Amtsblatt
der Europäischen Union

DE
Reihe L

2025/301

20.2.2025

DELEGIERTE VERORDNUNG (EU) 2025/301 DER KOMMISSION

vom 23. Oktober 2024

zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung des Inhalts und der Fristen für die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung schwerwiegender IKT-bezogener Vorfälle sowie des Inhalts der freiwilligen Meldung erheblicher Cyberbedrohungen

(Text von Bedeutung für den EWR)

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz 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 ([1]), insbesondere auf Artikel 20 Absatz 3,

in Erwägung nachstehender Gründe:

(1) Um eine Harmonisierung und Vereinfachung der in Artikel 19 Absatz 4 der Verordnung (EU) 2022/2554 genannten Meldungen und Meldepflichten bei schwerwiegenden IKT-bezogenen Vorfällen sicherzustellen, sollten die Fristen für die Meldung schwerwiegender IKT-bezogener Vorfälle für alle Arten von Finanzunternehmen einem einheitlichen Ansatz folgen. Aus demselben Grund sollten die Fristen so weit wie möglich auch mit dem mit den Anforderungen der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([2]) verfolgten Ansatz in Einklang stehen oder zumindest eine gleichwertige Wirkung haben.

(2) Um die Finanzunternehmen zu dem Zeitpunkt, zu dem sie mit dem IKT-bezogenen Vorfall beschäftigt sind, nicht zusätzlich mit unangemessenem Meldeaufwand zu belasten, sollte sich der Inhalt der Erstmeldung auf die wichtigsten Informationen beschränken. Um angemessene Aufsichtsmaßnahmen ergreifen zu können, benötigen die zuständigen Behörden schnellstmöglich Informationen zu schwerwiegenden IKT-bezogenen Vorfällen, sobald das Finanzunternehmen einen solchen Vorfall als schwerwiegend eingestuft hat. Folglich sollte die Frist für die Übermittlung einer in Artikel 19 Absatz 4 Buchstabe a der Verordnung (EU) 2022/2554 genannten Erstmeldung nach Einstufung eines IKT-bezogenen Vorfalls als schwerwiegend so kurz wie möglich sein, wobei jedoch Finanzunternehmen, die für einen IKT-bezogenen Vorfall mehr Zeit benötigen, nachdem sie von diesem Kenntnis erlangt haben, Spielraum gewährt werden sollte, insbesondere bei nicht betont zeitkritischen Geschäftsmodellen im Dienstleistungssektor.

(3) Nach Eingang der Erstmeldung sollten die zuständigen Behörden in der Zwischenmeldung ausführlichere Informationen über den IKT-bezogenen Vorfall und in der Abschlussmeldung dann alle relevanten Informationen erhalten. Die in diesen Meldungen enthaltenen Informationen sollten es den zuständigen Behörden ermöglichen, den IKT-bezogenen Vorfall weiter zu bewerten und etwaige Aufsichtsmaßnahmen, die sie ergreifen möchten, zu prüfen.

(4) Die in Artikel 20 Absatz 1 Buchstabe a Ziffer ii der Verordnung (EU) 2022/2554 genannten Meldefristen sollten daher sicherstellen, dass die zuständigen Behörden die Informationen rasch erhalten, zugleich aber auch gewährleisten, dass den Finanzunternehmen ausreichend Zeit zur Verfügung steht, um sich vollständige und genaue Informationen zu beschaffen.

(5) Unter Berücksichtigung der in Artikel 20 Absatz 1 Buchstabe a der Verordnung (EU) 2022/2554 festgelegten Kriterien sollten die Meldefristen keine unverhältnismäßige Belastung für Kleinstunternehmen und andere nicht bedeutende Finanzunternehmen darstellen. Um eine unverhältnismäßige Belastung für Finanzunternehmen zu vermeiden, sollten die Meldefristen darüber hinaus Wochenenden und Feiertage berücksichtigen.

([1]) ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Da erhebliche Cyberbedrohungen auf freiwilliger Basis gemeldet werden, sollte der Inhalt solcher Meldungen keine Belastung für die Finanzunternehmen darstellen und weniger Informationen enthalten müssen als bei schwerwiegenden IKT-bezogenen Vorfällen.

