ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

15.10.2026

MELDEHINWEISE – SCHWERWIEGENDE IKT-BEZOGENE VORFÄLLE GEM. DORA

ZWECK

Das gegenständliche Dokument beinhaltet operative Hinweise für die Meldung schwerwiegender IKT-bezogener Vorfälle gemäß Artikel 19 Absatz 1 DORA von Finanzunternehmen an die FMA. Die operativen Hinweise geben Orientierung zu Themen, die für die Meldung wesentlicher IKT-bezogener Vorfälle gemäß DORA sowie den einschlägigen technischen Standards relevant sind.

Hauptziel des Dokuments ist es, die **Datenqualität zu verbessern** und eine **höhere Konsistenz der Meldepraktiken** zu fördern.

Die Anwendung dieser Meldehinweise unterstützt die Finanzunternehmen bei der fristgerechten und qualitativ hochwertigen Erfüllung ihrer Meldepflichten gemäß Artikel 19 Absatz 1 DORA. Durch die Bereitstellung konkreter Hinweise, Beispiele und Klarstellungen werden Rückfragen, Korrekturschleifen sowie zusätzlicher Abstimmungsaufwand mit der FMA reduziert. Dies trägt zu einer effizienteren und einheitlicheren Abwicklung des Meldeprozesses bei.

Die Meldehinweise sind bei der Erfüllung der Meldepflichten gemäß Artikel 19 Absatz 1 DORA zu berücksichtigen.

Siehe hierzu insbesondere auch das Dokument **Operational Instructions der ESAs**. Das gegenständliche Dokument enthält vorwiegend Hinweise und Beobachtungen der FMA, welche teilweise auch die Erfahrungen und Erkenntnisse der ESAs widerspiegeln.

DEFINITIONEN

- FMA – österreichische Finanzmarktaufsichtsbehörde
- FU – Finanzunternehmen
- SI – Signifikantes Institut

- EZB – Europäische Zentralbank
- ESA – Europäische Aufsichtsbehörden
- IP – **FMA-Incoming Plattform**
- DORA – **Verordnung (EU) 2022/2554** des Europäischen Parlaments und des Rates über die digitale operationale Resilienz im Finanzsektor
- ITS zu Standardformularen, Vorlagen und Verfahren – **Durchführungsverordnung (EU) 2025/302 der Kommission**
  zur Festlegung technischer Durchführungsstandards für die Anwendung von DORA in Bezug auf die Standardformulare, Vorlagen und Verfahren, nach denen Finanzunternehmen einen schwerwiegenden IKT-bezogenen Vorfall zu melden sowie eine erhebliche Cyberbedrohung zu notifizieren haben.
- RTS zu Inhalt und Fristen – **Delegierte Verordnung (EU) 2025/301 der Kommission**
  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
- RTS zu Klassifizierungskriterien – **Delegierte Verordnung (EU) 2024/1772 der Kommission**
  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
- DORA-VG – **DORA-Vollzugsgesetz**

KONTAKT: dora@fma.gv.at

Meldeweg & allgemeine Hinweise

Schwerwiegende IKT-bezogene Vorfälle sind von den Finanzunternehmen an die FMA zu melden.
Auch SI haben solche Vorfälle an die jeweils zuständige nationale Behörde (in Österreich an die FMA) zu erstatten. Die FMA leitet diese unverzüglich an die EZB weiter.

Siehe dazu bereits das FMA-Schreiben zu DORA: neue Anzeigen und Meldungen gemäß DORA

ÖSTERREICHISCHE FMA · FINANZMARKTAUFSICHT

Meldeweg & allgemeine Hinweise	
Einbringung der Erstmeldung	Meldung eines **neuen** schwerwiegenden IKT-bezogenen Vorfalls Einbringungsweg auf der IP: Menüleiste „DORA“ – „**Neue Meldung**“ – „**neue Meldung eines schwerwiegenden IKT-bezogenen Vorfalls**" 1. Schritt: Datei hochladen 2. Schritt: File prüfen (Validierung) 3. Meldung an FMA absenden, ohne Ankreuzen des Kästchens „Testmeldung“ (Testmeldungen werden nicht in das FMA-System übernommen und dienen nur für Ihre Testzwecke).
Einbringung der Zwischenmeldung, Abschlussmeldung und Reklassifizierungsmeldung	Jede weitere Meldung (**Zwischenmeldung, Abschlussmeldung und Reklassifizierungsmeldung**), die zu einem **bereits (erst-)gemeldeten Vorfall** eingebracht wird Einbringungsweg auf der IP: Menüleiste „DORA“ – „**Neue Meldung**“ – „**Meldung zu vorhandener Meldung eines schwerwiegenden IKT-bezogenen Vorfalls hinzufügen**" 1. Schritt: Datei hochladen 2. Schritt: File prüfen (Validierung) 3. Vorhandene Vorfalls-ID auswählen (diese wird im Zuge der erfolgreich eingebrachten Erstmeldung per Mail übermittelt) 4. Meldung an FMA absenden, ohne Ankreuzen des Kästchens „Testmeldung“ (Testmeldungen werden nicht in das FMA-System übernommen und dienen nur für Ihre Testzwecke).
Technisch-konsolidierte Meldungen für von der EZB beaufsichtigte Institute (idR SI)	Gem. Artikel 7 Absatz 2 ITS zu Standardformularen, Vorlagen und Verfahren sind **Kreditinstitute**, die gemäß Artikel 2 Nummer 16 der Verordnung (EU) Nr. 468/2014 der Europäischen Zentralbank **als von erheblicher Bedeutung angesehen werden** (*ebenso Betreiber von Handelsplätzen und zentrale Gegenparteien*) vom konsolidierten Reporting **ausgenommen** und haben auf **Einzelinstitutsbasis** zu melden.

