



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**

(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 4,

in Erwägung nachstehender Gründe:

- (1) Um sicherzustellen, dass Finanzunternehmen den für sie zuständigen Behörden schwerwiegende Sicherheitsvorfälle einheitlich melden und diesen Behörden Daten von guter Qualität zur Verfügung stellen, sollte festgelegt werden, welche Datenfelder Finanzunternehmen in den verschiedenen Meldephasen nach Artikel 19 Absatz 4 der Verordnung (EU) 2022/2554 bereitstellen müssen. Es ist wichtig, dass diese Informationen in einer Weise dargestellt werden, die einen zentralen Überblick über den Vorfall gibt. Daher muss für diese Zwecke eine einheitliche Meldevorlage festgelegt werden.
- (2) Finanzunternehmen sollten diejenigen Datenfelder der Meldevorlage ausfüllen, die den Informationsanforderungen der betreffenden Meldung entsprechen. Finanzunternehmen, die bereits über Informationen verfügen, die sie zu einem späteren Meldezeitpunkt, d. h. in der Zwischen- oder Abschlussmeldung, bereitstellen müssen, sollten die Möglichkeit haben, die Übermittlung der Daten vorzuziehen.
- (3) Da mehrere oder wiederholte Vorfälle einen schwerwiegenden Vorfall im Sinne von Artikel 8 der Delegierten Verordnung (EU) 2024/1772 der Kommission⁽²⁾ darstellen können, sollten die Meldevorlage und die Datenfelder so gestaltet sein, dass die Finanzunternehmen solche wiederholten Vorfälle melden können.
- (4) Um sicherzustellen, dass korrekte und aktuelle Informationen zur Verfügung stehen, sollte die Meldevorlage es den Finanzunternehmen ermöglichen, bei der Übermittlung der Zwischen- und Abschlussmeldung alle zuvor bereits übermittelten Informationen zu aktualisieren und erforderlichenfalls schwerwiegende Vorfälle in nicht schwerwiegend zurückzustufen.
- (5) Die rechtliche Identifizierung der Unternehmen sollte an die Kennungen angepasst werden, die in den gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 erlassenen technischen Durchführungsstandards festgelegt sind.
- (6) Wenn Finanzunternehmen die Meldepflichten für schwerwiegende IKT-bezogene Vorfälle an einen Dritten auslagern, sollten die zuständigen Behörden die Identität des Dritten, der Meldungen im Namen des Finanzunternehmens übermittelt, bereits vor der Übermittlung der Erstmeldung kennen, um die Legitimität des meldenden Dritten überprüfen zu können.

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

⁽²⁾ 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 vom 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

- (7) Um die Auswirkungen eines Vorfalls, der bei einem Drittienstleister eingetreten ist oder von diesem verursacht wurde und mehrere Finanzunternehmen in demselben Mitgliedstaat betrifft, leicht einschätzen zu können und den Meldeaufwand für die Finanzunternehmen zu verringern, sollte die Meldevorlage die Übermittlung einer aggregierten Meldung mit aggregierten Informationen über die Auswirkungen des Vorfalls auf alle betroffenen Finanzunternehmen, die den Vorfall als schwerwiegend eingestuft haben, ermöglichen.
- (8) Die Meldevorlage sollte technologienutral gestaltet sein, damit sie in verschiedene Lösungen für die Meldung von Sicherheitsvorfällen implementiert werden kann, die zwecks Umsetzung der Anforderungen der Verordnung (EU) 2022/2554 bereits bestehen oder noch entwickelt werden.
- (9) Die Gestaltung der Meldevorlage und der Datenfelder sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Dritte, an die Finanzunternehmen ihre Meldepflicht gemäß Artikel 19 Absatz 5 der Verordnung (EU) 2022/2554 ausgelagert haben, erleichtern.
- (10) Die vorliegende Verordnung beruht auf dem Entwurf technischer Durchführungsstandards, der der Kommission von den Europäischen Aufsichtsbehörden übermittelt wurde.
- (11) 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 (¹), (EU) Nr. 1094/2010 (²) und (EU) Nr. 1095/2010 (³) des Europäischen Parlaments und des Rates eingesetzten Interessengruppe Bankensektor eingeholt.
- (12) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates (⁴) konsultiert und gab am 22. Juli 2024 eine befürwortende Stellungnahme ab. Jede Verarbeitung personenbezogener Daten im Anwendungsbereich dieser Verordnung sollte im Einklang mit den geltenden Datenschutzgrundsätzen und -bestimmungen der Verordnung (EU) 2018/1725 erfolgen.

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Vorlage für die Meldung schwerwiegender IKT-bezogener Vorfälle

- (1) Finanzunternehmen verwenden für die Übermittlung der in Artikel 19 Absatz 4 der Verordnung (EU) 2022/2554 genannten Erstmeldung, Zwischenmeldung und Abschlussmeldung die Vorlage in Anhang I wie folgt:
- a) Finanzunternehmen, die eine Erstmeldung übermitteln, füllen diejenigen Datenfelder der Vorlage aus, die den nach Artikel 2 der Delegierten Verordnung (EU) 2025/301 der Kommission (⁵) geforderten Informationen entsprechen, und können, wenn sie bereits über diese Informationen verfügen, diejenigen Datenfelder ausfüllen, die nicht für eine Erstmeldung, sondern für eine Zwischen- oder Abschlussmeldung ausgefüllt werden müssen.

(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. ELI: <http://data.europa.eu/eli/reg/2010/1093/oj>).

(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. ELI: <http://data.europa.eu/eli/reg/2010/1094/oj>).

(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. ELI: <http://data.europa.eu/eli/reg/2010/1095/oj>).

(⁴) 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>).

(⁵) 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. (Abl. L 2025/301 vom 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) Finanzunternehmen, die eine Zwischenmeldung übermitteln, füllen diejenigen Datenfelder der Vorlage aus, die den nach Artikel 3 der Delegierten Verordnung (EU) 2025/301 geforderten Informationen entsprechen, und können, wenn sie bereits über diese Informationen verfügen, diejenigen Datenfelder ausfüllen, die nicht für eine Zwischenmeldung, sondern für eine Abschlussmeldung ausgefüllt werden müssen.

c) Finanzunternehmen, die eine Abschlussmeldung übermitteln, füllen diejenigen Datenfelder der Vorlage aus, die den nach Artikel 4 der Delegierten Verordnung (EU) 2025/301 geforderten Informationen entsprechen.

(2) Die Finanzunternehmen stellen sicher, dass die in der Erstmeldung sowie in der Zwischenmeldung und der Abschlussmeldung enthaltenen Informationen vollständig und korrekt sind.

(3) Finanzunternehmen geben, soweit möglich, Schätzwerte auf der Grundlage anderer verfügbarer Daten und Informationen an, wenn zum Zeitpunkt der Erstmeldung oder der Zwischenmeldung keine genauen Daten verfügbar sind.

(4) Bei der Übermittlung einer Zwischen- oder Abschlussmeldung verwenden Finanzunternehmen die Vorlage in Anhang I, um alle erforderlichen Informationen zu übermitteln und gegebenenfalls die Informationen zu aktualisieren, die zuvor in der Erstmeldung oder in der Zwischenmeldung übermittelt wurden.

(5) Beim Ausfüllen der Vorlage in Anhang I beachten die Finanzunternehmen das Datenglossar und die Anleitung in Anhang II.

Artikel 2

Gleichzeitige Übermittlung der Erst-, Zwischen- und Abschlussmeldung

Finanzunternehmen können die Erstmeldung, die Zwischenmeldung und die Abschlussmeldung zusammenlegen und zwei oder alle Meldungen gleichzeitig übermitteln, wenn der reguläre Geschäftsbetrieb wiederhergestellt ist oder die Ursachenanalyse abgeschlossen wurde und die Fristen gemäß Artikel 5 der Delegierten Verordnung (EU) 2025/301 eingehalten werden.

Artikel 3

Wiederholte IKT-bezogene Vorfälle

Finanzunternehmen, die Informationen über wiederholte nicht schwerwiegende IKT-bezogene Vorfälle bereitstellen, die zusammen die Voraussetzungen für einen schwerwiegenden IKT-bezogenen Vorfall gemäß Artikel 8 Absatz 2 der Delegierten Verordnung (EU) 2024/1772 erfüllen, übermitteln diese Informationen in aggregierter Form.

Artikel 4

Nutzung sicherer elektronischer Kanäle

(1) Finanzunternehmen nutzen sichere elektronische Kanäle, die von ihrer zuständigen Behörde für die Übermittlung der Erst-, Zwischen- und Abschlussmeldung bereitgestellt werden.

(2) Finanzunternehmen, die nicht in der Lage sind, die von ihrer zuständigen Behörde bereitgestellten sicheren elektronischen Kanäle zu nutzen, unterrichten ihre zuständige Behörde im Einvernehmen mit der zuständigen Behörde auf andere sichere Weise über einen schwerwiegenden IKT-bezogenen Vorfall. Auf Verlangen der zuständigen Behörde übermitteln Finanzunternehmen die Erst-, Zwischen- oder Abschlussmeldung erneut über den von ihrer zuständigen Behörde bereitgestellten sicheren elektronischen Kanal, sobald sie dazu in der Lage sind.

Artikel 5

Rückstufung schwerwiegender IKT-bezogener Vorfälle

Kommt das Finanzunternehmen nach eingehender Prüfung zu dem Schluss, dass der zuvor als „schwerwiegend“ gemeldete IKT-bezogene Vorfall zu keinem Zeitpunkt die in Artikel 8 der Delegierten Verordnung (EU) 2024/1772 festgelegten Einstufungskriterien und Schwellenwerte erfüllte, so teilt es der zuständigen Behörde mit, dass es den IKT-bezogenen Vorfall von „schwerwiegend“ auf „nicht schwerwiegend“ zurückgestuft hat, und macht in der Vorlage in Anhang II dieser Verordnung in den Feldern „Art der Meldung“ und „Sonstige Informationen“ entsprechende Angaben zu dieser Rückstufung.

Artikel 6

Unterrichtung über die Auslagerung der Berichtspflichten

- (1) Finanzunternehmen, die die Verpflichtung zur Meldung schwerwiegender IKT-bezogener Vorfälle gemäß Artikel 19 Absatz 5 der Verordnung (EU) 2022/2554 ausgelagert haben, unterrichten ihre zuständige Behörde über die Vereinbarung zur Auslagerung, sobald diese abgeschlossen wurde, spätestens jedoch vor der ersten Meldung.
- (2) Finanzunternehmen teilen der zuständigen Behörde den Namen, die Kontaktdaten und den Identifikationscode des Dritten mit, der die Meldungen schwerwiegender IKT-bezogener Vorfälle für sie übermitteln wird.
- (3) Finanzunternehmen unterrichten ihre zuständige Behörde, sobald sie ihre Meldepflichten gemäß Artikel 19 Absatz 5 der Verordnung (EU) 2022/2554 nicht mehr auslagern.

Artikel 7

Aggregierte Meldung

- (1) Ein Drittdienstleister, an den Meldepflichten gemäß Artikel 19 Absatz 5 der Verordnung (EU) 2022/2554 ausgelagert wurden, kann die Vorlage in Anhang I dieser Verordnung verwenden, um aggregierte Informationen über einen schwerwiegenden IKT-bezogenen Vorfall, der sich auf mehrere Finanzunternehmen auswirkt, in einer einzigen Meldung bereitzustellen und diese Meldung im Namen aller betroffenen Finanzunternehmen der zuständigen Behörde zu übermitteln, sofern alle folgenden Voraussetzungen erfüllt sind:
 - a) Der zu meldende schwerwiegende IKT-bezogene Vorfall hat bei einem IKT-Drittdienstleister seinen Ursprung oder wird von diesem verursacht.
 - b) Dieser Drittdienstleister erbringt die betreffende IKT-Dienstleistung für mehr als ein Finanzunternehmen oder für eine Gruppe.
 - c) Der IKT-bezogene Vorfall wird von jedem in der aggregierten Meldung erfassten Finanzunternehmen als schwerwiegend eingestuft.
 - d) Der schwerwiegende IKT-bezogene Vorfall betrifft Finanzunternehmen im selben Mitgliedstaat und die aggregierte Meldung bezieht sich auf Finanzunternehmen, die von derselben zuständigen Behörde beaufsichtigt werden.
 - e) Die zuständigen Behörden haben dieser Art von Finanzunternehmen ausdrücklich gestattet, aggregierte Meldungen zu übermitteln.
- (2) Absatz 1 gilt nicht für Kreditinstitute, die gemäß Artikel 2 Nummer 16 der Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank (¹) als von erheblicher Bedeutung angesehen werden, Betreiber von Handelsplätzen und zentrale Gegenparteien, die nur die Vorlage in Anhang I verwenden, um Meldungen schwerwiegender IKT-bezogener Vorfälle einzeln an ihre zuständige Behörde zu übermitteln.

- (3) Verlangen die zuständigen Behörden Informationen über die individuellen Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls auf ein einzelnes Finanzunternehmen, so übermittelt das Finanzunternehmen auf Ersuchen der zuständigen Behörde eine Einzelmeldung über den schwerwiegenden IKT-bezogenen Vorfall.

(¹) Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank vom 16. April 2014 zur Einrichtung eines Rahmenwerks für die Zusammenarbeit zwischen der Europäischen Zentralbank und den nationalen zuständigen Behörden und den nationalen benannten Behörden innerhalb des einheitlichen Aufsichtsmechanismus (SSM-Rahmenverordnung) (EZB/2014/17) (Abl. L 141 vom 14.5.2014, S. 1, ELI: <http://data.europa.eu/eli/reg/2014/468/oj>).

Artikel 8

Meldung erheblicher Cyberbedrohungen

(1) Finanzunternehmen, die den zuständigen Behörden gemäß Artikel 19 Absatz 2 der Verordnung (EU) 2022/2554 erhebliche Cyberbedrohungen melden, verwenden die Vorlage in Anhang III dieser Verordnung und befolgen das Datenglossar und die Anleitung in Anhang IV dieser Verordnung.

(2) Finanzunternehmen stellen sicher, dass die in der Meldung erheblicher Cyberbedrohungen enthaltenen Informationen vollständig und korrekt sind.