(7) Diese Verordnung beruht auf dem Entwurf technischer Regulierungsstandards, der der Kommission von den Europäischen Aufsichtsbehörden übermittelt wurde.

(8) Die Europäischen Aufsichtsbehörden haben zu diesem Entwurf öffentliche Konsultationen durchgeführt, die damit verbundenen potenziellen Kosten- und Nutzeneffekte analysiert und die Stellungnahme der nach Artikel 37 der Verordnungen (EU) Nr. 1093/2010 ([3]), (EU) Nr. 1094/2010 ([4]) und (EU) Nr. 1095/2010 ([5]) des Europäischen Parlaments und des Rates eingesetzten Interessengruppen eingeholt.

(9) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([6]) konsultiert und gab am 22. Juli 2024 eine befürwortende Stellungnahme ab. Jede Verarbeitung personenbezogener Daten im Rahmen dieser Verordnung sollte im Einklang mit den einschlägigen Datenschutzgrundsätzen und den Bestimmungen der Verordnung (EU) 2018/1725 erfolgen —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Allgemeine Informationen, die in Erstmeldungen sowie in Zwischen- und Abschlussmeldungen schwerwiegender IKT-bezogener Vorfälle enthalten sein müssen

Finanzunternehmen nehmen in die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung gemäß Artikel 19 Absatz 4 der Verordnung (EU) 2022/2554 die folgenden allgemeinen Informationen auf:

a) Art der Übermittlung (Erstmeldung, Zwischenmeldung oder Abschlussmeldung),

b) Name des Finanzunternehmens, seinen LEI-Code und Art des Finanzunternehmens gemäß Artikel 2 Absatz 1 der Verordnung (EU) 2022/2554,

c) Name und Identifikationscode des Unternehmens, das die Erst-, Zwischen- oder Abschlussmeldung für das Finanzunternehmen übermittelt,

d) gegebenenfalls Namen und LEI-Codes aller Finanzunternehmen, die in der aggregierten Erst-, Zwischen- oder Abschlussmeldung erfasst sind,

e) Kontaktdaten der Personen, die für die Kommunikation mit der zuständigen Behörde über den schwerwiegenden IKT-bezogenen Vorfall verantwortlich sind,

f) gegebenenfalls Angabe des Mutterunternehmens der Gruppe, der das Finanzunternehmen angehört,

g) bei monetären Auswirkungen die Währung, in der die Beträge angegeben werden.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Artikel 2

Spezifische Informationen, die in Erstmeldungen enthalten sein müssen

Erstmeldungen gemäß Artikel 19 Absatz 4 Buchstabe a der Verordnung (EU) 2022/2554 enthalten mindestens alle nachfolgend genannten spezifischen Informationen:

a) vom Finanzunternehmen zugewiesener Referenzcode des Vorfalls,

b) Datum und Uhrzeit der Erkennung des Vorfalls sowie dessen Einstufung gemäß Artikel 8 der Delegierten Verordnung (EU) 2024/1772 der Kommission ([7]),

c) Beschreibung des IKT-bezogenen Vorfalls,

d) in den Artikeln 1 bis 8 der Delegierten Verordnung (EU) 2024/1772 festgelegte Kriterien, auf deren Grundlage das Finanzunternehmen den IKT-bezogenen Vorfall als schwerwiegend eingestuft hat,

e) Mitgliedstaaten, die von dem IKT-bezogenen Vorfall betroffen sind,

f) Angaben dazu, wie der IKT-bezogene Vorfall erkannt wurde,

g) soweit verfügbar, Angaben zum Ursprung des IKT-bezogenen Vorfalls,

h) Angaben dazu, ob das Finanzunternehmen einen Geschäftsfortführungsplan aktiviert hat,

i) gegebenenfalls Angaben zur Neueinstufung des schwerwiegenden IKT-bezogenen Vorfalls als nicht schwerwiegend,

j) soweit verfügbar, sonstige zweckdienliche Informationen.

