Translated and commented by Finance Latvia Association

Unofficial translation

Approved by the Cabinet of Ministers on July 3, 2018

Procedures for the entity obliged by the Law on the Prevention of Laundering of Proceeds of Crime and Terrorist Financing to perform the client remote identification

I. General Provisions

1. These regulations define the procedure according to which the obliged entity of the Law on the Prevention of Money Laundering and Terrorism Financing (hereinafter – the Law) performs identification of a customer not personally present for the identification purpose and where such identification is performed by technical solutions, including video identification, safe electronic signature and other technical tools (hereinafter – the Remote Identification) and defines the scope of such identification.

2. The remote customer identification is applied according to the risk-based approach, if prior to the identification the obliged entity has ensured fulfilment of the following requirements:

2.1. the money laundering and terrorism financing risk assessment has been conducted and documentarily fixed;

2.2. an internal control system has been set up based on the identified money laundering and terrorism financing risks;

2.3. in consideration of the respective duties and area of authority, the employees have been duly trained to be able to undergo remote customer identification consistent with the set requirements;

2.4. the customer has been supplied with information on the remote customer identification procedure and his rights and obligations hereunder;

2.5. the safety requirements for the technical solutions have been set in accordance with these requirements and the identified money laundering and terrorism financing risks.

II. Remote customer identification limitations

3. No remote customer identification is performed in case the Law obliges mandatory presence of the customer for identification purposes[1] or in case remote customer identification is not compatible with the customer – specific money laundering and

[1] Article 23 (2) https://likumi.lv/ta/en/en/id/178987-law-on-the-prevention-of-money-laundering-and-terrorism-financing

terrorism financing risks. These regulations apply insofar any other laws do not provide different remote customer identification requirements.

4. The obliged entity does not perform remote customer identification, terminates it or any other operations prescribed by the applicable laws are imposed to the remote customer identification, in case:

4.1. of establishing circumstances which prove that the remote customer identification is not applicable to the customer-specific money laundering and terrorism financing risk;

4.2. of establishing circumstances which speak for insufficient safety or suitability of the remote customer identification or authenticity of the acquired information;

4.3. of establishing noncompliance with the information acquired during the customer due diligence (CDD).

III. Rights and obligations of the obliged entity in connection with the remote customer identification

5. The obliged entity may anytime, without providing any additional explantation, apply to the customer that was made subject to the remote identification:

5.1. identification procedure, requiring the customer's presence at the identification procedure;

5.2. other form of remote customer identification as provided for in Paragraph 7 of these Regulations or to repeat the already performed customer identification by using the same remote identification procedure by eliminating the established shortcomings.

6. The obliged entity undergoes the remote customer identification himself within the framework of the same group of companies or outsources the given service. The obliged entity may assign the remote customer identification to the outsourcing service provider, if at least the following measures have been taken:

6.1. the outsourcing service provider acts in accordance with the anti-money laundering and terrorism financing requirements that derive from the EU laws;

6.2. prior to making use of the services of the outsourcing service provider the obliged entity verifies its ability to perform remote customer identification and monitors the compliance of the services provided by the outsourcing service provider with the requirements of the applicable laws;

6.3. other legal requirements applicable to the outsourcing service providers have been met.[2]

[2] E.g., Article 10.[1] https://likumi.lv/ta/en/id/37426-credit-institution-law

7. On the basis of the existing money laundering and terrorism financing risks, the obliged entity applies one or several of the following technical solutions:

7.1. safe electronic signature that ensures qualified electronic identification of increased security in accordance with the level that is set by relevant laws or the Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July2014 on electronic identification and trust services for electronic transactions in the internal market and repealing the Directive 1999/93/EC;

7.2. video identification in accordance with Paragraph 10 of these Regulations;

7.3. acquisition of data certifying the identity of a private individual from a credit institution or payment institution by using an identification payment or another method which allows acquisition of the data referred in Paragraph 13.2. from the credit institution or the payment institution;

7.4. the comparison of the photo image on the personal identification document with the electronic self-portrait photography (*selfie*);

8. For risk management purposes the obliged entity shall independently undergo safety management of the applied technical solution, with due regard of the identified vulnerabilities and fraud scenarios. To mitigate the risk level, the obliged entity may apply direct and also compensating (additional) controls (including concurrent use of several of the solutions referred in Paragraph 7 of these Regulations, digital behaviour analysis with self-study algorithms, verification of utility bills issued to the person, acquisition of information from other databases, social networks, keeping of audio recordings of conversations, acquisition of data that certify the identity of private individuals from state maintained registers for the inspection of results) in accordance with the requirements of the personal data processing laws.