Artikel 9

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

ANHANG I

VORLAGEN FÜR DIE MELDUNG SCHWERWIEGENDER SICHERHEITSVORFÄLLE

| Feld-nummer | Datenfeld | |
|---|--|--|
| Allgemeine Angaben zum Finanzunternehmen | | |
| 1.1 | Art der Übermittlung | |
| 1.2 | Name des Unternehmens, das die Meldung übermittelt | |
| 1.3 | Identifikationscode des Unternehmens, das die Meldung übermittelt | |
| 1.4 | Art des betroffenen Finanzunternehmens | |
| 1.5 | Name des betroffenen Finanzunternehmens | |
| 1.6 | LEI-Code des betroffenen Finanzunternehmens | |
| 1.7 | Name des Hauptansprechpartners | |
| 1.8 | E-Mail-Adresse des Hauptansprechpartners | |
| 1.9 | Telefonnummer des Hauptansprechpartners | |
| 1.10 | Name des zweiten Ansprechpartners | |
| 1.11 | E-Mail-Adresse des zweiten Ansprechpartners | |
| 1.12 | Telefonnummer des zweiten Ansprechpartners | |
| 1.13 | Name des obersten Mutterunternehmens | |
| 1.14 | LEI-Code des obersten Mutterunternehmens | |
| 1.15 | Meldewährung | |
| Inhalt der Erstmeldung | | |
| 2.1 | Vom Finanzunternehmen zugewiesener Referenzcode für den Vorfall | |
| 2.2 | Datum und Uhrzeit der Feststellung des schwerwiegenden IKT-bezogenen Vorfalls | |
| 2.3 | Datum und Uhrzeit der Einstufung des IKT-bezogenen Vorfalls als schwerwiegend | |
| 2.4 | Beschreibung des schwerwiegenden IKT-bezogenen Vorfalls | |
| 2.5 | Einstufungskriterien, die die Meldung des Vorfalls ausgelöst haben | |
| 2.6 | Wesentlichkeitsschwellen für das Einstufungskriterium „Geografische Ausbreitung“ | |
| 2.7 | Feststellung des schwerwiegenden IKT-bezogenen Vorfalls | |

| Feld-nummer | Datenfeld | |
|-------------|---|--|
| 2.8 | Angabe, ob der schwerwiegende IKT-bezogene Vorfall bei einem Drittienstleister oder einem anderen Finanzunternehmen seinen Ursprung hat | |
| 2.9 | Aktivierung des Plans zur Aufrechterhaltung des Geschäftsbetriebs, falls aktiviert | |
| 2.10 | Sonstige zweckdienliche Angaben | |

Inhalt der Zwischenmeldung

| | | |
|------|--|--|
| 3.1 | Von der zuständigen Behörde bereitgestellter Referenzcode für den Vorfall | |
| 3.2 | Datum und Uhrzeit des Eintretens des schwerwiegenden IKT-bezogenen Vorfalls | |
| 3.3 | Datum und Uhrzeit der Wiederherstellung der Dienste, Tätigkeiten oder Vorgänge | |
| 3.4 | Anzahl der betroffenen Kunden | |
| 3.5 | Prozentsatz der betroffenen Kunden | |
| 3.6 | Anzahl der betroffenen Gegenparteien im Finanzbereich | |
| 3.7 | Prozentsatz der betroffenen Gegenparteien im Finanzbereich | |
| 3.8 | Auswirkungen auf einschlägige Kunden oder Gegenparteien im Finanzbereich | |
| 3.9 | Anzahl der betroffenen Transaktionen | |
| 3.10 | Prozentsatz der betroffenen Transaktionen | |
| 3.11 | Wert der betroffenen Transaktionen | |
| 3.12 | Angaben dazu, ob es sich um tatsächliche Zahlen oder Schätzungen handelt oder ob es keine Auswirkungen gegeben hat | |
| 3.13 | Reputationsschaden | |
| 3.14 | Kontextbezogene Angaben zum Reputationsschaden | |
| 3.15 | Dauer des schwerwiegenden IKT-bezogenen Vorfalls | |
| 3.16 | Ausfallzeiten | |
| 3.17 | Angaben dazu, ob es sich bei der Dauer und den Ausfallzeiten um tatsächliche Zahlen oder Schätzungen handelt | |
| 3.18 | Arten von Auswirkungen in den Mitgliedstaaten | |
| 3.19 | Beschreibung der Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls in anderen Mitgliedstaaten | |
| 3.20 | Wesentlichkeitsschwellen für das Einstufungskriterium „Datenverluste“ | |
| 3.21 | Beschreibung der Datenverluste | |

| Feld-nummer | Datenfeld | |
|-------------|---|--|
| 3.22 | Einstufungskriterium „Betroffene kritische Dienstleistungen“ | |
| 3.23 | Art des schwerwiegenden IKT-bezogenen Vorfalls | |
| 3.24 | Andere Arten von Vorfällen | |
| 3.25 | Bedrohungen und Techniken des Angreifers | |
| 3.26 | Andere Arten von Techniken | |
| 3.27 | Angaben zu betroffenen Funktionsbereichen und Geschäftsprozessen | |
| 3.28 | Betroffene Infrastrukturkomponenten, die Geschäftsprozesse unterstützen | |
| 3.29 | Angaben zu betroffenen Infrastrukturkomponenten, die Geschäftsprozesse unterstützen | |
| 3.30 | Auswirkungen auf die finanziellen Interessen von Kunden | |
| 3.31 | Meldung an andere Behörden | |
| 3.32 | Angabe der „anderen“ Behörden | |
| 3.33 | Ergriffene oder geplante befristete Maßnahmen zur Wiederherstellung nach dem Vorfall | |
| 3.34 | Beschreibung etwaiger ergriffener oder geplanter befristeter Maßnahmen zur Wiederherstellung nach dem Vorfall | |
| 3.35 | Kompromittierungsindikatoren | |

Inhalt der Abschlussmeldung

| | | |
|------|---|--|
| 4.1 | Übergeordnete Einstufung der Ursachen des Vorfalls | |
| 4.2 | Detaillierte Einstufung der Ursachen des Vorfalls | |
| 4.3 | Weitergehende Einstufung der Ursachen des Vorfalls | |
| 4.4 | Andere Arten von Ursachen | |
| 4.5 | Angaben zu den Ursachen des Vorfalls | |
| 4.6 | Zusammenfassung der Behebung des Vorfalls | |
| 4.7 | Datum und Uhrzeit der Behebung der Ursache des Vorfalls | |
| 4.8 | Datum und Uhrzeit der Behebung des Vorfalls | |
| 4.9 | Angabe, falls das Datum der dauerhaften Behebung des Vorfalls von dem ursprünglich geplanten Umsetzungsdatum abweicht | |
| 4.10 | Bewertung des Risikos für kritische Funktionen für Abwicklungszwecke | |
| 4.11 | Für Abwicklungsbehörden relevante Angaben | |

| Feld-nummer | Datenfeld |
|-------------|---|
| 4.12 | Wesentlichkeitsschwelle für das Einstufungskriterium „Wirtschaftliche Auswirkungen“ |
| 4.13 | Betrag der direkten und indirekten Bruttokosten und Verluste |
| 4.14 | Betrag der finanziellen Rückflüsse |
| 4.15 | Angaben dazu, ob sich die nicht schwerwiegenden Vorfälle wiederholt haben |
| 4.16 | Datum und Uhrzeit des Eintretens wiederholter Vorfälle |

