JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

JC 2024 34

5. Juni 2024

Gemeinsame Leitlinien

für die Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste gemäß der Verordnung (EU) 2022/2554

Diese Leitlinien enthalten Verweise auf delegierte Verordnungen und Durchführungsverordnungen der Europäischen Kommission, die noch nicht im Amtsblatt der EU veröffentlicht wurden. Sobald diese Verordnungen im Amtsblatt veröffentlicht sind, werden diese Verweise in diese Leitlinien aufgenommen und die Leitlinien fertiggestellt. Die Verweise werden in die gelb markierten Abschnitte eingefügt.

Der Zeitpunkt der Anwendung dieser Leitlinien kann erst festgelegt werden, wenn diese Leitlinien fertiggestellt sind. Der voraussichtliche Zeitpunkt für die Anwendung dieser Leitlinien ist der 17. Januar 2025. Sollte es zu Verzögerungen bei der Fertigstellung dieser Leitlinien kommen, gelten diese Leitlinien spätestens zwei Monate nach dem Datum der Veröffentlichung der Übersetzungen dieser Leitlinien in allen Amtssprachen der EU.

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Gemeinsame Leitlinien für die Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste

Status dieser gemeinsamen Leitlinien

Dieses Dokument enthält gemeinsame Leitlinien, die gemäß Artikel 16 der Verordnung (EU) Nr. 1093/2010[1], Artikel 16 der Verordnung (EU) Nr. 1094/2010[2] und Artikel 16 der Verordnung (EU) Nr. 1095/2010[3] („die ESA-Verordnungen“) herausgegeben wurden. Gemäß Artikel 16 Absatz 3 der ESA-Verordnungen unternehmen die zuständigen Behörden und Finanzinstitute alle erforderlichen Anstrengungen, um diesen Leitlinien nachzukommen.

In den gemeinsamen Leitlinien wird dargelegt, welche Aufsichtspraktiken nach Ansicht der ESA im Rahmen des Europäischen Finanzaufsichtssystems angemessen sind oder wie das Unionsrecht in einem bestimmten Bereich angewendet werden sollte. Zuständige Behörden, an die sich die gemeinsamen Leitlinien richten, sollten diese in geeigneter Weise in ihre Aufsichtspraktiken aufnehmen (z. B. durch Änderung ihres Rechtsrahmens oder ihrer Aufsichtsverfahren), auch dann, wenn die gemeinsamen Leitlinien in erster Linie an Institute gerichtet sind.

Meldepflichten

Nach Artikel 16 Absatz 3 der ESA-Verordnungen müssen die zuständigen Behörden der jeweiligen ESA bis zum 19.05.2025 (zwei Monate nach der Herausgabe der Leitlinien) mitteilen, ob sie diesen gemeinsamen Leitlinien/Empfehlungen nachkommen oder nachzukommen beabsichtigen, oder die Gründe nennen, warum sie dies nicht tun. Geht innerhalb der genannten Frist keine Meldung ein, geht die jeweilige ESA davon aus, dass die zuständige Behörde den Leitlinien nicht nachkommt. Meldungen sind unter Angabe der Referenz „JC/GL/2024/34“ an compliance@eba.europa.eu, compliance@eiopa.europa.eu und DORA@esma.europa.eu zu richten. Eine entsprechende Meldevorlage steht auf den Websites der ESA zur Verfügung. Die Meldungen sollten durch Personen

[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] Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48-83).

[3] Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84-119).

erfolgen, die befugt sind, entsprechende Meldungen im Auftrag ihrer zuständigen Behörde zu übermitteln.

Die Meldungen werden gemäß Artikel 16 Absatz 3 auf den ESA-Websites veröffentlicht.

Titel I – Gegenstand, Anwendungsbereich, Adressaten und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

1. Mit diesen Leitlinien soll das den Europäischen Aufsichtsbehörden gemäß Artikel 11 Absatz 11 der Verordnung (EU) 2022/2554 [4] erteilte Mandat erfüllt werden, gemeinsame Leitlinien für die Schätzung der durch schwerwiegende IKT-bezogene Vorfälle verursachten aggregierten jährlichen Kosten gemäß Artikel 11 Absatz 10 dieser Verordnung auszuarbeiten. Diese Leitlinien enthalten auch eine gemeinsame Vorlage für die Meldung der aggregierten jährlichen Kosten und Verluste.

Adressaten

2. Diese Leitlinien richten sich an zuständige Behörden im Sinne von Artikel 46 der Verordnung (EU) 2022/2554 sowie an Finanzinstitute im Sinne von Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1093/2010, Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1094/2010 und Artikel 4 Absatz 1 der Verordnung (EU) Nr. 1095/2010.

Begriffsbestimmungen

3. Die in der Verordnung (EU) 2022/2554 verwendeten und definierten Begriffe haben in diesen Leitlinien dieselbe Bedeutung.

Titel II - Durchführung

Geltungsbeginn

4. Diese Leitlinien gelten ab dem 19.05.2025.

[4] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1-79).

Titel III – Bestimmungen über die Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste

5. Finanzunternehmen sollten die von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste schätzen, indem sie die Kosten und Verluste für schwerwiegende IKT-bezogene Vorfälle aggregieren, die in das Referenzjahr fallen, für das die zuständige Behörde die Schätzung angefordert hat. Finanzunternehmen können als Referenzjahr entweder das abgeschlossene Kalenderjahr oder das abgeschlossene Geschäftsjahr des Finanzunternehmens, für welches das Finanzunternehmen seinen Jahresabschluss erstellt hat, wählen. Die Entscheidung eines Finanzunternehmens, ob die Schätzung auf der Grundlage des Kalenderjahres oder des Geschäftsjahres vorgelegt wird, sollte auch bei künftigen Schätzungen der aggregierten jährlichen Kosten und Verluste gelten. Finanzunternehmen können diese Entscheidung ändern, indem sie dies der zuständigen Behörde mitteilen, und unter der Voraussetzung, dass die zuständige Behörde innerhalb von zwei Monaten nach Eingang der Mitteilung keine Einwände dagegen erhebt. Finanzunternehmen sollten Kosten und Verluste im Zusammenhang mit Vorfällen, die vor oder nach diesem Referenzjahr liegen, nicht berücksichtigen.