Meldeweg & allgemeine Hinweise	
	Die FMA ermöglicht jedoch für **bedeutende Kreditinstitute** ebenso eine Konsolidierung auf technischer Basis. Dafür ist ein separates Meldetemplate notwendig. Sollten Sie dieses in Anspruch nehmen wollen, nehmen Sie Kontakt mit Ihrem FMA-SPOC auf. Bei der Meldung mit dem technisch-konsolidierten Meldetemplate ist Folgendes **zwingend** zu beachten: • **Die technisch-konsolidierte Meldung darf <u>ausschließlich</u> von Instituten verwendet werden, welche der direkten Aufsicht der EZB unterliegen.** • Andere Institute (zB LSI, E-Geld-Institute, Non-CRR, …) dürfen in diesem Meldetemplate NICHT angeführt werden. Es ist stets eine separate Meldung einzubringen (Einzelmeldung oder „normal“ konsolidierte Meldung mittels des Meldetemplates auf der IP). • Melden Sie keinesfalls sektorübergreifend (zB für Banken, Versicherungen und Wertpapierfirmen) in einer technisch-konsolidierten Meldung. • Alle Werte sind mit einem „;“ zu trennen. Genaue Infos entnehmen Sie den reporting instructions des Meldetemplates für technisch-konsolidierte Meldungen. Bei einer „normalen“ konsolidierten Meldung hingegen dürfen Werte (wie zB betroffene Kund:innen) zusammengerechnet werden.
Zweigniederlassungen	Es wurde versucht, eine Meldung für eine Zweigniederlassung auf der IP der FMA einzubringen. Meldungen für **Zweigniederlassungen sind der Heimat-Aufsichtsbehörde der Hauptniederlassung** zu melden.
Einbringung von Erst-, Zwischen- und Abschlussmeldung in einem Schritt	Es ist möglich, Erst-, Zwischen- und Abschlussmeldung **in einem Schritt** einzubringen, wenn: • der reguläre Geschäftsbetrieb wiederhergestellt ist oder die Ursachenanalyse abgeschlossen wurde und • die Fristen gemäß Artikel 5 des RTS zu Inhalt und Fristen eingehalten werden. Es müssen bereits alle Daten zum Vorfall vorliegen. Siehe Artikel 2 des ITS zu Standardformularen, Vorlagen und Verfahren.
Recurring Incidents – „Wiederkehrende Vorfälle“	Recurring Incidents sind zu melden, sofern einzelne Vorfälle nicht als kritisch eingestuft werden, jedoch im Zeitraum der letzten **sechs Monate mindestens zweimal** aufgetreten sind, die **gleiche Grundursache** aufweisen und **zusammengenommen die Kriterien** für die Betrachtung als **schwerwiegender Vorfall erfüllen.**

Meldeweg & allgemeine Hinweise	
	Relevante Felder gem. ITS zu Standardformularen, Vorlagen und Verfahren: Feld 2.2 der Erstmeldung, Feld 3.2 der Zwischenmeldung und Feld 4.5, 4.15 und 4.16 der Abschlussmeldung.
Einhaltung der Meldefristen und Sanktionen Besonderheiten bei wesentlichen und wichtigen Einrichtungen gem. NIS-2-RL/NISG 2026	Die Fristen zur Meldung von schwerwiegenden IKT-bezogenen Vorfällen gemäß DORA sind verpflichtend einzuhalten. Fristverletzungen können als Verstöße gegen die Meldepflichten nach Artikel 19 DORA geahndet werden. Das **DORA-VG** sieht hierfür Geldstrafen von **bis zu EUR 150.000** für verantwortliche natürliche Personen vor. Gegen juristische Personen können Geldstrafen von **bis zu EUR 500.000 oder bis zu 1 % des jährlichen Gesamtnettoumsatzes** verhängt werden, **wobei der höhere Betrag maßgeblich ist**. **Meldefristen** Die Fristen finden sich in Artikel 5 des RTS zu Inhalt und Fristen und lauten wie folgt: **Erstmeldung** • So früh wie möglich, spätestens jedoch innerhalb von 4 Stunden nach Einstufung des Vorfalls als schwerwiegend und maximal 24 Stunden nach Kenntniserlangung vom Vorfall. • Wird der Vorfall erst später als schwerwiegend eingestuft, ist die Erstmeldung innerhalb von 4 Stunden nach dieser Einstufung zu übermitteln. **Zwischenmeldung** • Spätestens 72 Stunden nach Übermittlung der Erstmeldung, auch wenn sich Status oder Handhabung des Vorfalls nicht geändert haben. • Etwaige aktualisierte Zwischenmeldungen sind unverzüglich zu übermitteln, jedenfalls jedoch sobald der reguläre Geschäftsbetrieb wiederaufgenommen wurde. **Abschlussmeldung** • Spätestens einen Monat nach Übermittlung der Zwischenmeldung oder gegebenenfalls nach der letzten aktualisierten Zwischenmeldung.