ANHANG II

DATENGLOSSAR UND ANLEITUNG FÜR DIE MELDUNG SCHWERWIEGENDER SICHERHEITSVORFÄLLE

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--|--|-----------------------------------|---------------------------------------|--|---|
| Allgemeine Angaben zum Finanzunternehmen | | | | | |
| 1.1. Art der Übermittlung | Geben Sie die Art der Meldung des Vorfalls an, die der zuständigen Behörde übermittelt wird. | Ja | Ja | Ja | Auswahl: — Erstmeldung; — Zwischenmeldung; — Abschlussmeldung; — Schwerwiegender Vorfall, der in nicht schwerwiegend zurückgestuft wurde. |
| 1.2. Name des Unternehmens, das die Meldung übermittelt | Vollständige juristische Bezeichnung des Unternehmens, das die Meldung übermittelt. | Ja | Ja | Ja | Alphanumerisch |
| 1.3. Identifikationscode des Unternehmens, das die Meldung übermittelt | Identifikationscode des Unternehmens, das die Meldung übermittelt. Übermitteln Finanzunternehmen die Meldung, ist die Rechtsträgerkennung (Legal Entity Identifier; LEI-Code), ein eindeutiger alphanumerischer 20-stelliger Code nach ISO 17442-1:2020. Ein Drittdienstleister, der eine Meldung für ein Finanzunternehmen übermittelt, kann eine Rechtsträgerkennung verwenden, die in den gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 angenommenen technischen Durchführungsstandards festgelegt ist. | Ja | Ja | Ja | Alphanumerisch |
| 1.4. Art des betroffenen Finanzunternehmens | Art des Unternehmens gemäß Artikel 2 Absatz 1 Buchstaben a bis t der Verordnung (EU) 2022/2554, für das die Meldung übermittelt wird. Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung sind die verschiedenen Arten von Finanzunternehmen auszuwählen, die in der aggregierten Meldung erfasst sind. | Ja | Ja | Ja | Auswahl (Mehr-fach-auswahl): — Kreditinstitut; — Zahlungs-institut; — Ausge-nommenes Zahlungs-institut; — Kontoinfor-mationsdienst-leister; — E-Geld-Institut; — Ausge-nommenes E-Geld-Institut; — Wertpapier-firma; — Anbieter Kryptowerte-Dienstleis-tungen; — von Emittent wertreferen-zierter Token; — Zentral-verwahrer; — Zentrale Gegenpartei; — Handelsplatz; — Transak-tionsregister; |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|---|---|---|---|--|
| | | | | | <ul style="list-style-type: none"> — Verwalter alternativer Investment-fonds; — Verwaltungs-gesellschaft; — Datenbereit-stellungsdiest; — Versicherungs- und Rückversiche-rungsunter-nehmen; — Versicherungs-vermittler, Rückversiche-rungsvermittler und Versicherungs-vermittler in Nebentätigkeit; — Einrichtung der betrieblichen Altersverso-rung; — Ratingagentur; — Administrator kritischer Referenzwerte; — Schwarm-finanzierungs-dienstleister; — Verbriefungs-register. |
| 1.5. Name des betroffenen Finanzunternehmens | <p>Vollständige juristische Bezeichnung des von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Finanzunternehmens, das gemäß Artikel 19 der Verordnung (EU) 2022/2554 seiner zuständigen Behörde den schwerwiegenden Vorfall melden muss.</p> <p>Bei aggregierter Meldung:</p> <ul style="list-style-type: none"> a) Auflistung aller Namen der von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Finanzunternehmen, getrennt durch ein Semikolon. b) Der Dritt-dienstleister, der eine Meldung eines schwerwiegenden Vorfalls oder in aggregierter Form gemäß Artikel 7 dieser Verordnung übermittelt, führt die Namen aller von dem Vorfall betroffenen Finanzunternehmen auf, getrennt durch ein Semikolon. | Ja, wenn es sich bei dem von dem Vorfall betroffenen Finanzun-ter-nehmen nicht um das Unterneh-men handelt, das die Meldung übermit-telt, und im Falle einer aggregierten Meldung | Ja, wenn es sich bei dem von dem Vorfall betroffe-nen Finanz-un-ter-nehmen nicht um das Unter-neh-men handelt, das die Meldung übermit-telt, und im Falle einer aggre-gierten Meldung | Ja, wenn es sich bei dem von dem Vorfall betroffenen Finanzun-ter-nehmen nicht um das Unterneh-men handelt, das die Meldung übermit-telt, und im Falle einer aggregierten Meldung | Alphanumerisch |
| 1.6. LEI-Code des betroffenen Finanzunternehmens | <p>Der nach der Internationalen Organisation für Normung zugewiesene LEI-Code des von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Finanzunternehmens.</p> <p>Bei aggregierter Meldung:</p> <ul style="list-style-type: none"> a) Auflistung aller LEI-Codes der von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Finanzunternehmen, getrennt durch ein Semikolon; | Ja, wenn es sich bei dem von dem schwerwiegen-den IKT-bezogenen Vorfall betroffenen | Ja, wenn es sich bei dem von dem schwer-wiegen-den IKT-bezogenen Vorfall betroffe-nen | Ja, wenn es sich bei dem von dem schwer-wiegen-den IKT-bezogenen Vorfall | Eindeutiger alphanumerischer Code mit 20 Zeichen nach ISO 17442-1:2020 |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-mel-dung | Verpflichtend für die Abschluss-mel-dung | Feldtyp |
|--|--|--|---|--|----------------|
| | <p>b) der Dritt Dienstleister, der eine Meldung eines schwerwiegenden Vorfalls in aggregierter Form gemäß Artikel 7 dieser Verordnung übermittelt, führt die LEI-Codes aller von dem Vorfall betroffenen Finanzunternehmen auf, getrennt durch ein Semikolon.</p> <p>Die Reihenfolge der Auflistung der LEI-Codes muss mit derjenigen der Namen der Finanzunternehmen identisch sein.</p> | Finan-zun-ter-neh-men nicht um das Unterneh-men handelt, das die Meldung übermittelt, und bei einer aggregierten Meldung | Finanz-unter-neh-men nicht um das Unterneh-men handelt, das die Meldung übermittelt, und bei einer aggregierten Meldung | betroffenen Finan-zun-ter-neh-men nicht um das Unterneh-men handelt, das die Meldung übermittelt, und bei einer aggregierten Meldung | |
| 1.7. Name des Hauptansprech-partners | <p>Vor- und Nachname des Hauptansprechpartners des Finanzunternehmens.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung der Name des Hauptansprechpartners in dem Unternehmen, das die aggregierte Meldung übermittelt.</p> | Ja | Ja | Ja | Alphanumerisch |
| 1.8. E-Mail-Adresse des Hauptansprech-partners | <p>E-Mail-Adresse des Hauptansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die E-Mail-Adresse des Hauptansprechpartners in dem Unternehmen, das die aggregierte Meldung übermittelt.</p> | Ja | Ja | Ja | Alphanumerisch |
| 1.9. Telefonnummer des Hauptansprech-partners | <p>Telefonnummer des Hauptansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die Telefonnummer des Hauptansprechpartners in dem Unternehmen, das die aggregierte Meldung übermittelt.</p> <p>Die Telefonnummer ist mit allen internationalen Vorwahlen anzugeben (z. B. +33 XXXXXXXX).</p> | Ja | Ja | Ja | Alphanumerisch |
| 1.10. Name des zweiten Ansprech-partners | Vor- und Nachname des zweiten Ansprechpartners oder Name des verantwortlichen Teams des Finanzunternehmens oder des Unternehmens, das die Meldung im Namen des Finanzunternehmens übermittelt | Ja | Ja | Ja | Alphanumerisch |
| 1.11. E-Mail-Adresse des zweiten Ansprech-partners | E-Mail-Adresse des zweiten Ansprechpartners oder die funktionale E-Mail-Adresse des Teams, an die bzw. das sich die zuständige Behörde in der Folgemitteilung wenden kann. | Ja | Ja | Ja | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|---|--|--|--|--|
| 1.12. Telefonnummer des zweiten Ansprechpartners | Telefonnummer des zweiten Ansprechpartners oder eines Teams, an den bzw. das sich die zuständige Behörde in der Folgemitteilung wenden kann. Die Telefonnummer ist mit allen internationalen Vorwahlen anzugeben (z. B. +33 XXXXXXXX). | Ja | Ja | Ja | Alphanumerisch |
| 1.13. Name des obersten Mutterunternehmens | Gegebenenfalls Name des obersten Mutterunternehmens der Gruppe, der das betroffene Finanzunternehmen angehört. | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Alphanumerisch |
| 1.14. LEI-Code des obersten Mutterunternehmens | Gegebenenfalls LEI-Code des obersten Mutterunternehmens der Gruppe, der das betroffene Finanzunternehmen angehört. Zugewiesen gemäß der Internationalen Organisation für Normung. | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Ja, wenn das Finanzunternehmen einer Gruppe angehört | Eindeutiger alphanumerischer Code mit 20 Zeichen nach ISO 17442-1:2020 |
| 1.15. Meldewährung | Währung, die für die Meldung des Vorfalls verwendet wird. | Ja | Ja | Ja | Auswahl ist anhand der ISO 4217 Währungscodes zu treffen |
| Inhalt der Erstmeldung | | | | | |
| 2.1. Vom Finanzunternehmen zugewiesener Referenzcode für den Vorfall | Vom Finanzunternehmen vergebener eindeutiger Referenzcode zur eindeutigen Identifizierung des schwerwiegenden IKT-bezogenen Vorfalls. Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung der vom Dritt Dienstleister zugewiesene Referenzcode für den Vorfall. | Ja | Ja | Ja | Alphanumerisch |
| 2.2. Datum und Uhrzeit der Feststellung des IKT-bezogenen Vorfalls | Datum und Uhrzeit der Kenntnisnahme des IKT-bezogenen Vorfalls durch das Finanzunternehmen. Bei wiederholten Vorfällen das Datum und die Uhrzeit der Feststellung des letzten IKT-bezogenen Vorfalls. | Ja | Ja | Ja | ISO 8601 UTC-Format (JJJ-MM-TT hh:mm:ss) |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|---|--|--|---|--|
| 2.3. Datum und Uhrzeit der Einstufung des Vorfalls als schwerwiegend | Datum und Uhrzeit der Einstufung des IKT-bezogenen Vorfall als schwerwiegend gemäß den in der Delegierten Verordnung (EU) 2024/1772 festgelegten Einstufungskriterien. | Ja | Ja | Ja | ISO 8601 UTC-Format (JJJ-MM-TT hh:mm:ss) |
| 2.4. Beschreibung des IKT-bezogenen Vorfalls | <p>Beschreibung der relevantesten Aspekte des schwerwiegenden IKT-bezogenen Vorfalls.</p> <p>Finanzunternehmen geben einen allgemeinen Überblick über die folgenden Informationen, z. B. mögliche Ursachen, unmittelbare Auswirkungen, betroffene Systeme usw. Finanzunternehmen geben an, sofern bekannt oder nach vernünftigem Ermessen zu erwarten, ob sich der Vorfall auf Dritt Dienstleister oder andere Finanzunternehmen auswirkt, die Art des Dienstleisters oder Finanzunternehmens, ihren Namen, ihre jeweiligen Identifikationscodes und die Art des Identifikationscodes (z. B. LEI-Code oder EUID).</p> <p>In nachfolgenden Meldungen kann sich der Feldinhalt im Zeitverlauf ändern, um dem jeweils aktuellen Verständnis des IKT-bezogenen Vorfalls Rechnung zu tragen und andere relevante Informationen über den IKT-bezogenen Vorfall zu beschreiben, die nicht von den Datenfeldern erfasst werden, einschließlich der internen Bewertung der Schwere des IKT-bezogenen Vorfalls durch das Finanzunternehmen (z. B. sehr niedrig, niedrig, mittel, hoch, sehr hoch) und eines Hinweises auf Ebene und Name der höchsten Entscheidungsstrukturen, die an der Reaktion auf den IKT-bezogenen Vorfall beteiligt waren.</p> | | Ja | Ja | Alphanumerisch |
| 2.5. Einstufungskriterien, die die Meldung des Vorfalls ausgelöst haben | <p>Einstufungskriterien gemäß der Delegierten Verordnung (EU) 2024/1772, die dazu geführt haben, dass der IKT-bezogene Vorfall als schwerwiegender Vorfall eingestuft und gemeldet wurde.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung die Einstufungskriterien, die dazu geführt haben, dass der IKT-bezogene Vorfall für mindestens ein oder mehrere Finanzunternehmen als schwerwiegend eingestuft wurde.</p> | Ja | Ja | Ja | <p>Auswahl (Mehrfachauswahl):</p> <ul style="list-style-type: none"> — Betroffene Kunden, Gegenparteien im Finanzbereich und Transaktionen; — Reputations-schaden; — Dauer und Ausfallzeiten; — Geografische Ausbreitung; — Datenverluste; — Betroffene kritische Dienstleistun-gen; — Wirtschaftliche Auswirkungen |
| 2.6. Wesentlichkeits-schwellen für das Einstufungs-krite-rium „Geografische Ausbreitung“ | <p>EWR-Mitgliedstaaten, die von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind.</p> <p>Bei der Bewertung der Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls in anderen Mitgliedstaaten berücksichtigen Finanzunternehmen die Artikel 4 und 12 der Delegierten Verordnung (EU) 2024/1772.</p> | Ja, wenn der Schwellenwert für „Geografische Ausbreitung“ erreicht ist | Ja, wenn der Schwellenwert für „Geogra-fische Ausbrei-tung“ erreicht ist | Ja, wenn der Schwellen-wert für „Geografi sche Ausbrei-tung“ erreicht ist | Die Auswahl (Mehrfachauswahl) wird mithilfe von ISO 3166 ALPHA-2 der betroffenen Länder ausgefüllt |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-mel-dung | Verpflichtend für die Abschluss-mel-dung | Feldtyp |
|--|---|---|---|---|---|
| 2.7. Feststellung des schwerwiegenden IKT-bezogenen Vorfalls | Angaben dazu, wie der schwerwiegende IKT-bezogene Vorfall festgestellt wurde. | Ja | Ja | Ja | Auswahl: — IT-Sicherheit; — Personal; — Interne Revision; — Externe Prüfung; — Kunden; — Gegenparteien im Finanzbereich; — Dritt-dienst-leister; — Angreifer; — Überwachungssysteme; — Staatliches Strafverfol-gungsbehörde; — Sonstiges. Organ/Agentur/ |
| 2.8. Angaben dazu, ob der Vorfall bei einem Dritt-dienst-leister oder einem anderen Finanzunter-nehmen seinen Ursprung hat | Angaben dazu, ob der schwerwiegende IKT-bezogene Vorfall bei einem Dritt-dienst-leister oder einem anderen Finanzunternehmen seinen Ursprung hat. Finanzunternehmen geben an, ob der schwerwiegende IKT-bezogene Vorfall bei einem Dritt-dienst-leister oder einem anderen Finanzunternehmen (einschließlich Finanzunternehmen, die derselben Gruppe wie das meldende Unternehmen angehören) seinen Ursprung hat, und nennen den Namen, den Identifikationscode des Dritt-dienst-leisters oder des Finanzunternehmens und die Art des Identifikationscodes (z. B. LEI-Code oder EUID). | Ja, wenn der Vorfall seinen Ursprung bei einem Dritt-dienst-leister oder einem anderen Finanzunter-nehmen hat | Ja, wenn der Vorfall seinen Ursprung bei einem Dritt-dienst-leister oder einem anderen Finanzunter-nehmen hat | Ja, wenn der Vorfall seinen Ursprung bei einem Dritt-dienst-leister oder einem anderen Finanzunter-nehmen hat | Alphanumerisch |
| 2.9. Aktivierung des Plans zur Aufrechter-haltung des Geschäfts-betriebs, falls aktiviert | Angabe, ob die Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs des Finanzunternehmens formal aktiviert wurden. | Ja | Ja | Ja | Boolesch (Ja oder Nein) |
| 2.10. Sonstige zweckdienliche Angaben | Alle weiteren Informationen, die nicht in der Vorlage erfasst sind. Finanzunternehmen, die einen schwerwiegenden IKT-bezogenen Vorfall in nicht schwerwiegend zurückgestuft haben, beschreiben die Gründe, aus denen der IKT-bezogene Vorfall die Kriterien für die Einstufung als schwerwiegend nicht erfüllt und voraussichtlich nicht erfüllen wird. | Ja, wenn es andere Informationen gibt, die nicht in der Vorlage | Ja, wenn es andere Informationen gibt, die nicht in der Vorlage erfasst sind, oder | Ja, wenn es andere Informationen gibt, die nicht in der Vorlage | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|---|--|-----------------------------------|---|---|---|
| Inhalt der Zwischenmeldung | | | | | |
| 3.1. Von der zuständigen Behörde bereitgestellter Referenzcode für den Vorfall | Von der zuständigen Behörde zum Zeitpunkt des Eingangs der Erstmeldung zugewiesener eindeutiger Referenzcode zur eindeutigen Identifizierung des schwerwiegenden IKT-bezogenen Vorfalls. | Nein | Ja, falls zutreffend | Ja, falls zutreffend | Alphanumerisch |
| 3.2. Datum und Uhrzeit des Eintretens des Vorfalls | Datum und Uhrzeit des Eintretens des schwerwiegenden IKT-bezogenen Vorfalls, falls abweichend von dem Zeitpunkt, zu dem das Finanzunternehmen von dem schwerwiegenden IKT-bezogenen Vorfall Kenntnis erlangt hat. Bei wiederholten schwerwiegenden IKT-bezogenen Vorfällen Datum und Uhrzeit des Eintretens des letzten schwerwiegenden IKT-bezogenen Vorfalls. | Nein | Ja | Ja | ISO 8601 UTC-Format (JJJJ-MM-TT hh:mm:ss) |
| 3.3. Datum und Uhrzeit der Wiederherstellung der Dienste, Tätigkeiten oder Vorgänge | Angaben zu Datum und Uhrzeit der Wiederherstellung der von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Dienste, Tätigkeiten oder Vorgänge. | Nein | Ja, wenn Datenfeld 3.16 „Ausfall-zeiten“ ausgefüllt wurde | Ja, wenn Datenfeld 3.16 „Ausfall-zeiten“ ausgefüllt wurde | ISO 8601 UTC-Format (JJJJ-MM-TT hh:mm:ss) |
| 3.4. Anzahl der betroffenen Kunden | Anzahl der Kunden, die von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind und die Dienste des Finanzunternehmens in Anspruch nehmen. Bei der Ermittlung der Anzahl der betroffenen Kunden berücksichtigen Finanzunternehmen Artikel 1 Absatz 1 und Artikel 9 Absatz 1 Buchstabe b der Delegierten Verordnung (EU) 2024/1772. Ein Finanzunternehmen, das die tatsächliche Anzahl der betroffenen Kunden nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen. Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die Gesamtzahl der betroffenen Kunden in allen Finanzunternehmen. | Nein | Ja | Ja | Numerische ganze Zahl |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--|--|-----------------------------------|---------------------------------------|--|---|
| 3.5. Prozentsatz der betroffenen Kunden | <p>Prozentsatz der von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Kunden im Verhältnis zur Gesamtzahl der Kunden, die die betroffenen Dienste des Finanzunternehmens in Anspruch nehmen. Bei mehr als einer betroffenen Dienstleistung werden die Dienstleistungen aggregiert.</p> <p>Finanzunternehmen berücksichtigen bei der Ermittlung der Zahlen die Artikel 1 Absatz 1 und Artikel 9 Absatz 1 Buchstabe a der Delegierten Verordnung (EU) 2024/1772.</p> <p>Ein Finanzunternehmen, das den tatsächlichen Prozentsatz der betroffenen Kunden nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung teilt das Finanzunternehmen die Summe aller betroffenen Kunden durch die Gesamtzahl der Kunden aller betroffenen Finanzunternehmen.</p> | Nein | Ja | Ja | Wird als Prozentwert mitgeteilt — ein Wert mit bis zu fünf numerischen Zeichen, die bis zu einer Dezimalstelle umfassen, ausgedrückt als Prozentsatz (z. B. 2,4, nicht 2,4 %). Hat der Wert mehr als eine Stelle nach dem Dezimaltrennzeichen, wenden die meldenden Gegenparteien die kaufmännische Rundung an. |