IV. Video-identification

10. Video-identification is performed by ensuring compliance with at least the following requirements:

10.1. it is performed in real time, by interviewing the customer in a synchronized video and audio streaming and using an encrypted connection;

10.2. the comparison of the face image of the private individual with the image on the private individual's personal identity document that has been obtained during the video streaming;

10.3. the video-identification clearly reveals the head and the shoulders of the private individual, his/her face image without shadowing, the image can be clearly distinguished from the background and other objects;

10.4. the face of the private individual cannot be covered;

10.5. the photo images on the presented documents are clearly visible;

10.6. there are questions asked during the video-identification to adjust or verify the information regarding the customer;

10.7. the audit trail of the audio and image information flow is fixed with an unchangeable timestamp, the name and surname of the remotely identified private individual and his/her IP address;

10.8. ensured continuity of the streaming process. In case the process is interrupted, the video-identification is performed repeatedly.

V. Technical solutions applied for the remote customer identification

11. The technical solutions indicated in Paragraph 7.2 and 7.4 can be applied in case the used personal identification document of the customer, including its representative, corresponds to any of the types of personal identification document specified in the applicable laws and the following requirements are satisfied:

11.1. the document contains an area that is specially designed for optical text identification and the reading of the given text is ensured during the remote customer identification;

11.2. the document contains optical safety elements (e.g. holographic optical elements or printed elements with the effect of latent images);

11.3. there are solutions or approaches used for the identification of counterfeit personal identification documents.

12. The provisions of Paragraphs 7.3. or 7.4. of these Regulations are not applicable, in case the customer or its ultimate beneficial owner (UBO) are related to a high-risk jurisdiction according to the increased risk factors set out in the Law.[3] If in accordance with the provisions of Paragraph 7.3. or 7.4 of these Regulations, the monthly transaction amount of a remotely identified customer that is subject to the enhanced customer due diligence (EDD) because of any facts not-associated with his/her remote identification[4] exceeds 3000 EUR, the customer is identified being present at such identification or in accordance with the provisions of Paragraph 7.1. or 7.2.

13. In case the provisions of Paragraph 12 of these Regulations allow for the application of remote customer identification foreseen in sub-paragraph 7.3, in applying the provisions of sub-paragraph 7.3, all of the following requirements should be considered:

[3] Article 11.[1] (3) 2) https://likumi.lv/ta/en/en/id/178987-law-on-the-prevention-of-money-laundering-and-terrorism-financing
[4] E.g., see Paragraph 13, 40 – 43, 47 of https://likumi.lv/ta/id/296439-klientu-padzilinatas-izpetes-normativie-noteikumi-kreditiestadem-un-licencetam-maksajumu-un-elektroniskas-naudas-iestadem

13.1. the credit institution or the payment institution whose data are used for the remote customer identification is subject to the anti-money laundering and terrorism financing requirements deriving from the EU laws;

13.2. by making use of the identification payment or another method allowing to receive from the credit institution or the payment institution data confirming the identity of a private individual, the obliged entity acquires sufficient data, as prescribed by the Law,[5] to verify the identity of the private individual and to compare against the data provided by the customer to the obliged entity;

13.3. it is prohibited to identify a customer for the opening of any such account that is maintained by the customer's payment service provider or for issuing a payment card or other payment instrument that can be used for performing future identification according to sub-paragraph 7.3.

14. If in accordance with the requirements of these Regulations the remote customer identification foreseen in sub-paragraph 7.4 can be applied, the obliged entity fixes an unchangeable timestamp to the audit trail of the image and performs remote identification of the name, surname and IP address of the private individual.

15. The obliged entity incorporates in its internal policies and procedures the form and the procedure for the initiation of a business relationship with a customer that has been identified according to the remote customer identification procedure.

16. The obliged entity shall procure that the information that is obtained as the result of the remote customer identification procedure, including video streaming and audio streaming materials, is recorded and kept for the term indicated in the law and that the electronic identification and technical data obtained during the identification procedure cannot be changed.

17. The obliged entity registers information regarding customers that have been identified according to the remote procedure and ensures the possibility to select information on the customers identified according to the remote identification procedure, the employees of the legal entities referred in Paragraph 6 of these Regulations and on the applied technical solutions.

[5] Article 12 and 13 https://likumi.lv/ta/en/en/id/178987-law-on-the-prevention-of-money-laundering-and-terrorism-financing