggered in the case of an insufficient degree of certainty as to the validity of an identity document or the identity of the natural person;

(c) a procedure for recording and monitoring any deviations from the approved remote electronic identification process; and

(d) unacceptable risk criteria and a procedure to terminate remote electronic identification process where such criteria are not met.

12. Obliged entities shall, on an annual basis, review the remote electronic identification process and the technological solution applied, having regard to technological developments, emerging risks and any changes in the AML/CFT framework, so as to ensure informed decision-making regarding their suitability and the need to introduce additional control measures and mechanisms as appropriate.

13. Obliged entities shall without undue delay remedy any errors or weaknesses in the remote electronic identification process and the technological solution, as may be identified at any time or during a regular review, also taking the following additional actions:

(a) a review of all affected business relationships, to assess whether sufficient customer due diligence (CDD) has been applied to such relationships, in line with the obliged entity's policies and processes;

(b) an assessment, after the weaknesses have been corrected and adequate CDD has been applied, of whether any affected business relationships can be maintained or should be terminated, and/or the execution of transactions related to such business relationships should be stopped; and

(c) an assessment of whether or not, further to the above actions, a report should be submitted to the AML/CFT Authority.

Where the obliged entities have identified serious weaknesses in the technological solution or systematic errors related to its use, they shall comprehensively examine the level of reliability of the technological solution against the ML/TF risks involved, the scope for improvements to the solution and the continuation or discontinuation of its use, on the basis of their business continuity plans.

14. Obliged entities shall ensure that their internal audit functions conduct specific audits to verify the suitability, adequacy and reliability of the remote electronic identification process and the technological solution used. The outcome of such audits shall be notified to the AML/CFT Officer referred to in Article 38 of Law 4557/2018, in the context of the monitoring and assessment of the implementation of AML/CFT policies and processes, and shall be included in the latter's annual report. The suitability, adequacy and reliability of the remote electronic identification process and the technological solution shall also be audited by the external auditors and the outcome of such audits shall be included in their report, prepared in accordance with the provisions of Bank of Greece Governor's Act 2577/9.3.2006, Annex 3, Chapter II(e).

15. Obliged entities shall be in a position to prove to the Bank of Greece the suitability, adequacy and reliability of the remote electronic identification process and the technological solution adopted for this purpose, whether or not they have outsourced it, wholly or partly.

C. Permitted methods of remote electronic identification

16. The following remote electronic identification methods shall be permitted to obliged entities:

(a) video conference with a trained employee, which consists in an interactive, real-time audiovisual communication between a natural person and a trained employee who are in different locations and supports the exchange of files and messages;

(b) automatised identification via a dynamic selfie, without the physical presence of an employee, taken by the natural person in real time (as opposed to a static selfie), so as to ensure liveness detection.

17. For the purposes of remote electronic identification, original identity documents among those referred to in para. 5.5.1 of Banking and Credit Committee Decision no. 281/5/17.3.2009 shall be accepted, provided that they are included in the Public Register of Authentic travel and identity Documents Online (PRADO) and bear: (a) photograph and signature of holder; (b) a machine-readable zone (MRZ); and (c) two additional advanced visual security features among those specified in PRADO.

18. By exception to preceding para. 17, obliged entities may, after assessing the risk involved, accept as identity document of Greek citizens an ID card issued by the Hellenic Police with the full name written also in Latin characters:

(a) exclusively as part of the video conference method; and

(b) subject to ID card authenticity check through the Central Portal of Public Administration, in accordance with Article 39 of the Legislative Act of 13 April 2020.

19. Where obliged entities use the dynamic selfie identification method for remote electronic identification, they shall apply the additional ML/TF risk mitigation measures set out in Chapter E below.

D. Control measures and mechanisms in connection with remote electronic identification

20. Obliged entities shall have in place control measures and mechanisms to ensure the reliability of the remote electronic identification process, as follows:

(a) They shall adopt advanced technical specifications for the verification of the authenticity, validity and integrity of identity documents, making sure that they have not been altered or falsified in any manner whatsoever (e.g. by changing data of a genuine document, reproducing a genuine document, creating a fraudulent identity document using materials from legitimate documents). To this end, obliged entities shall check the submitted identity documents against the specifications of each document included in PRADO, in particular the security features, type, size of characters and structure of the document. Moreover, obliged entities shall verify the authenticity of the identity document on the one hand by reading and decrypting the information included in the MRZ and, on the other hand, by checking another two visual security features of those referred to in para. 17 of this Act.