6. Finanzunternehmen sollten in die Schätzung alle IKT-bezogenen Vorfälle einbeziehen, die unabhängig von den Gründen gemäß der Delegierten Verordnung der Kommission [OJ L, 2024/1772, 25.6.2024][5] zur Klassifizierung von Vorfällen als schwerwiegend eingestuft wurden, und

   (a) für die das Finanzunternehmen in dem betreffenden Referenzjahr gemäß Artikel 19 Absatz 4 Buchstabe c der Verordnung (EU) 2022/2554 eine Abschlussmeldung vorgelegt hat, oder

   (b) Vorfälle, zu denen das Finanzunternehmen in früheren Referenzjahren gemäß Artikel 19 Absatz 4 Buchstabe c der Verordnung (EU) 2022/2554 eine Abschlussmeldung vorgelegt hat und die im betreffenden Referenzjahr quantifizierbare finanzielle Auswirkungen auf das Finanzunternehmen hatten.

7. Finanzunternehmen sollten die aggregierten jährlichen Kosten und Verluste schätzen, indem sie wie folgt vorgehen:

   (a) Sie sollten die Kosten und Verluste für jeden einzelnen schwerwiegenden IKT-bezogenen Vorfall schätzen. Bei diesen Schätzungen sollten die Bruttokosten und -verluste unter Berücksichtigung der Arten von Kosten und Verlusten gemäß Artikel 7 Absätze 1 und 2 der Delegierten Verordnung der Kommission [OJ L, 2024/1772, 25.6.2024] ermittelt werden;

[5] Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle. [*OJ L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj*]

(b) für jeden schwerwiegenden IKT-bezogenen Vorfall sollten Finanzunternehmen auch die finanziellen Wiedereinziehungen schätzen, wie in Anhang II der Durchführungsverordnung der Kommission [*OJ L, 2025/302, 20.2.2025*][6] festgelegt;

(c) Finanzunternehmen sollten die Bruttokosten und -verluste sowie die finanziellen Wiedereinziehungen für alle schwerwiegenden IKT-bezogenen Vorfälle aggregieren.

8. Als Grundlage für die Schätzungen sollten Finanzunternehmen die Kosten, Verluste und finanziellen Wiedereinziehungen heranziehen, die in ihren Jahresabschlüssen wie der Gewinn- und Verlustrechnung oder gegebenenfalls in ihren Meldungen des betreffenden Referenzjahres an die Aufsicht ausgewiesen sind. Bei ihrer Schätzung sollten Finanzunternehmen auch buchhalterische Rückstellungen einbeziehen, die in ihren Jahresabschlüssen wie der Gewinn- und Verlustrechnung des betreffenden Referenzjahres ausgewiesen sind. Sind keine genauen Daten verfügbar, sollten Finanzunternehmen ihre Schätzung so weit wie möglich auf andere verfügbare Daten und Informationen stützen.

9. Finanzunternehmen sollten Anpassungen der Kosten und Verluste einer Schätzung, die sie für ein Vorjahr vorgelegt haben, in die Schätzung des betreffenden Referenzjahres aufnehmen, in dem die Anpassungen vorgenommen wurden.

10. Finanzunternehmen sollten in der Meldung ihrer Schätzung der aggregierten jährlichen Kosten und Verluste auch die Aufschlüsselung der in die Aggregation einbezogenen Bruttokosten und -verluste und der finanziellen Wiedereinziehungen für jeden schwerwiegenden IKT-bezogenen Vorfall aufnehmen.

11. Finanzunternehmen sollten für die Übermittlung der Schätzung ihrer aggregierten jährlichen Kosten und Verluste für das Referenzjahr die im Anhang beigefügte Vorlage verwenden. Für jeden der in die Schätzung des Referenzjahres einbezogenen Posten gemäß den Absätzen 6 und 9 sollten Finanzunternehmen dieselben vom Finanzunternehmen bereitgestellten Referenzcodes für Vorfälle verwenden, die auch in der Abschlussmeldung gemäß Artikel 19 Absatz 4 Buchstabe c der Verordnung (EU) 2022/2554 verwendet werden.

[6] Durchführungsverordnung (EU) 2025/302 der Kommission vom 23. Oktober 2024 zur Festlegung technischer Durchführungsstandards für die Anwendung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates im Hinblick auf Standardformulare, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung. [*OJ L, 2025/302, 20.2.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj*]

Anhang: Meldevorlage für Bruttokosten und -verluste und finanzielle Wiedereinziehungen in einem Referenzjahr

Name des Finanzunternehmens	
Legal Entity Identifier (LEI-Code)	
Anfangs- und Enddatum des Referenzjahres des Finanzunternehmens	
Währung	

Nummer des Vorfalls	Datum der Einreichung der Abschlussmeldung des Vorfalls	Referenznummer des Vorfalls	Durch den Vorfall entstandene Bruttokosten und -verluste im Referenzjahr (Angaben in 1000)	Wiedereinziehungen in Bezug auf den Vorfall im Referenzjahr (Angaben in 1000)
1				
2				
…				
Gesamtbetrag für das Referenzjahr	----------	----------		