Artikel 3

Spezifische Informationen, die in Zwischenmeldungen enthalten sein müssen

Zwischenmeldungen gemäß Artikel 19 Absatz 4 Buchstabe b der Verordnung (EU) 2022/2554 enthalten mindestens alle nachfolgend genannten spezifischen Informationen:

a) gegebenenfalls den von der zuständigen Behörde für den Vorfall mitgeteilten Referenzcode,

b) Datum und Uhrzeit des Eintretens des IKT-bezogenen Vorfalls,

c) gegebenenfalls Datum und Uhrzeit der Wiederaufnahme des regulären Geschäftsbetriebs des Finanzunternehmens,

d) Angaben dazu, inwieweit die in den Artikeln 1 bis 8 der Delegierten Verordnung (EU) 2024/1772 festgelegten Kriterien, auf deren Grundlage das Finanzunternehmen den IKT-bezogenen Vorfall als schwerwiegend eingestuft hat, erfüllt sind,

e) Art des IKT-bezogenen Vorfalls,

f) gegebenenfalls vom Angreifer artikulierte Bedrohungen und eingesetzte Techniken,

g) betroffene Funktionsbereiche und Geschäftsprozesse,

h) betroffene Infrastrukturkomponenten, die Geschäftsprozesse unterstützen,

i) Auswirkungen auf die finanziellen Interessen von Kunden,

j) Angaben zur Meldung des IKT-bezogenen Vorfalls an andere Behörden,

k) befristete Maßnahmen, die das Finanzunternehmen ergriffen hat oder zu ergreifen beabsichtigt, um sich von dem IKT-bezogenen Vorfall zu erholen,

l) gegebenenfalls Angaben zu Kompromittierungsindikatoren.

([7]) 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 (ABl. L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artikel 4

Spezifische Informationen, die in Abschlussmeldungen enthalten sein müssen

Abschlussmeldungen gemäß Artikel 19 Absatz 4 Buchstabe c der Verordnung (EU) 2022/2554 enthalten mindestens alle nachfolgend genannten spezifischen Informationen:

a) Angaben zu den Ursachen des IKT-bezogenen Vorfalls,

b) Datum und Uhrzeit der Behebung des IKT-bezogenen Vorfalls sowie der Beseitigung der zugrunde liegenden Ursache(n),

c) Angaben dazu, wie dem IKT-bezogenen Vorfall entgegengewirkt wurde,

d) gegebenenfalls Informationen, die für die Abwicklungsbehörden relevant sind,

e) Angaben zu direkten und indirekten Kosten und Verlusten, die infolge des IKT-bezogenen Vorfalls entstanden sind, und Angaben zu finanziellen Wiedereinziehungen,

f) gegebenenfalls Angaben zu wiederholten IKT-bezogenen Vorfällen.

Artikel 5

Fristen für die Erst-, Zwischen- und Abschlussmeldung

(1) Finanzunternehmen übermitteln die Erst-, Zwischen- und Abschlussmeldung gemäß Artikel 19 Absatz 4 Buchstaben a, b und c der Verordnung (EU) 2022/2554 innerhalb der folgenden Fristen:

a) bei der Erstmeldung: so früh wie möglich, in jedem Fall aber innerhalb von vier Stunden nach Einstufung des IKT-bezogenen Vorfalls als schwerwiegend und spätestens 24 Stunden nach dem Zeitpunkt, zu dem das Finanzunternehmen Kenntnis von dem IKT-bezogenen Vorfall erlangt hat,

b) bei der Zwischenmeldung: spätestens 72 Stunden nach Übermittlung der Erstmeldung, auch wenn sich gemäß Artikel 19 Absatz 4 Buchstabe b der Verordnung (EU) 2022/2554 der Status oder die Handhabung des Vorfalls nicht geändert hat. Die Finanzunternehmen übermitteln unverzüglich etwaige aktualisierte Zwischenmeldungen, in jedem Fall aber, sobald der reguläre Geschäftsbetrieb wiederaufgenommen wurde,

c) bei der Abschlussmeldung: spätestens einen Monat nach Übermittlung der Zwischenmeldung oder gegebenenfalls nach der letzten aktualisierten Zwischenmeldung.

