EBA/GL /2025/02

11/02/2025

Final Report

Guidelines

amending Guidelines EBA/GL/2019/04 on ICT and security risk management

Contents

1. Background and rationale

1. On 27 November 2019, the EBA published the Guidelines on ICT and security risk management (EBA/GL/2019/04) which were built on the provisions of Article 74 of Directive 2013/36/EU (CRD)[1] and Article 95(3) of Directive (EU) 2015/2366 (PSD2)[2]. These Guidelines establish requirements for credit institutions, investment firms and payment service providers (PSPs)[3] on the mitigation and management of their information and communication technology (ICT) and security risks and aim to ensure a consistent and robust approach across the Single market. The Guidelines entered into force the following year and are applicable to the present day replacing those on security measures for operational and security risks (EBA GL/2017/17), which were repealed.

2. DORA entered into force in January 2023 and will apply from 17 January 2025 onwards. DORA introduced inter alia harmonised requirements for Information and communication technology (ICT), risk management framework (RMF), incident reporting, and third-party risk management and testing for 21 types of financial entities across the banking, insurance/pension and securities/markets sectors. The EBA, ESMA and EIOPA were mandated to develop 13 mandates in support of the Act, which were developed through a subcommittee in the Joint Committee (JC SC DOR)[4], including RTS on RMF.

3. The entities within DORA's scope of action cover some of the PSPs within the scope of PSD2, namely credit institutions (CIs), payment institutions (PIs), e-money institutions (EMIs), account information service providers (AISPs), exempted PIs and exempted EMIs. DORA amends PSD2 by exempting CIs, PIs, EMIs, AISPs, exempted PIs and exempted EMIs from the application of Article 96(1)-(5) of PSD2[5].

4. However, for some types of PSPs that are not covered by DORA the Guidelines apply. These include post office giro institutions which are entitled under national law to provide payment service.

5. Article 7(4) of Directive (EU) 2022/2556, amended Article 95(1) of PSD2 by adding the following subparagraph: "The first subparagraph is without prejudice to the application of Chapter II of Regulation (EU) 2022/2554 to:

[1] EBA mandate to further harmonise financial institutions' governance arrangements, processes and mechanisms across the EU regarding internal governance

[2] EBA mandate to issue guidelines with regard to the establishment, implementation and monitoring of security measures for operational and security risks.

[3] The provisions of the 'Guidelines on the security measures for operational and security risks of payment services' (EBA/GL/2017/17) were transposed and incorporated into Guidelines on ICT and security risk management in their entirety.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1774, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1774

[5] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35–127)

(a)payment service providers referred to in points (a), (b) and (d) of Article 1(1) of that Directive;

(b)account information service providers referred to in Article 33(1) of that Directive;

(c)payment institutions exempted pursuant to Article 32(1) of this Directive; and

(d)electronic money institutions benefitting from a waiver as referred to in Article 9(1) of Directive 2009/110/EC."

6. Since the entities subject to DORA and the related RTS on RMF overlap with some addressees of the EBA Guidelines on ICT and security risk management, to ensure transparency and legal certainty for entities within the scope of DORA and the EBA Guidelines, the question that arose is whether the EBA Guidelines should be amended or repealed.

7. Accordingly, the EBA has reviewed the Guidelines and has arrived at the view that the entities subject to the EBA Guidelines should be narrowed down and the scope of the Guidelines reduced to Guideline 3.8 on relationship management of the payment service users in relation to the provision of payment services, with the other parts of the guidelines repealed. The sub-sections below provide an overview of the assessment carried out by the EBA and the rationale behind the approach taken.

Entities subject to the EBA Guidelines

8. Article 2(2)(f) of DORA, explicitly excludes from the scope of action of DORA post office giro institutions. Accordingly, retaining a parallel and different set of ICT requirements for a subset of financial entities not covered by DORA will go contrary to the objectives of DORA.

9. The number of post office giro institutions is minimal: only 11 such institutions are currently operating as PSPs across 11 Member States (i.e. 1 per jurisdiction), while the remaining 16 EU Member States have no such institutions at all. Also, with the exception of one Member State, these post office giro institutions do not have any sizeable market share, in their respective national market, let alone the EU.

10. In addition, National Competent Authorities have the possibility to subject PSPs that are not covered by DORA to national requirements irrespective of the existence or not of EBA Guidelines. This means that Competent Authorities that have an appetite to retain the approach taken in the EBA Guidelines on ICT and security risk management for those PSPs can choose to maintain their existing national framework/measures; and

11. The separate proposal that the Commission published in June 2023 on the revision of PSD2 towards a PSD3/PSR also does not include any security measures requirements for post office giro institutions.