(b) They shall ensure the reliability of the remote electronic identification process by relying, to the extent possible, on multiple alternative information sources. The

reliability of the remote electronic identification process is enhanced when obliged entities draw data from the Central Portal of Public Administration, in accordance with Article 39 of the Legislative Act of 13 April 2020, or other reliable and independent sources and databases in order to verify information or data obtained during the remote electronic identification process.

(c) They shall perform consistency checks against the natural person's profile, identity document and any other information, using an adequate range of data from reliable and independent sources.

(d) They shall dynamically develop the remote electronic identification process by designing a sufficient number of alternative standard identification scenarios and choosing randomly one of them.

21. Obliged entities shall adopt technical measures and safeguards in the remote electronic identification process, regardless of the method applied, as follows:

(a) They shall implement techniques of secure communication between the obliged entity and the natural person, ensuring the integrity and confidentiality of the information exchanged.

(b) They shall ensure that the remote electronic identification process occurs in real time and without interruptions and that no files created by the natural person in any manner before the initiation of the process are accepted.

(c) They shall ensure that any photographs and videos taken during the remote electronic identification process are of such quality that both the natural person and the data on his/her identity document are fully and unambiguously recognisable. Moreover, they shall ensure that during the remote electronic identification process there are proper lighting conditions, the natural person has the proper distance from the camera, without anything covering his/her face, and his/her required features are captured with absolute clarity.

(d) They shall ensure that all the data received, as well as the results of the controls conducted in the various stages of the remote electronic identification process, are kept on a digital record, properly protected from any attempt at tampering. These data shall include any photograph or video taken during the remote electronic identification process.

(f) They shall ensure that a single device is used throughout the remote electronic identification process.

22. As part of the remote electronic identification process and regardless of the method applied, obliged entities shall apply specific measures and controls, supported by dedicated media:

(a) They shall take photographs/snapshots, in proper lighting conditions, showing clearly:

(i) the face of the natural person under different angles, e.g. in profile, face on, using in parallel techniques to ensure liveness detection (such as eyes opened, eyes shut);

(ii) the pages/sides of the identity document that bear the photograph, signature and identity data of the natural person, so as they can be checked against the specifications and security features of the document.

(b) They shall use biometric algorithms to compare the natural person with the photograph on the identity document.

(c) They shall require the natural person to enter a unique number sent by email or SMS.

23. In the context of the video conference method of remote electronic identification, obliged entities shall, in addition to the above:

(a) ask the natural person to place a finger over the security zone of the document or move his/her hand in front of his/her face;

(b) in the case of ID cards issued by the Hellenic Police, also check whether the card lamination has been damaged or tampered with, or there are indications of attempted falsification of the document, or whether the photograph was inserted into the document after its issuance; and

(c) identify any suspicious behaviour of the natural person that may indicate that he/she is under the influence or is under duress or is mentally deranged.

E. Additional risk mitigation measures in the remote electronic identification process without the physical presence of an employee

24. Where obliged entities apply the remote electronic identification process, without the physical presence of an employee, supported by dynamic selfie identification, they shall also take one the following additional risk mitigation measures:

(a) they shall ensure that the first credit wire transfer to the natural person's account is made from an account kept in his/her name with a credit or financial institution situated in an EU Member State or a FATF member country. Obliged entities may, alternatively, confirm the existence of the above account by obtaining information from the account-holding credit or financial institution itself, as well as from any other reliable and independent source; or

(b) capping at €15,000 per year total credits to any accounts (including prepaid and credit cards) held with the obliged entity in the name of the natural person.

F. Termination of the remote electronic identification process

25. Obliged entities shall ensure that the remote electronic identification process is terminated without being completed in any of the following cases:

(a) the visual validation of the natural person and/or the official identity document is not possible, or there is any inconsistence or uncertainty; or

(b) there is any discrepancy between the data and information submitted during the remote electronic identification process and the data obtained from a reliable and independent source; or

(c) the unacceptable ML/TF risk criteria laid down by the obliged entity are met.

26. The reason of termination of the remote electronic identification process shall be recorded and kept in an adequately protected record for a period of at least five years, in accordance with Article 30 of Law 4557/2018 and the provisions of Chapter I below.

G. Organisational arrangements and staff training

27. Obliged entities shall ensure that the remote electronic identification process is conducted by qualified and trained staff, to whom they shall make available the necessary resources and special technical media for the smooth and secure implementation of the process. Training shall include the practical application of the technological solution and its functionalities; the security features of acceptable identity documents; common counterfeiting and falsification methods; the requirements of this Act; identification of unusual or suspicious transactions and reporting in line with the obliged entity's internal procedures. Training shall take place before the staff assume relevant duties, shall be repeated regularly and shall be

provided in addition to the general AML/CFT training under the applicable institutional framework.

28. Obliged entities shall ensure through appropriate procedures that the staff engaged in the identification and validation of customers through the technological solution do not collaborate with persons involved in illegal activities. These procedures shall include pre-hire and regular on-the-job fit for duty assessment; random assignment of natural persons' applications for remote electronic identification to the staff, so as to minimise manipulation risk; and sample checks of the staff's communications with natural persons during or after the remote electronic identification process.

29. Where obliged entities apply the video conference method for remote electronic identification, they shall ensure that the staff engaged are located in a specially designed area with restricted access.

H. Outsourcing of the remote electronic identification process to an external service provider

30. The remote electronic identification process is included in the material or important functions referred to in Annex 1 of Bank of Greece Governor's Act 2577/9.3.2006 and the relevant provisions on outsourcing shall apply thereto. If obliged entities decide to outsource, wholly or partly, the remote electronic identification process, they shall ensure, through appropriate assessment and control procedures, that the external service provider has adopted appropriate technical specifications and safeguards ensuring reliable identification and validation of the identity of natural persons, in line with the obliged entity's remote remote electronic identification process. In any case, the ultimate responsibility for complying with the provisions of this Act and the requirements of the AML/CFT framework shall rest with the obliged entity. Such responsibility shall include the ongoing monitoring of the efficiency and reliability of the remote electronic identification process, and granting explicit prior approval of any modification of the process by the external service provider.

31. Obliged entities shall ensure that the external service provider is bound by contractual arrangements to perform its duties under the outsourcing agreement in compliance with the provisions of this Act and the institutional framework applicable from time to time. The outsourcing agreement shall set out clearly and in detail the roles, responsibilities, rights and obligations of each party, including those arising

from expiry of the agreement or earlier termination thereof, in which case an exit plan shall be activated including the transfer of any information and data obtained by the external service provider in the performance of the agreement. The outsourcing agreement shall explicitly provide that no change to the remote electronic identification process is possible without the prior approval of the obliged entity.

32. Obliged entities shall ensure that the external service provider:

(a) provides adequate and accurate information on the information sources used, the controls conducted and the outcomes of the remote electronic identification process for every natural person, enabling the obliged entity to assess the quality of the process and establish the reliability of identification and verification;

(b) complies with the personal data protection legislation and has been certified for applying adequate information security standards; and

(c) uses qualified and trained staff in the remote electronic identification process. Training shall include the implementation of the technological solution and its operating potential; the security features of acceptable identity documents; common counterfeiting and falsification methods; the requirements of this Act; and identification of unusual or suspicious transactions.

33. Where the external service provider is situated in a third country, obliged entities shall have a good understanding of and address effectively the associated legal and operational risks and data protection requirements. Obliged entities shall not hire external service providers situated in a third country that has in place legal restrictions that do not allow the free exchange of information between the external service provider and the obliged entity or the Bank of Greece, or the external service provider's compliance with the AML/CFT framework.

34. The execution, in whole or in part, of the remote electronic identification process by an external service provider and the latter's relation with the obliged entity may under no circumstances jeopardise the operation and quality of the obliged entity's internal control system and the ability of the Bank of Greece to check, at such time and in such manner as it may deem expedient and appropriate, the obliged entity's compliance with the obligations arising from the provisions of this Act.

I. Record keeping and personal data protection

35. Obliged entities shall comply with the record keeping requirements of Articles 30 and 31 of Law 4557/2018 and this Act, as well as the personal data protection

legislation, regardless of the type or external provider of the technological solution they use in the remote electronic identification process.

36. Obliged entities shall keep intact all the necessary records/data allowing them to determine the exact date when documents are submitted and information and data are received during the remote electronic identification process.

37. Obliged entities shall ensure that natural persons are informed about the processing of their personal data. With regard to biometric and remote electronic identification, the explicit and specific consent of natural persons shall be required.

J. Final and transitional provisions

38. For as long as obliged entities are not connected with the Central Portal of Public Administration under Article 39 of the Legislative Act of 13 April 2020, they shall not be required to verify the authenticity of a natural person's ID card issued by the Hellenic Police pursuant to para. 18b of this Act.

39. The Supervised Institutions Inspection Department of the Bank of Greece is authorised to provide clarifications and instructions regarding the implementation of this Act.

40. The provisions of this Act shall take effect as from its publication in the Government Gazette.

This Act shall be published in the Government Gazette and posted on the website of the Bank of Greece.

The Deputy Governor	The Deputy Governor	The Governor
Theodoros Mitrakos	John (Iannis) Mourmouras	Yannis Stournaras

True and exact copy

Athens, 3 June 2020

(signed)

Ioanna Pantou, Secretary to the Executive Committee