| 3.6. Anzahl der betroffenen Gegenparteien im Finanzbereich | <p>Anzahl der Gegenparteien im Finanzbereich, die von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind und einen Vertrag mit dem Finanzunternehmen geschlossen haben.</p> <p>Bei der Ermittlung der Anzahl der betroffenen Gegenparteien im Finanzbereich berücksichtigen die Finanzunternehmen Artikel 1 Absatz 2 der Delegierten Verordnung (EU) 2024/1772. Ein Finanzunternehmen, das die tatsächliche Anzahl der betroffenen Gegenparteien im Finanzbereich nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung die Gesamtzahl der betroffenen Gegenparteien im Finanzbereich in allen Finanzunternehmen.</p> | Nein | Ja | Ja | Numerische ganze Zahl |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|---|-----------------------------------|--|--|---|
| 3.7. Prozentsatz der betroffenen Gegenparteien im Finanzbereich | <p>Prozentsatz der Gegenparteien im Finanzbereich, die von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind und einen Vertrag mit dem Finanzunternehmen geschlossen haben, im Verhältnis zur Gesamtzahl der Gegenparteien im Finanzbereich.</p> <p>Bei der Ermittlung des Prozentsatzes der betroffenen Gegenparteien im Finanzbereich berücksichtigen die Finanzunternehmen die Artikel 1 Absatz 1 und Artikel 9 Absatz 1 Buchstabe c der Delegierten Verordnung (EU) 2024/1772.</p> <p>Ein Finanzunternehmen, das den tatsächlichen Prozentsatz der betroffenen Gegenparteien im Finanzbereich nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung ist die Summe aller betroffenen Gegenparteien im Finanzbereich geteilt durch die Gesamtzahl der Gegenparteien im Finanzbereich aller betroffenen Finanzunternehmen anzugeben.</p> | Nein | Ja | Ja | Wird als Prozentwert mitgeteilt — ein Wert mit bis zu fünf numerischen Zeichen, die bis zu einer Dezimalstelle umfassen, ausgedrückt als Prozentsatz (z. B. 2,4, nicht 2,4 %). Hat der Wert mehr als eine Stelle nach dem Dezimaltrennzeichen, wenden die meldenden Gegenparteien die kaufmännische Rundung an. |
| 3.8. Auswirkungen auf einschlägige Kunden oder Gegenparteien im Finanzbereich | Festgestellte Auswirkungen auf relevante Kunden oder Gegenparteien im Finanzbereich gemäß Artikel 1 Absatz 3 und Artikel 9 Absatz 1 Buchstabe f der Delegierten Verordnung (EU) 2024/1772. | Nein | Ja, wenn der Schwellenwert für „Relevanz der Kunden und der Gegenparteien im Finanzbereich“ erreicht ist | Ja, wenn der Schwellenwert für „Relevanz der Kunden und der Gegenparteien im Finanzbereich“ erreicht ist | Boolesch (Ja oder Nein) |
| 3.9. Anzahl der betroffenen Transaktionen | <p>Anzahl der Transaktionen, die von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind.</p> <p>Bei der Bewertung der Auswirkungen auf Transaktionen berücksichtigen die Finanzunternehmen Artikel 1 Absatz 4 der Delegierten Verordnung (EU) 2024/1772; dies schließt alle betroffenen inländischen und grenzüberschreitenden Transaktionen ein, die einen Geldbetrag beinhalten, der mindestens teilweise mit einer in der Union ausgeführten Transaktion in Zusammenhang steht.</p> | Nein | Ja, wenn eine Transaktion von dem Vorfall betroffen war | Ja, wenn eine Transaktion von dem Vorfall betroffen war | Numerische ganze Zahl |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|---|-----------------------------------|---|---|---|
| | <p>Ein Finanzunternehmen, das die tatsächliche Anzahl der betroffenen Transaktionen nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung ist die Gesamtzahl der betroffenen Transaktionen in allen Finanzunternehmen anzugeben.</p> | | | | |
| 3.10. Prozentsatz der betroffenen Transaktionen | <p>Prozentsatz der betroffenen Transaktionen im Verhältnis zur durchschnittlichen Anzahl inländischer und grenzüberschreitender Transaktionen des Finanzunternehmens im Zusammenhang mit der betroffenen Dienstleistung.</p> <p>Finanzunternehmen berücksichtigen die Artikel 1 Absatz 4 und Artikel 9 Absatz 1 Buchstabe d der Delegierten Verordnung (EU) 2024/1772.</p> <p>Ein Finanzunternehmen, das den tatsächlichen Prozentsatz der betroffenen Transaktionen nicht bestimmen kann, verwendet Schätzungen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung teilt das Finanzunternehmen die Summe aller betroffenen Transaktionen durch die Gesamtzahl der Transaktionen aller betroffenen Finanzunternehmen.</p> | Nein | Ja, wenn eine Transaktion von dem Vorfall betroffen war | Ja, wenn eine Transaktion von dem Vorfall betroffen war | Wird als Prozentwert mitgeteilt — ein Wert mit bis zu fünf numerischen Zeichen, die bis zu einer Dezimalstelle umfassen, ausgedrückt als Prozentsatz (z. B. 2,4, nicht 2,4 %). Hat der Wert mehr als eine Stelle nach dem Dezimaltrennzeichen, wenden die meldenden Gegenparteien die kaufmännische Rundung an. |
| 3.11. Wert der betroffenen Transaktionen | <p>Der Gesamtwert der von dem schwerwiegenden IKT-bezogenen Vorfall betroffenen Transaktionen wird gemäß Artikel 1 Absatz 4 und Artikel 9 Absatz 1 Buchstabe e der Delegierten Verordnung (EU) 2024/1772 ermittelt.</p> <p>Ein Finanzunternehmen, das den tatsächlichen Wert der betroffenen Transaktionen nicht bestimmen kann, verwendet Schätzungen auf der Grundlage verfügbarer Daten aus vergleichbaren Referenzzeiträumen.</p> <p>Ein Finanzunternehmen hat den Geldbetrag als positiven Wert auszuweisen.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung der Gesamtwert der betroffenen Transaktionen in allen Finanzunternehmen.</p> | Nein | Ja, wenn Transaktionen von dem Vorfall betroffen waren | Ja, wenn eine Transaktion von dem Vorfall betroffen war | Monetär Finanzunternehmen weisen den Datenpunkt mit einer Mindestpräzision aus, die tausend Einheiten entspricht (z. B. 2,5, nicht 2 500 EUR). |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|--|-----------------------------------|---|---|--|
| 3.12. Angaben dazu, ob es sich um tatsächliche Zahlen oder Schätzungen handelt oder ob es keine Auswirkungen gegeben hat | Angaben dazu, ob es sich bei den in den Datenfeldern 3.4 bis 3.11 ausgewiesenen Werten um tatsächliche Werte oder Schätzungen handelt oder ob es keine Auswirkungen gegeben hat. | Nein | Ja | Ja | <p>Auswahl (Mehrfachauswahl):</p> <ul style="list-style-type: none"> — Tatsächliche Zahlen zu den betroffenen Kunden; — tatsächliche Zahlen zu den betroffenen Gegenparteien im Finanzbereich; — tatsächliche Zahlen zu den betroffenen Transaktionen; — Schätzungen zu den betroffenen Kunden; — Schätzungen zu den betroffenen Gegenparteien im Finanzbereich; — Schätzungen zu den betroffenen Transaktionen; — keine Auswirkungen auf Kunden; — keine Auswirkungen auf Gegenparteien im Finanzbereich; — keine Auswirkungen auf Transaktionen. |
| 3.13. Reputations-schaden | <p>Angaben zum Reputationsschaden infolge des schwerwiegenden IKT-bezogenen Vorfalls im Sinne der Artikel 2 und 10 der Delegierten Verordnung (EU) 2024/1772.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die Kategorien von Reputationsschaden, die auf mindestens ein Finanzunternehmen zutreffen.</p> | Nein | Ja, wenn das Kriterium „Reputati-ons-schaden“ erfüllt ist | Ja, wenn das Kriterium „Reputati-ons-schaden“ erfüllt ist | <p>Auswahl (Mehrfachauswahl):</p> <ul style="list-style-type: none"> — Über den schwerwie-genden IKT-bezogenen Vorfall wurde in den Medien berichtet; — der schwerwie-gende IKT-bezogene Vorfall hat zu wiederholten Beschwerden verschiedener Kunden oder Gegenparteien im Finanzbereich über kunden-orientierte Dienstleistun-gen oder kritische Geschäfts-beziehungen geführt; — das Finanzunter-nehmen wird aufgrund des schwerwie-genden IKT-bezogenen Vorfalls nicht oder wahrscheinlich nicht in der Lage sein, regulatorische Anforderungen zu erfüllen; — das Finanzunter-nehmen wird infolge des schwerwiegenden IKT-bezogenen Vorfalls Kunden oder Gegenparteien im Finanzbereich verlieren oder wahrscheinlich verlieren, was wesentliche Auswirkungen auf seine Geschäfts-tätigkeit haben wird. |
| 3.14. Kontextbezo-gene Angaben zum Reputations-schaden | Angaben dazu, wie der schwerwiegende IKT-bezogene Vorfall die Reputation des Finanzunternehmens beeinträchtigt hat oder beeinträchtigen könnte, einschließlich Verstößen gegen Rechtsvorschriften, nicht erfüllter regulatorischer Anforderungen, Anzahl der Kundenbeschwerden usw. | Nein | Ja, wenn das Kriterium „Reputati-ons-schaden“ erfüllt ist | Ja, wenn das Kriterium „Reputati-ons-schaden“ erfüllt ist | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--------------------------|---|-----------------------------------|---------------------------------------|--|----------|
| | <p>Die kontextbezogenen Angaben umfassen die Art der Medien (z. B. traditionelle und digitale Medien, Blogs, Streaming-Plattformen) und die Medienberichterstattung, einschließlich der Reichweite der Medien (lokal, national, international). Die Medienberichterstattung bezieht sich in diesem Zusammenhang nicht auf vereinzelte negative Kommentare von Followern oder Nutzern sozialer Netzwerke.</p> <p>Das Finanzunternehmen gibt auch an, ob die Medienberichterstattung erhebliche Risiken für seine Kunden im Zusammenhang mit dem schwerwiegenden IKT-bezogenen Vorfall aufgezeigt hat, einschließlich des Risikos der Insolvenz des Finanzunternehmens oder des Risikos, Mittel zu verlieren.</p> <p>Die Finanzunternehmen geben auch an, ob sie den Medien Informationen zur Verfügung gestellt haben, die dazu dienten, die Öffentlichkeit zuverlässig über den schwerwiegenden IKT-bezogenen Vorfall und seine Folgen zu informieren.</p> <p>Die Finanzunternehmen können auch angeben, ob in den Medien im Zusammenhang mit dem IKT-bezogenen Vorfall Falschinformationen verbreitet wurden, worunter auch solche fallen, die sich auf vorsätzlich vom Angreifer verbreitete Falschinformationen stützen, oder die mutwillige Veränderung der Website des Finanzunternehmens betreffen oder zum Ausdruck bringen.</p> | | | | |
| 3.15. Dauer des Vorfalls | <p>Finanzunternehmen bestimmen die Dauer des schwerwiegenden IKT-bezogenen Vorfalls vom Zeitpunkt des Eintretens des schwerwiegenden IKT-bezogenen Vorfalls bis zu dem Zeitpunkt, zu dem der Vorfall behoben wurde.</p> <p>Finanzunternehmen, die nicht in der Lage sind, den Zeitpunkt zu bestimmen, zu dem der schwerwiegende IKT-bezogene Vorfall eingetreten ist, bestimmen die Dauer des schwerwiegenden IKT-bezogenen Vorfalls ab dem Zeitpunkt, zu dem das Finanzunternehmen den Vorfall festgestellt hat, bis zu dem Zeitpunkt, zu dem das Finanzunternehmen den Vorfall in Netzwerk- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet hat, je nachdem, welcher Zeitpunkt zuerst eintritt. Finanzunternehmen, die den Zeitpunkt der Behebung des schwerwiegenden IKT-bezogenen Vorfalls noch nicht kennen, verwenden Schätzungen. Der Wert ist in Tagen, Stunden und Minuten anzugeben.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung bestimmen Finanzunternehmen bei Unterschieden zwischen den Finanzunternehmen die längste Dauer des schwerwiegenden IKT-bezogenen Vorfalls.</p> | Nein | Ja | Ja | TT:HH:MM |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-mel-dung | Verpflichtend für die Abschluss-mel-dung | Feldtyp |
|--|--|-----------------------------------|--|---|--|
| 3.16. Ausfallzeiten | <p>Ausfallzeiten, gemessen ab dem Zeitpunkt, zu dem der Dienst für Kunden, Gegenparteien im Finanzbereich oder andere interne oder externe Nutzer vollständig oder teilweise nicht mehr verfügbar ist, bis zu dem Zeitpunkt, zu dem die regulären Tätigkeiten oder Vorgänge in dem vor dem schwerwiegenden IKT-bezogenen Vorfall herrschenden Umfang wiederhergestellt sind.</p> <p>Führen die Ausfallzeiten nach der Wiederherstellung der regulären Tätigkeiten oder Vorgänge zu einer Verzögerung bei der Bereitstellung von Dienstleistungen, so messen die Finanzunternehmen die Ausfallzeiten vom Beginn des schwerwiegenden IKT-bezogenen Vorfalls bis zu dem Zeitpunkt, zu dem die verzögerte Dienstleistung erbracht ist. Finanzunternehmen, die den Beginn der Ausfallzeiten nicht bestimmen können, messen die Dauer der Ausfallzeiten ab dem Zeitpunkt der Feststellung des Vorfalls bis zu dem Zeitpunkt, zu dem sie aufgezeichnet wurde, je nachdem, welcher Zeitpunkt zuerst eintritt.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung bestimmen Finanzunternehmen bei Unterschieden zwischen den Finanzunternehmen <u>die längste Dauer der Ausfallzeiten</u>.</p> | Nein | Ja, wenn der Vorfall zu Ausfall-zeiten geführt hat | Ja, wenn der Vorfall zu Ausfall-zeiten geführt hat | TT:HH:MM |
| 3.17. Angaben dazu, ob es sich bei der Dauer und den Ausfallzeiten um tatsächliche Zahlen oder Schätzungen handelt | Angaben dazu, ob es sich bei den in den Datenfeldern 3.15 und 3.16 ausgewiesenen Werten um tatsächliche Werte oder Schätzungen handelt. | Nein | Ja, wenn das Kriterium „Dauer und Ausfall-zeiten“ erfüllt ist | Ja, wenn das Kriterium „Dauer und Ausfall-zeiten“ erfüllt ist | Auswahl: — Tatsächliche Zahlen; — Schätzungen; — tatsächliche Zahlen und Schätzungen; — keine Informationen verfügbar. |
| 3.18. Arten von Auswirkungen in den Mitgliedstaaten | <p>Art der Auswirkung in den jeweiligen EWR-Mitgliedstaaten.</p> <p>Angabe, ob der schwerwiegende IKT-bezogene Vorfall Auswirkungen in anderen EWR-Mitgliedstaaten (ausgenommen der Mitgliedstaat der zuständigen Behörde, der der Vorfall direkt gemeldet wird) gemäß Artikel 4 der Delegierten Verordnung (EU) 2024/1772 hat und insbesondere im Hinblick auf die Bedeutung der Auswirkungen in Bezug auf:</p> <p>a) betroffene Kunden und Gegenparteien im Finanzbereich in anderen Mitgliedstaaten oder</p> | Nein | Ja, wenn der Schwellenwert für „Geogra-fische Ausbrei-tung“ erreicht ist | Ja, wenn der Schwellenwert für „Geogra-fische Ausbreitung“ erreicht ist | Auswahl (Mehrfachauswahl): — Kunden; — Gegenparteien im Finanzbereich; — Zweigniederlassung des Finanzunternehmens; — Finanzunternehmen innerhalb der Gruppe, die in dem betreffenden Mitgliedstaat tätig sind; — Finanzmarktinfra-struktur; — Dritt Dienstleister, die möglicherweise auch von anderen Finanzunternehmen in Anspruch genommen werden. |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--|--|-----------------------------------|--|--|---|
| | b) Zweigniederlassungen oder andere Finanzunternehmen innerhalb der Gruppe, die in anderen Mitgliedstaaten tätig sind, oder Finanzmarktinfrastrukturen oder Drittienstleister mit möglichen Auswirkungen auf Finanzunternehmen in anderen Mitgliedstaaten, für die sie Dienstleistungen erbringen, soweit diese Informationen verfügbar sind. c) | | | | |
| 3.19. Beschreibung der Auswirkungen des Vorfalls in anderen Mitgliedstaaten | Beschreibung der Auswirkungen und Schwere des schwerwiegenden IKT-bezogenen Vorfalls in jedem betroffenen Mitgliedstaat, einschließlich einer Bewertung der Auswirkungen und Schwere in Bezug auf: a) Kunden; b) Gegenparteien im Finanzbereich; c) Zweigniederlassungen des Finanzunternehmens; d) Andere Finanzunternehmen innerhalb der Gruppe, die in anderen Mitgliedstaaten tätig sind; e) Finanzmarktinfrastrukturen; f) Drittienstleister, die möglicherweise auch von anderen Finanzunternehmen in anderen Mitgliedstaaten in Anspruch genommen werden. | Nein | Ja, wenn der Schwellenwert für „Geografische Ausbreitung“ erreicht ist | Ja, wenn der Schwellenwert für „Geografische Ausbreitung“ erreicht ist | Alphanumerisch |
| 3.20. Wesentlichkeitsschwellen für das Einstufungs-kriterium „Datenverluste“ | Art der mit dem schwerwiegenden IKT-bezogenen Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- und Vertraulichkeitsverluste von Daten. Finanzunternehmen berücksichtigen bei ihrer Bewertung die Artikel 5 und 13 der Delegierten Verordnung (EU) 2024/1772. Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die Datenverluste, die mindestens ein Finanzunternehmen betreffen. | Nein | Ja, wenn das Kriterium „Daten-verluste“ erfüllt ist | Ja, wenn das Kriterium „Daten-verluste“ erfüllt ist | Auswahl (Mehrfachauswahl): — Verfügbarkeit; — Authentizität; — Integrität; — Vertraulichkeit. |
| 3.21. Beschreibung der Datenverluste | Beschreibung der Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit kritischer Daten gemäß den Artikeln 5 und 13 der Delegierten Verordnung (EU) 2024/1772. Angaben zu den Auswirkungen auf die Umsetzung der Geschäftsziele des Finanzunternehmens oder auf die Erfüllung regulatorischer Anforderungen. Als Teil der bereitgestellten Informationen geben Finanzunternehmen an, ob es sich bei den betroffenen Daten um Kundendaten, Daten anderer Unternehmen (z. B. Gegenparteien im Finanzbereich) oder um Daten des Finanzunternehmens selbst handelt. | Nein | Ja, wenn das Kriterium „Daten-verluste“ erfüllt ist | Ja, wenn das Kriterium „Daten-verluste“ erfüllt ist | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--|--|-----------------------------------|---------------------------------------|--|----------------|