12. Credit institutions and investment firms as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013, addressees of the EBA Guidelines on ICT and security risk management overlap with the financial entities subject to DORA and the related RTS on RMF.

Scope of the EBA Guidelines

13. The EBA carried out a gap analysis in May 2024 and arrived at the view that the majority of the gaps identified which relate to authentication methods, requirements for the information security policy and ICT operations management, were not material and holistically covered by the new DORA framework.

14. However, in a subsequent assessment of the gap analysis performed, the EBA identified that the relationship management of the payment service users in relation to the provision of payment services were not covered by DORA as well as the post office giro institutions which are entitled under national law to provide payment service.

15. Given that the amendments made in these guideline stem from the fact that DORA enters into force and renders most part of these guidelines obsolete in substance, and due to the fact that the parts of these guidelines which will remain applicable have already been in place, it is disproportionate to conduct a public consultation and cost benefit analysis to that end.

Definitions of the EBA Guidelines

16. The definitions included in EBA Guidelines on ICT and security risk management overlap with DORA Article (3).

Next steps

17. The guidelines will be translated into the official EU languages and published on the EBA website along with a consolidated version The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from the data indicated in section 4.

2. Guidelines

EBA/GL/2025/02

11/02/2025

Guidelines

amending Guidelines EBA/2019/04 on ICT and security risk management

1. Compliance and reporting obligations

Status of these guidelines

1. This document contains guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010[1]. In accordance with Article 16(3) of Regulation (EU) No 1093/2010, competent authorities and financial institutions must make every effort to comply with the guidelines.

2. Guidelines set the EBA view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at institutions.

Reporting requirements

3. According to Article 16(3) of Regulation (EU) No 1093/2010, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by [dd.mm.yyyy]. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form available on the EBA website with the reference 'EBA/GL/2025/02'. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities. Any change in the status of compliance must also be reported to EBA.

4. Notifications will be published on the EBA website, in line with Article 16(3).

[1] Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC, (OJ L 331, 15.12.2010, p.12).

2. Addresses

5. These guidelines are addressed to competent authorities as defined in Article 4 point (2)(vii) of Regulation (EU) No 1093/2010 and to financial institutions as defined in Article 4(1) of Regulation No 1093/2010, which are payment service providers as referred to in Article 1(1) of Directive (EU) 2015/2366[2].

3. Implementation

Date of application

6. These guidelines apply from the latest by XX.XX.XXX [*2 months after issuance, i.e. publication of translated versions], at which point the precise date will be inserted here*].

4. Amendments

7. Guideline EBA/GL/2019/04 is amended as follows:

8. The subject matter as set out in paragraphs 5 and 6 is replaced with the following:

   'These guidelines are based on the mandate to issue guidelines under Article 95(3) of Directive (EU) 2015/2366 and cover aspects of payment user relationship management'.

   These guidelines complement the risk management measures under Digital Operational Resilience Act (DORA) and the related Regulatory Technical Standards that payment service providers referred to in paragraph 5 above must take, in accordance with Article 95(1) of PSD2, to manage the operational and security risks relating to the payment services they provide.

9. The scope of application as set out in paragraphs 7 and 8 is deleted.

[2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35–127)

‘‘These Guidelines specify requirements for the establishment, implementation and monitoring of the security measures that PSPs must take, in accordance with Article 95(1) of Directive (EU) 2015/2366, to manage the operational and security risks relating to the payment services they provide. ‘

10. The addressees as set out in paragraph 9 are replaced by the following:

‘These guidelines are addressed to competent authorities as defined in Article 4 point (2) point (vii) of Regulation (EU) No 1093/2010 and to financial institutions as defined in Article 4(1) of Regulation No 1093/2010, which are payment service providers as defined in Article 1(1) point (a), point (b) and point (d) of Directive (EU) 2015/2366, including natural or legal persons benefiting from an exemption pursuant to Article 32 or 33 of Directive (EU) 2015/2366 and legal persons exempted under Article 9 of Directive 2009/110/EC[3].’

11. The definitions as set out in paragraph 10 are deleted.

12. Paragraphs 1 to 91 which correspond to Sections 3.1 to 3.7 are deleted.

[3] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10/10/2009, p. 7–17)