



Online Identification Regulation **(Online-IDV; Online-Identifikationsverordnung)**

Full title

Regulation of the Financial Market Authority (FMA) on video-based online identification of customers (Online Identification Regulation – Online-IDV; Online-Identifikationsverordnung)

Original Version: Federal Law Gazette II No. 5/2017

Amendments: Federal Law Gazette II No. 199/2018; 169/2020; 414/2020; 265/2021; 455/2021; 572/2021; 470/2022

Preamble/Promulgation clause

On the basis of Article 6 para. 4 of the Financial Markets Anti-Money Laundering Act (FM-GwG - Finanzmarkt-Geldwäschegesetz), published in Federal Law Gazette I no. 118/2016, most recently amended by Federal Act in Federal Law Gazette I no. 98/2021 the following shall be determined by regulation with the consent of the Federal Minister of Finance:

Text

Part 1

General provisions

Subject matter

Article 1. (1) This Regulation determines the required security measures to be taken to mitigate the increased risk, which results from the determination and verification of the identity of a person, where they or the natural person representing them is not physically present, where instead a video-based electronic procedure (online identification) is used.

(2) The required security measures to be defined in this Regulation shall apply regard of additional due diligence obligations for the prevention of money laundering or terrorist financing pursuant to the FM-GwG.

(3) The obliged entities may set additional security measures to increase the level of security regardless of the security measures to be taken in accordance with this Regulation.

(4) The provisions of this Regulation shall apply regardless of the applicable requirements under data protection law in relation to online identification.

Definition of Terms

Article 2. For the purposes of this Regulation, the following definitions shall apply:

1. screenshot: a graphical representation generated and stored by means of electronic data processing, which reproduces the content shown on screen as a visual component of the online identification process at the point in time at which it is generated and of such a quality, that it corresponds to the respective standards for verification and documentation purposes;
2. official photo identification document: an official photo identification document within the meaning of Article 6 para. 2 no. 1 FM-GwG, which contains optical security features that are at least comparable to (holographic) elements that visually change when moved;
3. processor: a processor pursuant to Article 4 (8) of Regulation (EU) 2016/679 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,

All English translation of the authentic German text is unofficial and serves merely information purposes. The official wording in German can be found in the Austrian Federal Law Gazette (Bundesgesetzblatt; BGBl.). All translations have been prepared with great care, but linguistic compromises had to be made. The reader should also bear in mind that some provisions of these laws will remain unclear without certain background knowledge of the Austrian legal and political system. Please note that these laws may be amended in the future and check occasionally for updates.



04.05.2016, p. 1, in the version of the corrigendum, OJ L 74, 04.03.2021, p. 35, upon whom the provisions with regard to third parties pursuant to Section 4 of the FM-GwG shall apply.

4. Biometric identification processes: online identification processes, in which the entire online identification process or individual steps thereof are conducted by means of an automated electronic process without the participation of a staff member.

Part 2

Safeguards

Organisational safeguards

Article 3. (1) The obliged entity may only use employees for the online identification process, who have been adequately trained to be able to conduct online identification and who are of good personal reliability. The training for online identification shall address the legal framework, the technical requirements and the practical aspects of ensuring the verification.

(2) The obliged entity shall ensure that the applications used in the online identification process as well as the data that is transmitted does not lead to any conflict with other processes conducted by the obliged entity, that the possibility of any influence is excluded, and that the applications and data are protected against any unauthorised access.

(3) Employees of the obliged entity shall only be allowed to conduct the online identification process in a separate room equipped with an access control system.

COVID-19-related provision in force until 31.12.2023

(4) By way of derogation from para. 3, staff members of the obliged entity shall be allowed to conduct online identification at their place of residence in a separate locked room (online identification while working from home). It must be ensured that the staff member is alone and undisturbed in this room for the entire duration of the online identification process. Where online identification is to be conducted by a staff member who is working from home, the potential customer must be informed about this circumstance in advance and be made aware that alternative identification options exist. The remaining provisions in this Regulation shall remain unaffected.

Process-related safeguards

Article 4. (1) Where personal data are to be processed in accordance with the provisions in this Regulation, this shall take place on the basis of Article 6 para. 4 FM-GwG for the purposes of prevention of money laundering and terrorist financing (Article 21 para. 4 FM-GwG).

(2) The conversation or the part of the conversation that serves the purposes of online identification, shall in any case be recorded as a sound file in entirety; Article 12 para. 4 no. 2 DSG shall be applicable. Furthermore, screenshots shall also be generated, which in suitable lighting conditions graphically depict the following items from the online identification process:

1. in all cases the face of the potential customer or the natural person authorised to represent the potential customer,
2. the presenting of the front side of the official photo identification document, and
3. the presenting of the reverse side of the official photo identification document or the page containing data.

The screenshots shall in any case have to be of such a quality, that the potential customer or the natural person authorised to represent the potential customer and the data contained on the official photo identification document are clearly and fully recognisable.

