Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Comments

EBA Consultation Paper - Draft Guidelines on the use of Remote Customer Onboarding Solutions under Article 13(1) of Directive (EU) 2015/849 (EBA/CP/2021/40)

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:
Diana Campar
Associate Director
Telephone: +49 30 1663-1546
E-Mail: diana.campar@bdb.de

Berlin, 18 March 2022

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

Questions for consultation

1. Do you have any comments on the section 'Subject matter, scope and definitions'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

General comments

We have fundamental reservations about whether every single financial sector operator will be able to fulfil the requirements in the envisaged breadth and depth without expending a disproportionate amount of time and effort.

It is essential, in any event, to avoid different interpretations of the guidelines leading to further fragmentation and to institutions applying different identification standards. Instead, consideration should be given to the use of common standards such as ETSI TS 119 461.

Irrespective of these basic concerns, national supervisors should continue to be able to approve remote onboarding processes. Financial sector operators using such approved processes should not be obliged to comply with the requirements of these guidelines as well.

In addition, the scope of application of the guidelines should be explicitly limited to the introduction of new processes. We strongly recommend that existing state-regulated processes should be grandfathered by clarifying that the use of state-regulated processes is deemed to satisfy the requirements of these guidelines or that the guidelines in their entirety do not apply. Otherwise, institutions will face an unnecessary and substantial burden which may cause considerable damage.

We consider it unrealistic, moreover, to expect the guidelines to be incorporated into national law and implemented by institutions within the envisaged three-month time frame. Identification processes are an integral part of the business activity of financial institutions. Discontinuing the use of some identification processes may cause significant loss or damage to this business activity. A period of at least 12 months should be allowed for institutions to implement the requirements after their incorporation into national law. The time frame should give institutions sufficient opportunity to review their existing processes, subsequently adjust them and introduce new processes where necessary. This will ensure coherent and consistent implementation of the requirements in a manner compatible with other rules and regulations.

The guidelines should also clarify that they should be applied to the initial identification of any additional persons subject to identification requirements, even in an existing business relationship.

Finally, it should be ensured that all the guidelines are consistent with planned future European legislation, namely DORA and the EU anti-money laundering package, as well as with the revised eIDAS Regulation, especially with regard to the EU digital ID wallet.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

Paragraph 6

The question arises as to the distinction between the requirements of these guidelines and further rules or restrictions issued by state authorities with respect to approved processes. Provided that institutions carry out the prescribed internal processes and assessments when selecting a solution and document them as required, the use also of other processes (which have yet to be approved by the state) would be in line with the objective of the guidelines to create a common European standard. It would therefore be helpful to spell out this objective at an appropriate point in the guidelines themselves since national implementation of the guidelines will possibly necessitate further changes to national legislation.

Paragraph 9

Digital Identity: The definition should be expanded to make it clear what data are to be covered in general (e.g. those in the chip of a physical ID card or credentials on an end device) and to which category they should be assigned ("material unit" or "immaterial unit").

Digital Identity Issuer: We assume this means a provider of digital identities or trust services provider. It would be helpful to expand the definition to make this clear.

Remote Customer Onboarding: Onboarding involves several due diligence steps (collection of information for identification purposes, identity verification, recording of collected data and documents, clarification of the nature and purpose, possibly clarification of the source of funds, etc.). The guidelines do not make it clear whether onboarding will be classified as remote if at least one of these steps is carried out remotely or whether all steps have to be carried out without physical contact. Should only one step suffice, it would be helpful to define the relevant individual steps.

A definition of "remote customer onboarding" should therefore be included in the guidelines. The definition should be compatible with Directive (EU) 2015/849 and the EBA/GL/2021/02 guidelines, which talk of "non-face-to-face" interactions but do not provide an adequate definition of "remote".