| | <p>Das Finanzunternehmen kann auch die Art der von dem Vorfall betroffenen Daten angeben, insbesondere, ob die Daten vertraulich sind und um welche Art von Vertraulichkeit es sich handelt (z. B. Geschäftsgeheimnisse, personenbezogene Daten, Berufsgeheimnis wie etwa Bankgeheimnis, Versicherungsgeheimnis, Zahlungsdienstegeheimnis usw.).</p> <p>Die Informationen können auch mögliche Risiken im Zusammenhang mit den Datenverlusten umfassen, z. B. ob die von dem Vorfall betroffenen Daten zur Identifizierung einzelner Personen verwendet werden können und von dem Angreifer genutzt werden könnten, um Kredite oder Darlehen ohne die Zustimmung dieser Personen zu erhalten, Spear-Phishing-Angriffe durchzuführen oder Informationen öffentlich preiszugeben.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung eine allgemeine Beschreibung der Auswirkungen des Vorfalls auf die betroffenen Finanzunternehmen. Gibt es Unterschiede bei den Auswirkungen, so sind in der Beschreibung der Auswirkungen die spezifischen Auswirkungen auf die verschiedenen Finanzunternehmen eindeutig anzugeben.</p> | | | | |
| 3.22. Einstufungskriterium „Betroffene kritische Dienstleistungen“ | <p>Angaben beim Kriterium „Betroffene kritische Dienstleistungen“.</p> <p>Finanzunternehmen berücksichtigen bei ihrer Bewertung Artikel 6 der Delegierten Verordnung (EU) 2024/1772, einschließlich Informationen über</p> <ul style="list-style-type: none"> — die betroffenen Dienstleistungen oder Tätigkeiten, die einer Zulassung oder Registrierung bedürfen oder von den zuständigen Behörden beaufsichtigt werden, oder — die IKT-Dienste oder Netzwerk- und Informationssysteme, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen, und — die Art des böswilligen und unbefugten Zugriffs auf die Netzwerk- und Informationssysteme des Finanzunternehmens. <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung die Auswirkungen auf kritische Dienstleistungen, die auf mindestens ein Finanzunternehmen zutreffen.</p> | Nein | Ja | Ja | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-mel-dung | Verpflichtend für die Abschluss-mel-dung | Feldtyp |
|--|---|-----------------------------------|---|--|---|
| 3.23. Art des Vorfalls | Einstufung der Vorfälle nach Art. | Nein | Ja | Ja | Auswahl (Mehrfachauswahl): <ul style="list-style-type: none"> — Cybersicherheits-bezogen; — Prozessversagen; — Systemversagen; — Externes Ereignis; — Zahlungsbezogen; — Sonstiges (bitte angeben). |
| 3.24. Andere Arten von Vorfällen | Andere Arten von IKT-bezogenen Vorfällen: Finanzunternehmen, die im Datenfeld 3.23 „Sonstiges“ als Art des Vorfalls ausgewählt haben, geben die Art des IKT-bezogenen Vorfalls an. | Nein | Ja, wenn in Datenfeld 3.23 „Sonsti-ges“ als Art des Vorfalls ausge-wählt wurde | Ja, wenn in Datenfeld 3.23 „Sonstiges“ als Art des Vorfalls ausgewählt wurde | Alphanumerisch |
| 3.25. Bedrohungen und Techniken des Angreifers | Geben Sie die Bedrohungen und Techniken an, die der Angreifer einsetzt, wie zum Beispiel: <ul style="list-style-type: none"> a) Social Engineering, einschließlich Phishing; b) (D)DoS; c) Identitätsdiebstahl; d) Datenverschlüsselung mit weitergehenden Folgen, einschließlich Ransomware; e) Kaperung von Ressourcen; f) Datenexfiltration und -manipulation, ausgenommen Identitätsdiebstahl; g) Datenvernichtung; h) mutwillige Veränderung (Defacement); i) Lieferkettenangriff; j) Sonstiges (bitte angeben). | Nein | Ja, wenn als Art des IKT-bezogenen Vorfalls in Feld 3.23 „Cyber-si-cher-heitsbe-zo-gen“ ausge-wählt wurde | Ja, wenn als Art des IKT-bezogenen Vorfalls in Feld 3.23 „Cyber-sicher-heits-bezo-gen“ ausge-wählt wurde | Auswahl (Mehrfachauswahl): <ul style="list-style-type: none"> — Social Engineering (einschließlich Phishing); — (D)DoS; — Identitätsdiebstahl; — Datenverschlüsse-lung mit weitergehenden Folgen, einschließlich Ransomware; — Kaperung von Ressourcen; — Datenexfiltration und -manipulation, einschließlich Identitätsdiebstahl; — Datenvernichtung; — mutwillige Veränderung (Defacement); — Lieferkettenangriff; — Sonstiges (bitte angeben). |
| 3.26. Andere Arten von Techniken | Andere Arten von Techniken Finanzunternehmen, die im Datenfeld 3.25 „Sonstiges“ als Art der Technik ausgewählt haben, geben die Art der Technik an. | Nein | Ja, wenn in Datenfeld 3.25 „Sonstiges“ als Art der Technik ausge-wählt wurde | Ja, wenn in Datenfeld 3.25 „Sonstiges“ als Art der Technik ausge-wählt wurde | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|--|---|-----------------------------------|---------------------------------------|--|----------------|
| 3.27. Angaben zu betroffenen Funktionsbereichen und Geschäftsprozessen | <p>Angabe der Funktionsbereiche und Geschäftsprozesse, die von dem Vorfall betroffen sind, einschließlich Produkten und Dienstleistungen.</p> <p>Die Funktionsbereiche umfassen unter anderem:</p> <ul style="list-style-type: none"> a) Marketing und Geschäftsentwicklung; b) Kundenservice; c) Produktmanagement; d) Rechtskonformität; e) Risikomanagement; f) Finanz- und Rechnungswesen; g) Personal und allgemeine Dienstleistungen; h) Informationstechnologie. <p>Die Geschäftsprozesse umfassen unter anderem:</p> <ul style="list-style-type: none"> — Kontoinformationen; — Dienstleistungen im Bereich Versicherungsmathematik; — Annahme und Abrechnung („Acquiring“) von Zahlungsvorgängen; — Authentifizierung/Autorisierung; — Verfasser; — Kunden-Onboarding; — Benefit-Management; — Management von Benefit-Zahlungen; — Kauf und Verkauf von Pauschalversicherungen zwischen Versicherungen; — Kartenzahlungen; — Liquiditätsmanagement; — Platzierung oder Entnahme von Bargeld; — Management von Versicherungsansprüchen; — Schadenregulierung; — Clearing; — Unternehmenskreditkonglomerate; — Kollektivversicherungen; — Überweisungen; — Verwahrung von Vermögenswerten; — Kunden-Onboarding; — Datenaufnahme; — Datenverarbeitung; — Lastschriften; — Ausfuhrversicherungen; — Finalisierung von Geschäften/Abschlüssen; — Platzierung von Finanzinstrumenten; — Fondsbuchhaltung; | Nein | Ja | Ja | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|--|-----------------------------------|--|---|---|
| | <ul style="list-style-type: none"> — Devisen; — Anlageberatung; — Anlageverwaltung; — Emission von Zahlungsinstrumenten; — Kreditmanagement; — Zahlungsverfahren für Lebensversicherungen; — Finanztransfer; — Berechnung des Nettovermögens; — Order; — Zahlungsauslösung; — Abschluss von Versicherungen; — Portfolioverwaltung; — Prämieneinzug; — Empfang/Übermittlung/Ausführung; — Rückversicherung; — Abwicklung; — Transaktionsüberwachung. <p>Bei einer aggregierten Meldung gemäß Artikel 7 der vorliegenden Verordnung die betroffenen Funktionsbereiche und Geschäftsprozesse bei mindestens einem Finanzunternehmen.</p> | | | | |
| 3.28. Betroffene Infrastruktur-komponenten, die Geschäftspro-zesse unterstützen | Angaben dazu, ob Infrastrukturkomponenten (Server, Betriebssysteme, Software, Anwendungsserver, Middleware, Netzwerkkomponenten usw.), die Geschäftsprozesse unterstützen, von dem schwerwiegenden IKT-bezogenen Vorfall betroffen sind. | Nein | Ja | Ja | Auswahl: <ul style="list-style-type: none"> — Ja; — Nein; — keine Informationen verfügbar. |
| 3.29. Angaben zu betroffenen Infrastruktur-komponenten, die Geschäfts-prozesse unterstützen | <p>Beschreibung der Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls auf Infrastrukturkomponenten, die Geschäftsprozesse unterstützen, einschließlich Hardware und Software.</p> <p>Hardware umfasst Server, Computer, Rechenzentren, Switches, Router und Hubs. Software umfasst Betriebssysteme, Anwendungen, Datenbanken, Sicherheitstools und Netzwerkkomponenten. Bei „Sonstiges“ bitte Angaben machen. In den Beschreibungen sind die betroffenen Infrastrukturkomponenten oder -systeme zu beschreiben oder zu benennen und, soweit verfügbar, folgende Angaben zu machen:</p> <ol style="list-style-type: none"> Versionsinformationen; Interne Infrastruktur/Teilweise ausgelagert/Vollständig ausgelagert — Name des Dritt-dienstleisters; | Nein | Ja, wenn der Vorfall Infra-struk-tur-komponen-ten beein-trächtigt hat, die Geschäfts-pro-zesse unter-stützen | Ja, wenn der Vorfall Infra-struk-tur-kompo-nen-ten beeinträchtigt hat, die Geschäfts-pro-zesse unterstützen | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|---|---|-----------------------------------|---|---|---|
| | c) Ob die Infrastruktur von mehreren Geschäftsfunktionen separat/ gemeinsam genutzt wird; d) Ob einschlägige Regelungen zur Resilienz/Kontinuität/ Wiederherstellung/Substituierbarkeit getroffen wurden. | | | | |
| 3.30. Auswirkungen auf die finanziellen Interessen von Kunden | Angaben dazu, ob sich der schwerwiegende IKT-bezogene Vorfall auf die finanziellen Interessen der Kunden ausgewirkt hat. | Nein | Ja | Ja | Auswahl: — Ja; — Nein; — keine Informationen verfügbar. |
| 3.31. Meldung an andere Behörden | Angabe, welche Behörden über den schwerwiegenden IKT-bezogenen Vorfall informiert wurden. Unter Berücksichtigung der Unterschiede, die sich aus den nationalen Rechtsvorschriften der Mitgliedstaaten ergeben, ist der Begriff der Strafverfolgungsbehörde von den Finanzunternehmen im weitesten Sinne so zu verstehen, dass er Behörden umfasst, die zur Verfolgung von Cyberkriminalität befugt sind, einschließlich Polizei, Organe zur Aufrechterhaltung der öffentlichen Ordnung und Staatsanwaltschaften. | Nein | Ja | Ja | Auswahl (Mehrfachauswahl): — Polizei/Straf-verfolgung; — CSIRT; — Datenschutz-behörde; — nationale Agentur für Cyber-sicherheit; — keine; — andere (bitte angeben). |
| 3.32. Angabe der „anderen“ Behörden | Angabe, welche „anderen“ Behörden über den schwerwiegenden IKT-bezogenen Vorfall informiert wurden. Falls in Datenfeld 3.31 „Andere“ ausgewählt wurde: In die Beschreibung sind nähere Informationen über die Behörde, der das Finanzunternehmen Informationen über den schwerwiegenden IKT-bezogenen Vorfall übermittelt hat, aufzunehmen. | Nein | Ja, wenn das Finanz-unter-neh-men „andere“ Behörden über den schwer-wiegen-den IKT-bezogenen Vorfall informiert hat | Ja, wenn das Finanzun-ter-nnehmen „andere“ Behörden über den schwer-wiegen-den IKT-bezogenen Vorfall informiert hat | Alphanumerisch |
| 3.33. Ergriffene oder geplante befristete Maßnahmen zur Wiederher-stellung nach dem Vorfall | Angabe, ob das Finanzunternehmen befristete Maßnahmen umgesetzt hat (oder dies plant), die ergriffen wurden (oder geplant sind), um den normalen Geschäftsbetrieb nach dem schwerwiegenden IKT-bezogenen Vorfall wiederherzustellen. | Nein | Ja | Ja | Boolesch (Ja oder Nein) |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|---|---|-----------------------------------|--|--|----------------|
| 3.34. Beschreibung etwaiger ergriffener oder geplanter befristeter Maßnahmen zur Wiederherstellung nach dem Vorfall | <p>Es ist zu beschreiben, welche Sofortmaßnahmen ergriffen wurden, einschließlich der Isolierung des Vorfalls auf Netzwerkebene, der Aktivierung von Workaround-Verfahren, der Sperrung von USB-Ports, der Aktivierung der Site für die Wiederherstellung im Notfall und anderer vorübergehend eingerichteter zusätzlicher Sicherheitsmechanismen.</p> <p>Finanzunternehmen geben das Datum und die Uhrzeit der Umsetzung der befristeten Maßnahmen sowie den voraussichtlichen Zeitpunkt der Rückkehr zur primären Site an. Bei befristeten Maßnahmen, die nicht umgesetzt wurden, aber noch geplant sind, ist das Datum anzugeben, bis zu dem sie voraussichtlich umgesetzt werden.</p> <p>Falls keine befristeten Maßnahmen ergriffen wurden, bitte den Grund angeben.</p> | Nein | Ja, wenn befristete Maßnahmen ergriffen wurden oder geplant sind (Daten-feld 3.33) | Ja, wenn befristete Maßnahmen ergriffen wurden oder geplant sind (Daten-feld 3.33) | Alphanumerisch |
| 3.35. Kompromittierungsindikatoren | <p>Gegebenenfalls Informationen im Zusammenhang mit dem schwerwiegenden IKT-bezogenen Vorfall, die dazu beitragen können, böswillige Aktivitäten innerhalb eines Netzwerks oder Informationssystems zu erkennen (Kompromittierungsindikatoren).</p> <p>Das Feld betrifft nur Finanzunternehmen, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates (!) fallen, und Finanzunternehmen, die gegebenenfalls gemäß den nationalen Vorschriften zur Umsetzung des Artikels 3 der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Unternehmen ermittelt wurden.</p> <p>Die von dem Finanzunternehmen bereitgestellten Kompromittierungsindikatoren enthalten die folgenden Datenkategorien:</p> <ul style="list-style-type: none"> a) IP-Adressen; b) URL-Adressen; c) Domains; d) Datei-Hashes; e) Daten zu Schadsoftware (Name der Schadsoftware, Dateinamen und ihre Speicherorte, spezifische Registrierungsschlüssel im Zusammenhang mit Schadsoftware-Aktivitäten); f) Daten zu Netzaktivitäten (Ports, Protokolle, Adressen, Referrer, User Agents, Header, spezifische Protokolle oder auffällige Muster im Netzwerkverkehr); g) Daten zu E-Mail-Nachrichten (Absender, Empfänger, Betreff, Header, Inhalt); | Nein | Ja, wenn „Cyber-sicher-heitsbe-zogen“ als Art des Vorfalls in Datenfeld 3.23 ausge-wählt wurde | Ja, wenn „Cyber-sicher-heits-bezogen“ als Art des Vorfalls in Daten-feld 3.23 ausgewählt wurde | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|--|-----------------------------------|---------------------------------------|--|---|
| | <p>h) DNS-Anfragen und Registrierungskonfigurationen;</p> <p>i) Nutzerkontoaktivitäten (Anmeldungen, Kontoaktivitäten privilegierter Nutzer, Rechteausweitung);</p> <p>j) Datenbankverkehr (Lesen/Schreiben), Anfragen für dieselbe Datei.</p> <p>Diese Art von Informationen kann in der Praxis Daten umfassen, die sich unter anderem auf Indikatoren, die Muster im Netzwerkverkehr im Zusammenhang mit bekannten Angriffen/Botnetkommunikation beschreiben, IP-Adressen von mit Schadsoftware infizierten Rechnern (Bots), Daten über von Schadsoftware genutzte „Command and Control“-Server (in der Regel Domains oder IP-Adressen) und URLs in Bezug auf Phishing-Websites oder Websites, bei denen beobachtet wurde, dass sie für das Hosting von Schadsoftware oder Exploit Kits genutzt werden, beziehen.</p> | | | | |
| Inhalt der Abschlussmeldung | | | | | |
| 4.1. Übergeordnete Einstufung der Ursachen des Vorfalls | <p>Übergeordnete Einstufung der Ursache des schwerwiegenden IKT-bezogenen Vorfalls bei den Arten von Vorfällen, einschließlich der folgenden übergeordneten Kategorien:</p> <ul style="list-style-type: none"> a) Böswillige Handlungen; b) Prozessversagen; c) Systemversagen/-störung; d) menschliches Versagen; e) externes Ereignis. | Nein | Nein | Ja | <p>Auswahl (Mehrfachauswahl):</p> <ul style="list-style-type: none"> — Böswillige Handlungen; — Prozess-versagen; — System-versagen/-störung; — menschliches Versagen; — externes Ereignis. |
| 4.2. Detaillierte Einstufung der Ursachen des Vorfalls | <p>Detaillierte Einstufung der Ursachen des schwerwiegenden IKT-bezogenen Vorfalls bei den Arten von Vorfällen, einschließlich der folgenden detaillierten Kategorien im Zusammenhang mit den in Datenfeld 4.1 ausgewiesenen übergeordneten Kategorien:</p> <ol style="list-style-type: none"> 1. Böswillige Handlungen (falls ausgewählt, eine oder mehrere der folgenden Optionen wählen): <ul style="list-style-type: none"> a) Vorsätzliche interne Handlungen; b) vorsätzliche physische Schäden/Manipulation/Diebstahl; c) betrügerische Handlungen. 2. Prozessversagen (falls ausgewählt, eine oder mehrere der folgenden Optionen wählen): <ul style="list-style-type: none"> a) Unzureichende Überwachung oder mangelhafte Überwachung und Kontrolle; | Nein | Nein | Ja | <p>Auswahl (Mehrfachauswahl):</p> <ul style="list-style-type: none"> — Böswillige Handlungen: Vorsätzliche interne Handlungen; — böswillige Handlungen: Vorsätzliche physische Schäden/Manipulation/Diebstahl; — böswillige Handlungen: Betrügerische Handlungen; — Prozess-versagen: Unzureichende Überwachung oder mangelhafte Überwachung und Kontrolle; — Prozess-versagen: Unzureichende/unklare Rollen und Zuständigkeiten; — Prozess-versagen: Versagen des IKT-Risiko-management-prozesses; — Prozess-versagen: Unzureichende oder nicht funktionie-rende IKT-Abläufe und IKT-Sicherheits-abläufe; |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|-----------|---|-----------------------------------|--|---|--|