(3) The potential customer of the natural person authorised to represent them shall also upon request:



1. move their head including showing their face, as well as separately
 2. communicate the serial number of their official photo identification document or a string of characters or words of at least four characters in length generated randomly by the obliged entity.
- (4) The employee, who conducts the online identification process, shall ascertain that the official photo identification document is authentic by the following means:
1. visual verification of the presence of optical security features including (holographic) security features that visibly react to movement or comparable security features, which must be clearly recognisable when asked to tilt the official photo identification document horizontally and vertically,
 2. verification of the correct numbering convention being used for the serial number,
 3. checking that the laminating used to seal the official photo identification document is not damaged, or comparable features that show that the document has not been tampered with,
 4. checking to be able to rule out the possibility that the photograph has only subsequently been attached to the official photo identification document,
 5. Verification of the logical consistency
 - a) of the features of the potential customer or the natural person authorised to represent the potential customer against the personal description and the photograph contained in the official photo identification document, as well as
 - b) of the photograph, the issue date and the date of birth contained in the official photo identification document with one another, as well as
 - c) of all other customer information which might already be available against the corresponding supplementary information contained on the official photo identification document.
- (5) The potential customer or the natural person authorised to represent the potential customer shall enter a string of numbers valid specially for the purpose of online identification, that has been centrally generated and communicated to them by e-mail or SMS, without delay during the ongoing video transmission and return them to the employee electronically.
- (6) Online identification may also be conducted using suitable biometric identification processes provided that this is permissible pursuant to Article 9 (2) a) of Regulation (EU) 2016/679 and the obliged entity takes suitable technical and organisational measures to achieve a level of protection as defined in Article 32 of Regulation (EU) 2016/679 that is adequate for the risk entailed. In so doing, the requirements of this Regulation must be observed in accordance with the following provisions:
1. The biometric identification process must in any case correspond to the technological state of the art, be updated on an ad hoc basis, and must achieve a level of security, through which it can be ensured that it is performed in a way that is at least comparable to online identification process conducted by a staff member. The obliged entity must take appropriate measures to safeguard the integrity and security of the procedures used, including constant active monitoring measures, in order to recognise and rectify any problems without delay.
 2. The biometric identification processes must be documented by the obliged entity in a comprehensible manner. The first sentence of para. 2 shall apply with the proviso that recordings that are made for online identification purposes, are to be stored electronically as defined in Article 21 para. 1 no. 1 FM-GwG by the obliged entity. The documentation shall in any case also cover the security factors applied when verifying identity as well as the results of the individual steps of the check.
 3. para. 2 nos. 2 and 3 shall apply with the proviso that instead of screenshots being made when verifying electronically signed photo identification documents (no. 5), the electronically signed data shall be stored instead.
 4. If the requirements pursuant to paras. 3 and 5 are fulfilled by a biometric identification process, then the obliged entity shall use suitable safeguards to check the actual participation of the potential customer or the natural person authorised to represent them in the online identification



process, which shall in any case include a video recording created during the online identification process (presence checking). Presence checking may deviate from para. 3 nos. 1 and 2 and para. 5 and may also be conducted as a passive presence check.

5. Only photo identification documents, for which the content has been electronically signed by the issuing authority, shall be allowed to be used for biometric identification processes. The obliged entity shall be required to check the authenticity of the electronic signature on the photo identification document and the integrity of the electronically signed data, and to ensure that a compromised key has not been used for the signature. During the biometric identification process the obliged entity shall also be required to perform a logical consistency check pursuant to para. 4 no. 5. Para. 4 nos. 1 to 4 shall not apply to the checking of the authenticity of the photo identification document as part of a biometric identification process.

Compulsory termination of the online identification process

Article 5. (1) The online identification process shall be terminated except in the cases listed pursuant to para. 2, if

1. a suitable verification of the potential customer, or of the official photo identification document, or both, is not possible under consideration of the safeguards in relation to the process (§ 4),
2. any other inconsistencies exist,
3. any other uncertainties exist,

(2) Where the obliged entity has an obligation to determine and verify the identity of the customer or of the natural person authorised to represent them pursuant Article 5 no. 4 or no. 5 FM-GwG, then the online identification process shall be continued to the end and making a suspicious activity report pursuant to Article 6 FM-GwG to the Financial Intelligence Unit (Geldwäschemeldestelle) considered.

Conducting of the online identification process by processors

Article 6. (1) If an obliged entity makes use of a processor to conduct the online identification process, it shall have to ensure that the processor takes security measures that correspond both in terms of their scope as well as their quality with the requirements in this regulation. However, ultimate responsibility for meeting those requirements shall remain with the obliged entity, which relies on the processor. When concluding, implementing and terminating an agreement with a processor, due professionalism and diligence shall be exercised and a clear delineation of rights and obligations to be arranged in writing.

(2) Outsourcing and agency relationships as defined in Article 15 FM-GwG shall not be allowed to significantly compromise the quality of the internal control mechanism, nor the possibility for the FMA to check compliance with all requirements relating to the online identification process.

Part 3

Final provisions

References

Article 7. (1) Where references are made to provisions in the FM-GwG, the Financial Markets Anti-Money Laundering Act (FM-GwG - Finanzmarkt- Geldwäschegesetz) as published in Federal Law Gazette I No. 118/2016 shall apply in its version amended by Federal Act in Federal Law Gazette I No. 37/2018.

(2) Where references are made to provisions in the DSG, the Data Protection Act (DSG - Datenschutzgesetz), as published in Federal Law Gazette I no. 165/1999 shall apply in its version amended by Federal Act in Federal Law Gazette I no. 24/2018.

Personal-related designations

Article 8. Where the designations used in this Regulation refer to natural persons, the form used applies to both genders.



Entry into force and repeal

Article 9. (1) Article 3 para. 4 in the version of the Regulation amended in Federal Law Gazette II No. 414/2020 shall enter into force of following day after announcement and shall be repealed at the end of 31 December 2023.

(2) Article 2 nos. 3 and 4, Article 4 para. 3 no. 2 and para. 6 as well as Article 5 para. 1 no. 1 in the version of the Regulation amended in Federal Law Gazette II No. 455/2021 shall enter into effect on the day following publication. Until 31 December 2022 obliged entities may make use of biometric identification processes that diverge from those listed in Article 4 para. 6 no. 5 in the version of the Regulation amended by Regulation in Federal Law Gazette II No. 455/2021 provided that the process used corresponds to Article 4 para. 4 nos. 1 to 5.