(2) Hat das Finanzunternehmen einen IKT-bezogenen Vorfall nicht innerhalb von 24 Stunden nach dem Zeitpunkt, zu dem es Kenntnis von dem IKT-bezogenen Vorfall erlangt hat, sondern erst zu einem späteren Zeitpunkt als schwerwiegend eingestuft, übermittelt es die Erstmeldung innerhalb von vier Stunden, nachdem es den IKT-bezogenen Vorfall als schwerwiegend eingestuft hat.

(3) Finanzunternehmen, die nicht in der Lage sind, die Erstmeldung, die Zwischenmeldung oder die Abschlussmeldung innerhalb der in Absatz 1 genannten Fristen zu übermitteln, teilen dies der zuständigen Behörde unverzüglich, spätestens jedoch innerhalb der jeweiligen Fristen für die Übermittlung der Meldung mit und geben die Gründe für die Verzögerung an.

(4) Fällt die Frist für die Übermittlung der Erstmeldung, der Zwischenmeldung oder der Abschlussmeldung auf ein Wochenende oder einen Feiertag im Mitgliedstaat des meldenden Finanzunternehmens, so kann das Finanzunternehmen die Erstmeldung, die Zwischenmeldung oder die Abschlussmeldung bis 12.00 Uhr des darauffolgenden Arbeitstages übermitteln.

(5) Absatz 4 gilt nicht für die Übermittlung einer Erstmeldung oder einer Zwischenmeldung durch Kreditinstitute, zentrale Gegenparteien, Betreiber von Handelsplätzen und andere Finanzunternehmen, die gemäß Artikel 3 der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Einrichtungen eingestuft sind.

(6) Die zuständigen Behörden können beschließen, dass Absatz 4 nicht für die Übermittlung einer Erstmeldung oder einer Zwischenmeldung durch andere Finanzinstitute als die in Absatz 5 genannten gilt, die bedeutend oder für den Finanzsektor auf nationaler oder Unionsebene systemrelevant sind. Die zuständigen Behörden teilen den betreffenden Finanzunternehmen ihren Beschluss mit. Der Beschluss der zuständigen Behörde gilt nur für Vorfälle, die sich ereignet haben, nachdem die zuständige Behörde den betreffenden Finanzunternehmen ihre Entscheidung mitgeteilt hat.

Artikel 6

Inhalt der freiwilligen Meldung erheblicher Cyberbedrohungen

Eine freiwillige Meldung in Bezug auf erhebliche Cyberbedrohungen gemäß Artikel 19 Absatz 2 der Verordnung (EU) 2022/2554 umfasst Folgendes:

a) allgemeine Angaben zu dem meldenden Finanzunternehmen gemäß Artikel 1,

b) Datum und Uhrzeit der Erkennung einer erheblichen Cyberbedrohung und sonstige relevante Zeitstempel im Zusammenhang mit der erheblichen Cyberbedrohung,

c) Beschreibung der erheblichen Cyberbedrohung,

d) Angaben zu den möglichen Auswirkungen der erheblichen Cyberbedrohung auf das Finanzunternehmen, seine Kunden oder Gegenparteien im Finanzbereich,

e) Einstufungskriterien, die die Meldung eines schwerwiegenden Vorfalls gemäß den Artikeln 1 bis 8 der Delegierten Verordnung (EU) 2024/1772 ausgelöst hätten, wenn die Cyberbedrohung eingetreten wäre,

f) Angaben zum Status der erheblichen Cyberbedrohung und dazu, ob sich die Bedrohungsaktivität verändert hat,

g) gegebenenfalls Beschreibung der Maßnahmen, die das Finanzunternehmen ergriffen hat, um das Eintreten erheblicher Cyberbedrohungen zu verhindern,

h) Angabe dazu, ob andere Finanzunternehmen oder Behörden über die erhebliche Cyberbedrohung benachrichtigt wurden,

i) gegebenenfalls Angaben zu Kompromittierungsindikatoren,

j) soweit verfügbar, sonstige zweckdienliche Informationen.

Artikel 7

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 23. Oktober 2024

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN