EBA/GL/2025/02

11.002.2025

Leitlinien

zur Änderung der Leitlinien EBA/2019/04 für das Management von IKT- und Sicherheitsrisiken

1. Verpflichtung zur Einhaltung der Leitlinien und Meldepflichten

Status dieser Leitlinien

1. Das vorliegende Dokument enthält Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010[1] herausgegeben wurden. Gemäß Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen unternehmen, um den Leitlinien nachzukommen.

2. Die Leitlinien legen fest, was nach Ansicht der EBA angemessene Aufsichtspraktiken innerhalb des Europäischen Finanzaufsichtssystems sind oder wie das Unionsrecht in einem bestimmten Bereich anzuwenden ist. Zuständige Behörden im Sinne von Artikel 4 Nummer 2 der Verordnung (EU) Nr. 1093/2010 sollten die für sie geltenden Leitlinien einhalten, indem sie sie in geeigneter Weise in ihre Aufsichtspraktiken integrieren (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren), und zwar einschließlich der Leitlinien, die in erster Linie an Institute gerichtet sind.

Meldepflichten

3. Nach Artikel 16 Absatz 3 der Verordnung (EU) Nr. 1093/2010 müssen die zuständigen Behörden der EBA bis zum 20.05.2025 mitteilen, ob sie diesen Leitlinien nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Mitteilung ein, geht die EBA davon aus, dass die zuständigen Behörden den Anforderungen nicht nachkommen. Die Mitteilungen sind unter Verwendung des auf der Website der EBA abrufbaren Formulars mit dem Betreff „EBA/GL/2025/02“ zu übermitteln. Die Mitteilungen sollten durch Personen erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer zuständigen Behörde zu übermitteln. Jegliche Änderungen des Status der Einhaltung müssen der EBA ebenfalls gemeldet werden.

4. Die Meldungen werden gemäß Artikel 16 Absatz 3 der EBA-Verordnung auf der Website der EBA veröffentlicht.

[1] Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

2. Adressaten

5. Diese Leitlinien richten sich an zuständige Behörden und Institute im Sinne von Artikel 4 Absatz 2 Ziffer vii der Verordnung (EU) Nr. 1093/2010 sowie an Finanzinstitute im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010, bei denen es sich um Zahlungsdienstleister im Sinne von Artikel 1 Absatz 1 der Verordnung (EU) 2015/2366[2] handelt.

3. Umsetzung

Geltungsbeginn

6. Diese Leitlinien gelten spätestens ab dem 20.05.2025.

4. Änderungen

7. Die Leitlinien EBA/GL/2019/04 werden wie folgt geändert:

8. Der in den Absätzen 5 und 6 beschriebene Gegenstand wird durch folgenden Wortlaut ersetzt:

   „Diese Leitlinien ergeben sich aus dem Mandat zur Veröffentlichung von Leitlinien gemäß Artikel 95 Absatz 3 der Richtlinie (EU) 2015/2366 (PSD2) und decken Aspekte der Pflege der Kundenbeziehungen mit Zahlungsdienstnutzern ab.

   Diese Leitlinien ergänzen die Maßnahmen für das Management von Risiken gemäß der Verordnung über die digitale operationale Resilienz im Finanzsektor (Digital Operational Resilience Act, DORA) und den damit verbundenen technischen Regulierungsstandards, die die in Absatz 5 genannten Zahlungsdienstleister gemäß Artikel 95 Absatz 1 der PSD2 ergreifen müssen, um die operationellen und sicherheitsrelevanten Risiken in Bezug auf die von ihnen erbrachten Zahlungsdienste zu beherrschen.

9. Der in den Absätzen 7 und 8 festgelegte Anwendungsbereich wird gestrichen.

[2] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

„Diese Leitlinien enthalten Anforderungen für die Festlegung, Anwendung und Überwachung der Sicherheitsmaßnahmen, die die Zahlungsdienstleister gemäß Artikel 95 Absatz 1 der Richtlinie (EU) 2015/2366 zur Beherrschung der operationellen und sicherheitsrelevanten Risiken im Zusammenhang mit den von ihnen erbrachten Zahlungsdiensten ergreifen müssen."

10. Die Nennung der Adressaten in Absatz 9 wird durch folgenden Wortlaut ersetzt:

„Diese Leitlinien richten sich an zuständige Behörden im Sinne von Artikel 4 Absatz 2 Ziffer vii der Verordnung (EU) Nr. 1093/2010 und an Finanzinstitute im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010, bei denen es sich um Zahlungsdienstleister im Sinne von Artikel 1 Absatz 1 Buchstabe a, Buchstabe b und Buchstabe d der Verordnung (EU) 2015/2366 handelt, einschließlich natürlicher oder juristischer Personen, für die eine Ausnahme nach Artikel 32 oder Artikel 33 der Richtlinie (EU) 2015/2366 gilt, und juristische Personen, denen eine Freistellung nach Artikel 9 der Richtlinie 2009/110/EG[3] gewährt wird."

11. Die Begriffsbestimmungen gemäß Absatz 10 werden gestrichen.

12. Die Absätze 1 bis 91, die den Abschnitten 1.1 bis 1.7 entsprechen, werden gestrichen.

[3] Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).