| | <p>b) unzureichende/unklare Rollen und Zuständigkeiten;</p> <p>c) Versagen des IKT-Risikomanagementprozesses;</p> <p>d) unzureichende oder nicht funktionierende IKT-Abläufe und IKT-Sicherheitsabläufe;</p> <p>e) unzureichendes oder nicht funktionierendes IKT-Projektmanagement;</p> <p>f) unzureichende interne Richtlinien, Verfahren und Dokumentation;</p> <p>g) unzureichende Beschaffung, Entwicklung und Wartung von IKT-Systemen;</p> <p>h) Sonstiges (bitte angeben).</p> <p>3. Systemversagen/-störung (falls ausgewählt, eine oder mehrere der folgenden Optionen wählen):</p> <p>a) Hardwarekapazität und -leistung: schwerwiegende IKT-bezogene Vorfälle, die durch Hardwareressourcen verursacht werden, die sich in Bezug auf Kapazität oder Leistung als unzureichend erweisen, um die geltenden rechtlichen Anforderungen zu erfüllen;</p> <p>b) Wartung der Hardware: schwerwiegende IKT-bezogene Vorfälle infolge unangemessener oder unzureichender Wartung von Hardwarekomponenten (ausgenommen „Veralterung/Alterung der Hardware“);</p> <p>c) Veralterung/Alterung der Hardware: Diese Ursache betrifft schwerwiegende IKT-bezogene Vorfälle aufgrund veralteter oder alternder Hardwarekomponenten;</p> <p>d) Softwarekompatibilität/-konfiguration: schwerwiegende IKT-bezogene Vorfälle, die durch Softwarekomponenten verursacht werden, die mit anderen Software- oder Systemkonfigurationen nicht kompatibel sind, einschließlich schwerwiegender IKT-bezogener Vorfälle aufgrund von Softwarekonflikten, fehlerhaften Einstellungen oder falsch konfigurierten Parametern, die sich auf die Gesamtfunktionalität des Systems auswirken;</p> <p>e) Softwareleistung: schwerwiegende IKT-bezogene Vorfälle infolge von Softwarekomponenten, die aus anderen als den unter „Softwarekompatibilität/-konfiguration“ genannten Gründen eine schlechte Leistung oder Ineffizienz aufweisen, einschließlich schwerwiegender IKT-bezogener Vorfälle, die durch langsame Reaktionszeiten, übermäßigen Ressourcenverbrauch oder ineffiziente Abfragen, die sich auf die Leistung der Software oder des Systems auswirken, verursacht werden;</p> | | | | <ul style="list-style-type: none"> — Prozess-versagen: Unzureichen-des oder nicht funktionie-rendes IKT-Projekt-management; — Prozess-versagen: Unzureichende interne Richtlinien, Verfahren und Dokumentation; — Prozess-versagen: Unzureichende Beschaffung, Entwicklung und Wartung von IKT-Systemen; — Prozess-versagen: Sonstiges (bitte angeben); — System-versagen: Hardware-kapazität und -leistung; — System-versagen: Wartung der Hardware; — System-versagen: Veralterung/ Alterung der Hardware; — System-versagen: — Software-kompatibilität/-konfiguration; — System-versagen: Software-leistung; — System-versagen: Netzwerk-konfiguration; — System-versagen: Physische Schäden; — System-versagen: Sonstiges (bitte angeben); — menschliches Versagen: Unterlassung; — menschliches Versagen: Irrtum; — menschliches Versagen: Fähigkeiten und Kenntnisse; — menschliches Versagen: Unzureichende personelle Ausstattung; — menschliches Versagen: Fehlkommu-nikation; — menschliches Versagen: Sonstiges (bitte angeben); — externes Ereignis: Naturkatastro-phen/ höhere Gewalt; — externes Ereignis: Ausfälle bei Dritten; — externes Ereignis: Sonstiges (bitte angeben). |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|-----------|---|-----------------------------------|---------------------------------------|--|---------|
| | <p>f) Netzwerkkonfiguration: schwerwiegende IKT-bezogene Vorfälle, die auf fehlerhafte oder falsch konfigurierte Netzwerkeinstellungen oder -infrastruktur zurückzuführen sind, einschließlich schwerwiegender IKT-bezogener Vorfälle aufgrund von Netzwerkkonfigurationsfehlern, Routingproblemen, Fehlkonfigurationen der Firewall oder anderen netzwerkbezogenen Problemen, die die Konnektivität oder die Kommunikation beeinträchtigen;</p> <p>g) physische Schäden: schwerwiegende IKT-bezogene Vorfälle, die durch physische Schäden an der IKT-Infrastruktur verursacht werden, die zu Systemversagen führen;</p> <p>h) Sonstiges (bitte angeben).</p> <p>4. Menschliches Versagen (falls ausgewählt, eine oder mehrere der folgenden Optionen wählen):</p> <p>a) Unterlassung (unbeabsichtigt);</p> <p>b) Irrtum;</p> <p>c) Fähigkeiten und Kenntnisse: schwerwiegende IKT-bezogene Vorfälle, die durch mangelndes Fachwissen oder mangelnde Kompetenz im Umgang mit IKT-Systemen oder -Prozessen verursacht werden, was auf unzureichende Ausbildung, unzureichendes Wissen oder Qualifikationsdefizite im Hinblick auf die durchzuführenden Aufgaben oder die Bewältigung technischer Herausforderungen zurückzuführen sein kann;</p> <p>d) unzureichende personelle Ausstattung: schwerwiegende IKT-bezogene Vorfälle, die durch einen Mangel an erforderlichen Ressourcen, einschließlich Hardware, Software, Infrastruktur oder Personal, verursacht werden, einschließlich Situationen, in denen unzureichende Ressourcen zu operativen Ineffizienzen, Systemversagen oder der Unfähigkeit der Unternehmen, die geschäftlichen Anforderungen zu erfüllen, führen;</p> <p>e) Fehlkomunikation;</p> <p>f) Sonstiges (bitte angeben).</p> <p>5. Externes Ereignis (falls ausgewählt, eine oder mehrere der folgenden Optionen wählen):</p> <p>a) Naturkatastrophen/höhere Gewalt;</p> <p>b) Ausfälle bei Dritten;</p> | | | | |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|---|-----------------------------------|---------------------------------------|--|---|
| | c) Sonstiges (bitte angeben). Finanzunternehmen achten darauf, dass bei wiederholten schwerwiegenden IKT-bezogenen Vorfällen die spezifische offensichtliche Ursache des Sicherheitsvorfalls und nicht die in diesem Feld enthaltenen allgemeinen Kategorien berücksichtigt werden. | | | | |
| 4.3. Weitergehende Einstufung der Ursachen des Vorfalls | <p>Weitergehende Einstufung der Ursachen des schwerwiegenden IKT-bezogenen Vorfalls bei der Art des Vorfalls, einschließlich der folgenden weitergehenden Einstufungskategorien im Zusammenhang mit den in Datenfeld 4.2 ausgewiesenen detaillierten Kategorien</p> <p>Das Feld ist bei der Abschlussmeldung ein Pflichtfeld, wenn bestimmte Kategorien, die weiter ausgeführt werden müssen, in Datenfeld 4.2 angegeben werden.</p> <p>2(a) Unzureichende oder mangelhafte Überwachung und Kontrolle:</p> <ul style="list-style-type: none"> a) Überwachung der Einhaltung von Richtlinien; b) Überwachung von Dritt-dienstleistern; c) Überwachung und Überprüfung der Behebung von Schwachstellen; d) Identitäts- und Zugangsmanagement; e) Verschlüsselung und Kryptografie; f) Protokollierung. <p>2(c) Versagen des IKT-Risikomanagementprozesses:</p> <ul style="list-style-type: none"> a) Versäumnis, genaue Risikotoleranzen festzulegen; b) unzureichende Bewertungen von Bedrohungen und Schwachstellen; c) unzureichende Maßnahmen für die Risikobehandlung; d) Unzureichendes Management der IKT-Risiken. <p>2(d) Unzureichende oder nicht funktionierende IKT-Abläufe und IKT-Sicherheitsabläufe:</p> <ul style="list-style-type: none"> a) Schwachstellen- und Patch-Management; b) Änderungsmanagement; c) Kapazitäts- und Leistungsmanagement; d) Management von IKT-Assets und Informationsklassifizierung; | Nein | Nein | Ja | Auswahl (Mehr-fachauswahl): <ul style="list-style-type: none"> — Überwachung der Einhaltung von Richtlinien; — Überwachung von Dritt-dienstleistern; — Überwachung und Überprüfung der Behebung von Schwachstellen; — Identitäts- und Zugangs-management; — Verschlüsselung und Kryptografie; — Protokollierung; — Versäumnis, genaue Risikotoleranzen festzulegen; — unzureichende Bewertungen von Bedrohungen und Schwachstellen; — unzureichende Maßnahmen für die Risiko-behandlung; — unzureichendes Management der IKT-Risiken; — Schwachstellen- und Patch-Management; — Änderungs-management; — Kapazitäts- und Leistungs-management; — Management von IKT-Assets und Informationsklassifizierung; — Sicherung und Wiederher-stellung; — Fehler-behandlung; — unzureichende Beschaffung, Entwicklung und Wartung von IKT-Systemen; — unzureichende Software-Tests oder Versagen von Software-Tests. |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|---|--|-----------------------------------|--|---|----------------|
| | e) Sicherung und Wiederherstellung; f) Fehlerbehandlung. 2(g) Unzureichende Beschaffung, Entwicklung und Wartung von IKT-Systemen: a) Unzureichende Beschaffung, Entwicklung und Wartung von IKT-Systemen; b) unzureichende Software-Tests oder Versagen von Software-Tests. | | | | |
| 4.4. Andere Arten von Ursachen | Finanzunternehmen, die in Datenfeld 4.2 „Sonstiges“ als Art der Ursache ausgewählt haben, geben die anderen Arten von Ursachen an. | Nein | Nein | Ja, wenn in Datenfeld 4.2 „Sonstiges“ als Art der Ursache ausgewählt wurde. | Alphanumerisch |
| 4.5. Angaben zu den Ursachen des Vorfalls | Beschreibung der Abfolge der Ereignisse, die zu dem schwerwiegenden IKT-bezogenen Vorfall geführt haben, und Beschreibung, wie der schwerwiegende IKT-bezogene Vorfall eine offensichtlich ähnliche Ursache hat, wenn dieser Sicherheitsvorfall als wiederholter Vorfall eingestuft wird, einschließlich einer kurzen Beschreibung aller zugrunde liegenden Gründe und Hauptfaktoren, die zum Eintreten des schwerwiegenden IKT-bezogenen Vorfalls beigetragen haben. Bei böswilligen Handlungen Beschreibung des Mechanismus der böswilligen Handlung, einschließlich der verwendeten Taktiken, Techniken und Verfahren, sowie des Eintrittsvektors des schwerwiegenden IKT-bezogenen Vorfalls, gegebenenfalls einschließlich einer Beschreibung der Untersuchungen und Analysen, die zur Ermittlung der Ursachen geführt haben. | Nein | Nein | Ja | Alphanumerisch |
| 4.6. Behebung des Vorfalls | Zusätzliche Angaben zu den Maßnahmen, die ergriffen wurden/geplant sind, um den schwerwiegenden IKT-bezogenen Vorfall dauerhaft zu beheben und zu verhindern, dass sich dieser Vorfall erneut ereignet. Aus dem schwerwiegenden IKT-bezogenen Vorfall gewonnene Erkenntnisse. | Nein | Nein | Ja | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|---|-----------------------------------|--|---|--|
| | <p>Die Beschreibung muss folgende Punkte enthalten:</p> <ol style="list-style-type: none"> 1. Beschreibung der Maßnahmen zur Behebung <ol style="list-style-type: none"> a) Maßnahmen zur dauerhaften Behebung des schwerwiegenden IKT-bezogenen Vorfalls (ausgenommen befristete Maßnahmen); b) bei jeder ergriffenen Maßnahme Angabe der potenziellen Beteiligung eines Dritt Dienstleisters und des Finanzunternehmens; c) Angabe, ob die Verfahren nach dem schwerwiegenden IKT-bezogenen Vorfall angepasst wurden; d) Angabe etwaiger zusätzlicher Kontrollen, die eingeführt wurden oder geplant sind (mit Zeitplan für die Umsetzung). <p>Mögliche Probleme in Bezug auf die Robustheit der betroffenen IT-Systeme bzw. gegebenenfalls in Bezug auf die bestehenden Verfahren oder Kontrollen.</p> <p>Finanzunternehmen geben eindeutig an, wie mit den geplanten Abhilfemaßnahmen die ermittelten Ursachen behoben werden sollen und wann der schwerwiegende IKT-bezogene Vorfall voraussichtlich dauerhaft behoben sein wird.</p> <ol style="list-style-type: none"> 2. Gewonnene Erkenntnisse Finanzunternehmen beschreiben die Ergebnisse der Überprüfung nach dem Vorfall. | | | | |
| 4.7. Datum und Uhrzeit der Behebung der Ursache des Vorfalls | Datum und Uhrzeit der Behebung der Ursache des Vorfalls. | Nein | Nein | Ja | ISO 8601 UTC-Format (JJJJ-MM-TT hh: mm:ss) |
| 4.8. Datum und Uhrzeit der Behebung des Vorfalls | Datum und Uhrzeit der Behebung des Vorfalls. | Nein | Nein | Ja | ISO 8601 UTC-Format (JJJJ-MM-TT hh: mm:ss) |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-meldung | Verpflichtend für die Abschluss-meldung | Feldtyp |
|--|---|-----------------------------------|--|--|----------------|
| 4.9. Angabe, ob das Datum der dauerhaften Behebung der Vorfälle von dem ursprünglich geplanten Umsetzungs-datum abweicht | Gegebenenfalls eine Beschreibung des Grundes, warum das Datum der dauerhaften Behebung der schwerwiegenden IKT-bezogenen Vorfälle von dem ursprünglich geplanten Umsetzungsdatum abweicht. | Nein | Nein | Ja | Alphanumerisch |
| 4.10. Bewertung des Risikos für kritische Funktionen für Abwick-lungs-zwecke | <p>Bewertung, ob der schwerwiegende IKT-bezogene Vorfall ein Risiko für kritische Funktionen im Sinne des Artikels 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates (2) darstellt.</p> <p>Die in Artikel 1 Absatz 1 der Richtlinie 2014/59/EU genannten Unternehmen geben an, ob der in der Vorlage Z07.01 der Durchführungsverordnung (EU) 2018/1624 der Kommission (2) gemeldete und dem betreffenden Unternehmen in der Vorlage Z07.02 zugeordnete Vorfall ein Risiko für kritische Funktionen im Sinne des Artikels 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellt.</p> | Nein | Nein | Ja, wenn der Vorfall ein Risiko für kritische Funktionen von Finanz-unter-neh-men im Sinne des Artikels 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellt | Alphanumerisch |
| 4.11. Für Abwicklungs-behör-den relevante Angaben | <p>Beschreibung, ob und, wenn ja, wie sich der schwerwiegende IKT-bezogene Vorfall auf die Abwicklungsfähigkeit des Unternehmens oder der Gruppe ausgewirkt hat.</p> <p>Die in Artikel 1 Absatz 1 der Richtlinie 2014/59/EU genannten Unternehmen stellen Informationen darüber bereit, ob und, wenn ja, wie sich der schwerwiegende IKT-bezogene Vorfall auf die Abwicklungsfähigkeit des Unternehmens oder der Gruppe ausgewirkt hat.</p> <p>Diese Unternehmen geben auch an, ob sich der schwerwiegende IKT-bezogene Vorfall auf die Solvenz oder Liquidität des Finanzunternehmens auswirkt, und geben die potenzielle Quantifizierung der Auswirkungen an.</p> <p>Diese Unternehmen machen auch Angaben zu den Auswirkungen auf die Aufrechterhaltung des Geschäftsbetriebs, den Auswirkungen auf die Abwicklungsfähigkeit des Unternehmens, etwaigen weitergehenden Auswirkungen des schwerwiegenden IKT-bezogenen Vorfalls auf die Kosten und Verluste, einschließlich der Kapitalposition des Finanzunternehmens, und geben an, ob die vertraglichen Vereinbarungen über die Nutzung von IKT-Diensten im Falle einer Abwicklung des Unternehmens nach wie vor robust und uneingeschränkt durchsetzbar sind.</p> | Nein | Nein | Ja, wenn der Vorfall die Abwick-lungs-fähig-keit des Unterneh-mens oder der Gruppe beeinträchtigt hat | Alphanumerisch |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|---|-----------------------------------|---------------------------------------|--|----------------|
| 4.12. Wesentlichkeits-schwelle für das Einstufungs-kriterium „Wirtschaftliche Auswirkungen“ | Detailierte Informationen über Schwellenwerte, die der schwerwiegende IKT-bezogene Vorfall am Ende erreicht hat, in Bezug auf das in den Artikeln 7 und 14 der Delegierten Verordnung (EU) 2024/1772 genannte Kriterium „Wirtschaftliche Auswirkungen“. | Nein | Nein | Ja | Alphanumerisch |
| 4.13. Betrag der direkten und indirekten Bruttokosten und Verluste | <p>Gesamtbetrag der direkten und indirekten Bruttokosten und Verluste, die dem Finanzunternehmen aufgrund des schwerwiegenden IKT-bezogenen Vorfalls entstanden sind, einschließlich</p> <ul style="list-style-type: none"> a) der Höhe der enteigneten Mittel oder finanziellen Vermögenswerte, für die das Finanzunternehmen haftet, b) der Höhe der Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur, c) der Höhe der Personalkosten, einschließlich der Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung von zusätzlichem Personal, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen des Personals, d) der Höhe der Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen, e) der Höhe der Entschädigungs- und Wiedergutmachungskosten für Kunden, f) der Höhe der Verluste wegen entgangener Einnahmen, g) der Höhe der Kosten für die interne und externe Kommunikation, h) der Höhe der Beratungskosten, einschließlich Kosten für Rechtsberatung, forensische Dienstleistungen und Behebungsdienstleistungen, i) der Höhe der sonstigen Kosten und Verluste, einschließlich: <ul style="list-style-type: none"> i) der in der Gewinn- und Verlustrechnung erfassten direkten Belastungen einschließlich Wertminderungen und Vergleichszahlungen sowie Abwertungen aufgrund des schwerwiegenden IKT-bezogenen Vorfalls, ii) der in der Gewinn- und Verlustrechnung erfassten Rückstellungen oder Rücklagen für wahrscheinliche Verluste im Zusammenhang mit dem schwerwiegenden IKT-bezogenen Vorfall, | Nein | Nein | Ja | Monetär |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischenmeldung | Verpflichtend für die Abschlussmeldung | Feldtyp |
|---|---|-----------------------------------|---------------------------------------|--|--|
| | <p>iii) der drohenden Verluste in Form von Verlusten aufgrund des schwerwiegenden IKT-bezogenen Vorfalls, die vorübergehend auf Übergangs- oder Zwischenkonten gebucht werden und noch nicht in der Gewinn- und Verlustrechnung erfasst sind und die nach einem gewissen Zeitraum, der der Größe und dem Alter des drohenden Verlusts entspricht, erfasst werden sollen,</p> <p>iv) der wesentlichen nicht realisierten Einnahmen im Zusammenhang mit vertraglichen Verpflichtungen gegenüber Dritten, darunter die Entscheidung, einen Kunden nach dem schwerwiegenden IKT-bezogenen Vorfall durch eine Anpassung der Erlöse, bei der die vertraglichen Kosten für einen bestimmten Zeitraum ausgesetzt oder verringert werden, zu entschädigen (anstelle einer Rückerstattung oder einer direkten Zahlung),</p> <p>v) Timing Losses, die über ein Geschäftsjahr hinausgehen und ein Rechtsrisiko nach sich ziehen.</p> <p>Finanzunternehmen berücksichtigen bei ihrer Bewertung Artikel 7 Absätze 1 und 2 der Delegierten Verordnung (EU) 2024/1772. Finanzunternehmen dürfen in diesen Wert keine wie auch immer gearbeiteten Rückflüsse einbeziehen.</p> <p>Finanzunternehmen weisen den Geldbetrag als positiven Wert aus.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung berücksichtigen Finanzunternehmen den Gesamtbetrag der Kosten und Verluste in allen Finanzunternehmen.</p> <p>Finanzunternehmen weisen den Datenpunkt mit einer Mindestpräzision aus, die tausend Einheiten entspricht.</p> | | | | |
| 4.14. Betrag finanziellen Rückflusses der | Gesamtbetrag der finanziellen Rückflüsse. Finanzielle Rückflüsse müssen sich auf den ursprünglichen Verlust beziehen, der durch das Ereignis verursacht wurde, unabhängig davon, wann sie in Form von Geldern oder Zuflüssen wirtschaftlichen Nutzens vereinnahmt werden. | Nein | Nein | Ja | Monetär Finanzunternehmen weisen den Datenpunkt mit einer Mindestpräzision aus, die tausend Einheiten entspricht. |