Furthermore, the term "end-to-end" should be clarified in more detail in relation to the "remote customer onboarding solution" (see paragraph 10(g)). It should also be made clear whether the term "solution" refers to the entire onboarding process or only the part of the process that is supported/mapped by IT and replaces face-to-face contact in the same physical location.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

2. Do you have any comments on Guideline 4.1 'Internal policies and procedures'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 10

Letter (c): If the requirement is intended to mean that no remote onboarding should be offered to customers with a high ML/TF risk, this would go too far since any such risks can be mitigated by accompanying measures. From a practical point of view, the requirement is not feasible as a risk classification can only be carried out after all relevant information about the customer has been obtained. Differentiation according to certain product or service categories is equally impracticable. There is no logical link between a customer's risk qualification and the use of a remote onboarding solution officially recognised as secure. This requirement should therefore be deleted.

Letters (d) and (e): The distinction between the "information" required under (d) and (e) is not clear.

Letter (h): This requirement is at odds with Article 14(2) of Directive (EU) 2015/849, which gives member states the option of allowing obliged entities to complete the verification of identity immediately after the business relationship has been established. German lawmakers have exercised this option in Section 11(1) of the German Anti-money Laundering Act. The requirement should therefore be deleted.

Letters (g) and (i): It should be made clear that these requirements can be met by the existing record-keeping requirements in accordance with the ICT risk management guidelines EBA/GL/2019/04 for implementing ICT solutions and in future in accordance with DORA.

Paragraph 14

It should be made clear that this pre-implementation assessment requirement can be fulfilled by taking due account of AML aspects when conducting the pre-implementation assessment in accordance with general risk management requirements (such as MaRisk, BAIT or the EBA's ICT risk management guidelines).

In any event, no pre-implementation assessment should be required if a new process is being implemented which has been officially approved, recognised or otherwise accepted by a state authority. An exemption to this effect should be included in the guidelines.

It should be made clear that solutions will also be exempt from the pre-implementation assessment requirement if they are already in place before the guidelines take effect and are implemented nationally. It is absolutely essential to grant such solutions grandfathered status as some of them have been in use for many years and are continually checked for their reliability.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

Paragraph 15

Letter d): In practice, the tests to assess fraud risk are difficult, can only be done in conjunction with the trust service provider and do not reflect real-life scenarios. When service providers are used, providing a reference to the service provider's testing procedure should suffice. We would appreciate clarification on this.

Letter e): Assessing the level of adaptability of the solutions can only be done from today's standpoint. It would be very difficult to forecast future changes. As a result, it is not possible to define specific and practicable benchmarks for assessing the level of adaptability of the solutions. This requirement should therefore be removed.

Letter f): We assume that only functionality is meant here. It is possible, however, to perform functional tests with test data in conjunction with the trust service provider. We would appreciate clarification on this.

Paragraph 16

We propose the following wording: "Solutions that include qualified trust services in accordance with Regulation (EU) 910/2014 are considered to fulfil the criteria listed in paragraph 15. An additional technological assessment by the financial sector operator is not required."

Section 4.1.4 (Paragraphs 19 - 24)

We assume that, where a service provider is used, ongoing monitoring is to be implemented primarily by the service provider itself and in accordance with the stipulations in this section. In order to meet these requirements, the financial sector operator can only agree the criteria for ongoing monitoring with the service provider or define strategies, but cannot perform the technical monitoring itself.

Where this task is outsourced, additional requirements for outsourcing contained in the EBA Guidelines on Outsourcing Arrangements EBA/GL/2019/02 would also apply, which call for a review of the service provider by the institution. It should be clarified here that ongoing monitoring is covered by meeting the requirements contained in the EBA's Outsourcing Guidelines.

Paragraph 24

It would be useful for this data to be stored for a maximum of 10 years.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

3. Do you have any comments on the Guideline 4.2 'Acquisition of Information'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 25

Letter b): This data should not be stored in a machine-readable format such as OCR as this would require complex reformatting processes. Storing the data in commonly used formats would also be sufficient for the purpose of identifying the customer, also retrospectively.

Letter d): This requirement should be deleted or at least reworded. This places the responsibility on institutions to investigate every connection interruption, which seems unnecessary and unfeasible. Where identification cannot be completed, the onboarding process can be stopped and restarted at a later date, if necessary. For example, it might be that the customer's internet connection is not working. It is therefore an excessive amount of extra work, if not impossible, to investigate interruptions that they have no control over.

Paragraph 26

We assume that the requirements for proofs to be stored securely can be met from current standards to fulfil other criteria, such as ICT Risk Management Guidelines EBA/GL/2019/04, and other existing stipulations. Clarification on this would be helpful.

Paragraph 28

The data mentioned in the second sentence are not relevant for identifying the person. Preventing the spoofing of IP addresses and obfuscating of location data through VPNs can only be achieved with a disproportionate amount of effort.

The second sentence should be amended as follows: "This **may** also include situations where location data such as Internet Protocol (IP) addresses can be spoofed or services such as Virtual Private Networks (VPNs) used to obfuscate the location of the customer's device."

4. Do you have any comments on the Guideline 4.3 'Document Authenticity & Integrity'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 35

Since there are a number of technical solutions available, it should be up to the individual institution whether or not they use data collected by the customer's own device, e.g. via the eID function of a national identity card, in onboarding processes. As there is no uniform standard, it would be unreasonable to expect all technical solutions to be supported. If this option is technically supported by an institution, the customer must also give their explicit

consent before it can be used. The institution must also have the option, at its own discretion (for example, due to suspected misuse or known technical vulnerabilities), of refusing to use data collected by the customer's own device and of offering the customer a secure alternative.

5. Do you have any comments on the Guideline 4.4 'Authenticity Checks'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 39

The use of biometric data can only be referable to information from the trust service and end device provider in compliance with the required technical standards. More details on this would be helpful.

Paragraph 40

In process terms, this requirement would be difficult to implement because risk classification only occurs after all the relevant information about the customer has been obtained.

Paragraph 42

It should be clarified that face-to-face verification does not have to be performed in the same location as the remote checks. The last phrase in the sentence should therefore be deleted. A more flexible approach is required. If identity checks cannot be performed due to connection problems, it should be possible to simply repeat the process instead of proceeding to face-to-face verification.

Paragraph 45

Randomising the sequence of actions for verification is very difficult to do in practice and does not prevent collusion between customers and the responsible staff member. The only sensible and practicable measure available is to allocate incoming calls for video identification randomly to employees, which is already being done in practice.

Paragraph 46

Letters b), d) and e): In this phase of customer onboarding, there is as yet no established, secure channel of communication. Consequently, these requirements do not represent an additional safeguarding option. These requirements should therefore be removed.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

6. Do you have any comments on the Guideline 4.5 'Digital Identities'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 48

The approval of digital identity issuers for AML/CFT identification purposes is extremely important for the level of assurance of the procedures and legal certainty for the financial sector operators. The supervisor must have sufficient expertise about the procedures used no later than when they actually examine them. It would therefore be necessary to include a presumption of reliability for digital identities issued by issuers that have been authorised by state bodies. In such cases, banks need not perform additional level of assurance checks. There should definitely be relevant institutions at the national level that are able to grant authorisation to issuers that are not providers of qualified trust services.

Paragraph 49

We assume that, when using service providers, it is sufficient to call on those service providers to take appropriate measures, such as the level of assurance of employees, providing employees with special training etc. More details on this would be helpful.

Paragraph 51

We assume that a secure environment and strong authentication are to be understood within the meaning of EBA/RTS/2017/02. Is that correct?

Paragraph 52

Where a service provider is used, it must be sufficient to call on the service provider to take appropriate measures. Clarification would be helpful.

7. Do you have any comments on the Guideline 4.6 'Reliance on third parties and outsourcing'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

No comments.

GBIC Comments - Draft Guidelines on the use of Remote Customer Onboarding Solutions (EBA/CP/2021/40), 9 March 2022

8. Do you have any comments on the Guideline 4.7 'ICT and security risk management'? If you do not agree, please set out why you do not agree and if possible, provide evidence of the adverse impact provisions in this section would have.

Paragraph 63

It must be made clear that not all security measures need to be mentioned as this would lead to new risks.

Proposed wording of the last sentence:
"The customer or representative should be informed about all applicable security measures that should be taken to ensure secure use of the system."