| Datenfeld | Beschreibung | Verpflichtend für die Erstmeldung | Verpflichtend für die Zwischen-mel-dung | Verpflichtend für die Abschluss-mel-dung | Feldtyp |
|--|--|-----------------------------------|---|--|--|
| 4.15. Angaben dazu, ob sich die nicht schwerwie-genden Vorfälle wiederholt haben | <p>Finanzunternehmen weisen den Geldbetrag als positiven Wert aus.</p> <p>Bei einer aggregierten Meldung gemäß Artikel 7 dieser Verordnung berücksichtigen Finanzunternehmen den Gesamtbetrag der finanziellen Rückflüsse in allen Finanzunternehmen.</p> <p>Angaben dazu, ob ein nicht schwerwiegender IKT-bezogener Vorfall wiederholt eingetreten ist und diese Vorfälle zusammen als schwerwiegender Vorfall im Sinne des Artikels 8 Absatz 2 der Delegierten Verordnung (EU) 2024/1772 zu betrachten sind.</p> <p>Finanzunternehmen geben an, ob sich die nicht schwerwiegenden IKT-bezogenen Vorfälle wiederholt haben und zusammen als ein schwerwiegender IKT-bezogener Vorfall zu betrachten sind.</p> <p>Finanzunternehmen geben auch an, wie oft diese nicht schwerwiegenden IKT-bezogenen Vorfälle eingetreten sind.</p> | Nein | Nein | Ja, wenn der schwer-wie-gende Vorfall mehr als einen nicht schwer-wiegen-den wieder-holten Vorfall umfasst | Alphanumerisch |
| 4.16. Datum und Uhrzeit des Eintretens wiederholter Vorfälle | Wenn Finanzunternehmen wiederholte IKT-bezogene Vorfälle melden, Datum und Uhrzeit des ersten IKT-bezogenen Vorfalls. | Nein | Nein | Ja, bei wieder-holten Vorfällen | ISO 8601 UTC-Format (JJJ-MM-TT hh:mm:ss) |

(¹) 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>).

(²) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (Abl. L 173 vom 12.6.2014, S. 190, ELI: <http://data.europa.eu/eli/dir/2014/59/oj>).

(³) Durchführungsverordnung (EU) 2018/1624 der Kommission vom 23. Oktober 2018 zur Festlegung technischer Durchführungsstandards in Bezug auf Verfahren, Standardformulare und Meldebögen für die Bereitstellung von Informationen für die Erstellung von Abwicklungsplänen für Kreditinstitute und Wertpapierfirmen gemäß der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates und zur Aufhebung der Durchführungsverordnung (EU) 2016/1066 der Kommission (Abl. L 277 vom 7.11.2018, S. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ANHANG III

VORLAGEN FÜR DIE MELDUNG ERHEBLICHER CYBERBEDROHUNGEN

| Feldnummer | Datenfeld |
|------------|---|
| 1 | Name des Unternehmens, das die Meldung übermittelt |
| 2 | Identifikationscode des Unternehmens, das die Meldung übermittelt |
| 3 | Art des Finanzunternehmens, das die Meldung übermittelt |
| 4 | Name des Finanzunternehmens |
| 5 | LEI-Code des Finanzunternehmens |
| 6 | Name des Hauptansprechpartners |
| 7 | E-Mail-Adresse des Hauptansprechpartners |
| 8 | Telefonnummer des Hauptansprechpartners |
| 9 | Name des zweiten Ansprechpartners |
| 10 | E-Mail-Adresse des zweiten Ansprechpartners |
| 11 | Telefonnummer des zweiten Ansprechpartners |
| 12 | Datum und Uhrzeit der Feststellung der Cyberbedrohung |
| 13 | Beschreibung der erheblichen Cyberbedrohung |
| 14 | Angaben zu möglichen Auswirkungen |
| 15 | Kriterien für die Einstufung potenzieller Vorfälle |
| 16 | Status der Cyberbedrohung |
| 17 | Zur Verhinderung des Eintretens ergriffene Maßnahmen |
| 18 | Benachrichtigung anderer Beteiligter |
| 19 | Kompromittierungsindikatoren |
| 20 | Sonstige zweckdienliche Angaben |

ANHANG IV

DATENGLOSSAR UND ANLEITUNG FÜR DIE MELDUNG ERHEBLICHER CYBERBEDROHUNGEN

| Datenfeld | Beschreibung | Pflichtfeld | Feldtyp |
|--|--|--|--|
| 1. Name des Unternehmens, das die Meldung übermittelt | Vollständige juristische Bezeichnung des Unternehmens, das die Meldung übermittelt. | Ja | Alphanumerisch |
| 2. Identifikationscode des Unternehmens, das die Meldung übermittelt | Identifikationscode des Unternehmens, das die Meldung übermittelt. Übermitteln Finanzunternehmen die Meldung, ist die Rechtsträgerkennung (Legal Entity Identifier; LEI-Code), ein eindeutiger alphanumerischer 20-stelliger Code nach ISO 17442-1:2020. Übermittelt ein Drittienstleister eine Meldung für ein Finanzunternehmen, kann er einen Identifikationscode verwenden, der in den gemäß Artikel 28 Absatz 9 der Verordnung (EU) 2022/2554 angenommenen technischen Durchführungsstandards festgelegt ist. | Ja | Alphanumerisch |
| 3. Art des Finanzunternehmens, das die Meldung übermittelt | Art des Unternehmens gemäß Artikel 2 Absatz 1 Buchstaben a bis t der Verordnung (EU) 2022/2554, das die Meldung übermittelt. | Ja, wenn die Meldung nicht direkt von dem betroffenen Finanzunternehmen übermittelt wird | Auswahl (Mehrfachauswahl): — Kreditinstitut; — Zahlungsinstitut; — Ausgenommenes Zahlungsinstitut; — Kontoinformations-dienstleister; — E-Geld-Institut; — Ausgenommenes E-Geld-Institut; — Wertpapierfirma; — Anbieter von Kryptowerte-Dienstleistungen; — Emittent wertreferenzierter Token; — Zentralverwahrer; — Zentrale Gegenpartei; — Handelsplatz; — Transaktionsregister; — Verwalter alternativer Investmentfonds; — Verwaltungsgesellschaft; — Datenbereitstellungs-dienst; |

| Datenfeld | Beschreibung | Pflichtfeld | Feldtyp |
|---|--|--|--|
| | | | <ul style="list-style-type: none"> — Versicherungs- und Rückversicherungsunternehmen; — Versicherungsvermittler, Rückversicherungs-vermittler und Versicherungsvermittler in Nebentätigkeit; — Einrichtung der betrieblichen Altersversorgung; — Ratingagentur; — Administrator kritischer Referenzwerte; — Schwarmfinanzie-rungsdiens-leister; — Verbriefungsregister. |
| 4. Name des Finanzunternehmens | Vollständige juristische Bezeichnung des Finanzunternehmens, das die erhebliche Cyberbedrohung meldet. | Ja, wenn es sich bei dem Finanzunternehmen nicht um das Unternehmen handelt, das die Meldung übermittelt | Alphanumerisch |
| 5. LEI-Code des Finanzunternehmens | Die nach der Internationalen Organisation für Normung zugewiesene Rechtsträgerkennung (LEI-Code) des Finanzunternehmens, das die erhebliche Cyberbedrohung meldet. | Ja, wenn das Finanzunternehmen, das die erhebliche Cyberbedrohung meldet, nicht mit dem meldenden Unternehmen identisch ist | Eindeutiger alphanumerischer Code mit 20 Zeichen nach ISO 17442-1:2020 |
| 6. Name des Hauptansprechpartners | Vor- und Nachname des Hauptansprechpartners des Finanzunternehmens. | Ja | Alphanumerisch |
| 7. E-Mail-Adresse des Hauptansprechpartners | E-Mail-Adresse des Hauptansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann. | Ja | Alphanumerisch |
| 8. Telefonnummer des Hauptansprechpartners | Telefonnummer des Hauptansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann. Die Telefonnummer ist mit allen internationalen Vorwahlen anzugeben (z. B. +33 XXXXXXXX). | Ja | Alphanumerisch |
| 9. Name des zweiten Ansprechpartners | Vor- und Nachname des zweiten Ansprechpartners des Finanzunternehmens oder des Unternehmens, das die Meldung im Namen des Finanzunternehmens übermittelt. | Ja, wenn Vor- und Nachname des zweiten Ansprechpartners des Finanzunternehmens oder eines Unternehmens, das die Meldung für das Finanzunternehmen übermittelt, vorliegen | Alphanumerisch |

| Datenfeld | Beschreibung | Pflichtfeld | Feldtyp |
|--|--|---|--|
| 10. E-Mail-Adresse des zweiten Ansprechpartners | Gegebenenfalls E-Mail-Adresse des zweiten Ansprechpartners oder die funktionale E-Mail-Adresse des Teams, an den bzw. das sich die zuständige Behörde in der Folgemitteilung wenden kann. | Ja, wenn die E-Mail-Adresse des zweiten Ansprechpartners oder die funktionale E-Mail-Adresse des Teams, an den bzw. das sich die zuständige Behörde in der Folgemitteilung wenden kann, vorliegen | Alphanumerisch |
| 11. Telefonnummer des zweiten Ansprechpartners | Gegebenenfalls Telefonnummer des zweiten Ansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann. Die Telefonnummer ist mit allen internationalen Vorwahlen anzugeben (z. B. +33 XXXXXXXX). | Ja, wenn die Telefonnummer des zweiten Ansprechpartners, an den sich die zuständige Behörde in der Folgemitteilung wenden kann, vorliegt | Alphanumerisch |
| 12. Datum und Uhrzeit der Feststellung der Cyber-bedrohung | Datum und Uhrzeit der Kenntnisnahme der erheblichen Cyberbedrohung durch das Finanzunternehmen. | Ja | ISO 8601 UTC-Format (JJJJ-MM-TT hh:mm:ss) |
| 13. Beschreibung der erheblichen Cyber-bedrohung | Beschreibung der wichtigsten Aspekte der erheblichen Cyberbedrohung. Finanzunternehmen übermitteln folgende Informationen: a) Allgemeine Darstellung der relevantesten Aspekte der erheblichen Cyberbedrohung; b) Die damit verbundenen Risiken, einschließlich potenzieller Schwachstellen der Systeme des Finanzunternehmens, die ausgenutzt werden könnten; c) Angaben zur Eintrittswahrscheinlichkeit der erheblichen Cyberbedrohung und d) Angaben zur Informationsquelle über die Cyberbedrohung. | Ja | Alphanumerisch |
| 14. Angaben zu möglichen Auswirkungen | Angaben zu den möglichen Auswirkungen der Cyberbedrohung auf das Finanzunternehmen, seine Kunden oder Gegenparteien im Finanzbereich, wenn die Cyberbedrohung eingetreten ist | Ja | Alphanumerisch |
| 15. Kriterien für die Einstufung potenzieller Vorfälle | Die Einstufungskriterien, die eine Meldung über einen schwerwiegenden Vorfall hätten auslösen können, wenn die Cyberbedrohung eingetreten wäre. | Ja | Auswahl (Mehrfachauswahl): — Betroffene Kunden, Gegenparteien im Finanzbereich und Transaktionen — Reputationsschaden — Dauer und Ausfallzeiten — Geografische Ausbreitung — Datenverluste — Betroffene Dienstleistungen kritische — Wirtschaftliche Auswirkungen |

| Datenfeld | Beschreibung | Pflichtfeld | Feldtyp |
|--|---|---|----------------------------------|
| 16. Status der Cyber-bedrohung | <p>Angaben zum Status der Cyberbedrohung für das Finanzunternehmen und dazu, ob sich die Bedrohungsaktivität verändert hat.</p> <p>Wenn die Cyberbedrohung nicht mehr mit den Informationssystemen des Finanzunternehmens kommuniziert, kann der Status auf inaktiv gesetzt werden. Liegen dem Finanzunternehmen Informationen darüber vor, dass die Bedrohung gegen andere Parteien oder das Finanzsystem insgesamt aktiv bleibt, ist der Status als aktiv zu kennzeichnen.</p> | Ja | Auswahl: — Aktiv — Inaktiv |
| 17. Zur Verhinderung des Eintretens ergriffene Maßnahmen | Gegebenenfalls detaillierte Informationen über die Maßnahmen, die das Finanzunternehmen ergriffen hat, um das Eintreten der erheblichen Cyberbedrohungen zu verhindern. | Ja | Alphanumerisch |
| 18. Benachrichtigung anderer Beteiligter | Angaben zur Benachrichtigung anderer Finanzunternehmen oder Behörden über die Cyberbedrohung. | Ja, wenn andere Finanzunternehmen oder Behörden über die Cyberbedrohung informiert wurden | Alphanumerisch |
| 19. Kompromittierungs-indikatoren | <p>Gegebenenfalls Informationen im Zusammenhang mit der erheblichen Cyberbedrohung, die dazu beitragen können, böswillige Aktivitäten innerhalb eines Netzwerks oder Informationssystems zu erkennen (Kompromittierungsindikatoren).</p> <p>Die von dem Finanzunternehmen bereitgestellten Kompromittierungsindikatoren können unter anderem die folgenden Datenkategorien enthalten:</p> <ul style="list-style-type: none"> a) IP-Adressen; b) URL-Adressen; c) Domains; d) Datei-Hashes; e) Daten zu Schadsoftware (Name der Schadsoftware, Dateinamen und ihre Speicherorte, spezifische Registrierungsschlüssel im Zusammenhang mit Schadsoftware-Aktivitäten); f) Daten zu Netzaktivitäten (Ports, Protokolle, Adressen, Referrer, User Agents, Header, spezifische Protokolle oder auffällige Muster im Netzwerkverkehr); g) Daten zu E-Mail-Nachrichten (Absender, Empfänger, Betreff, Header, Inhalt); h) DNS-Anfragen und Registrierungskonfigurationen; i) Nutzerkontoaktivitäten (Anmeldungen, Kontoaktivitäten privilegierter Nutzer, Rechteausweitung); j) Datenbankverkehr (Lesen/Schreiben), Anfragen für dieselbe Datei. <p>Diese Art von Informationen kann Daten umfassen, die sich unter anderem auf Indikatoren, die Muster im Netzwerkverkehr im Zusammenhang mit bekannten Angriffen/Botnetkommunikation beschreiben, IP-Adressen von mit Schadsoftware infizierten Rechnern (Bots), Daten über von Schadsoftware genutzte „Command and Control“-Server (in der Regel Domains oder IP-Adressen) und URLs in Bezug auf Phishing-Websites oder Websites, bei denen beobachtet wurde, dass sie für das Hosting von Schadsoftware oder Exploit Kits genutzt wird, beziehen.</p> | Ja, wenn Informationen über Kompromittierungs-indikatoren im Zusammenhang mit der Cyberbedrohung verfügbar sind | Alphanumerisch |
| 20. Sonstige zweckdienliche Angaben | Sonstige zweckdienliche Angaben zu der erheblichen Cyberbedrohung. | Ja, falls zutreffend und wenn andere Informationen verfügbar sind, die nicht in der Vorlage ausgewiesen sind. | Alphanumerisch |