Meldeweg & allgemeine Hinweise	
	Kann eine Meldung nicht fristgerecht übermittelt werden, ist die zuständige Behörde unverzüglich, spätestens jedoch innerhalb der jeweiligen Frist, unter Angabe der Gründe für die Verzögerung zu informieren (Artikel 5 Absatz 3 RTS zu Inhalt und Fristen). **Besondere Fristenregelung** Fällt eine Meldefrist auf ein Wochenende oder einen Feiertag, kann die Meldung bis 12:00 Uhr des nächsten Arbeitstages übermittelt werden. **Achtung:** Diese Fristverlängerung gilt nicht für Erst- und Zwischenmeldungen von Kreditinstituten, zentralen Gegenparteien, Handelsplätzen sowie sonstigen Finanzunternehmen, die gemäß Artikel 3 der Richtlinie (EU) 2022/2555 (**NIS-2-Richtlinie**) als **wesentliche oder wichtige Einrichtungen** eingestuft sind. **Hinweis zum NISG 2026:** Mit Inkrafttreten des NISG 2026 in Österreich ab 1. Oktober 2026 sollten Finanzunternehmen prüfen, ob sie als wesentliche oder wichtige Einrichtung im Sinne der NIS-2-Regelungen einzustufen sind. **Für diese Unternehmen kommen die genannten Fristenerleichterungen <u>nicht</u> zur Anwendung.**
Böswillige Zugriffe – Meldepflicht bereits bei Verdacht auf Datenverlust – auch auf Ebene von IKT-(Sub-)Dienstleistern	**Erfolgreiche, böswillige und unbefugte Zugriffe** stellen nach Artikel 6 lit. c RTS ein Kriterium für die Beurteilung der Kritikalität betroffener Dienstleistungen dar. Die FMA empfiehlt daher, bei entsprechenden Vorfällen eine frühzeitige und umfassende Prüfung vorzunehmen, ob die Voraussetzungen für eine Meldung nach DORA vorliegen. Bei dieser Beurteilung ist zu berücksichtigen, dass DORA hinsichtlich des Begriffs „Netz- und Informationssysteme“ auf die Definition der NIS-2-Richtlinie verweist. Vor diesem Hintergrund sollten nicht ausschließlich Systeme betrachtet werden, die unmittelbar vom Finanzunternehmen selbst betrieben werden. Vielmehr können auch Systeme und Daten relevant sein, die für die Erbringung, Absicherung oder Aufrechterhaltung der Dienstleistungen des Finanzunternehmens von Bedeutung sind. Insbesondere gilt:

Meldeweg & allgemeine Hinweise	
	• Bereits ein begründeter Verdacht auf einen Datenverlust infolge eines erfolgreichen, böswilligen und unbefugten Zugriffs kann Anlass für eine entsprechende Prüfung der Meldepflicht sein, auch wenn zu diesem Zeitpunkt noch keine abschließende forensische Bestätigung vorliegt. • Ergibt eine spätere Analyse, dass sich der Verdacht nicht bestätigt, kann eine Reklassifizierung des Vorfalls in Betracht kommen. • Für die Beurteilung erfolgreicher, böswilliger und unbefugter Zugriffe ist unerheblich, ob die betroffenen Netz- und Informationssysteme kritische oder wichtige Funktionen unterstützen. • Bei der Beurteilung sollten auch Vorfälle im Zusammenhang mit IKT-Drittdienstleistern oder deren Subdienstleistern berücksichtigt werden. • Dies kann insbesondere Konfigurations-, Betriebs- oder Protokolldaten (Logdaten) umfassen, auch wenn diese bei einem IKT-Drittdienstleister gespeichert, verarbeitet oder übertragen werden. Die vorstehenden Ausführungen orientieren sich an der derzeitigen Auslegung von DORA und den einschlägigen technischen Regulierungsstandards. **Hinweis:** Maßgeblich bleiben die Vorgaben von DORA, den RTS sowie die Auslegung durch die Europäischen Aufsichtsbehörden (ESAs). Sofern die ESAs künftig weitere Konkretisierungen veröffentlichen, wird die FMA ihre Aufsichtspraxis an diesen Vorgaben ausrichten.

HINWEISE DER FMA

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
1	Verwendete Sprache in den DORA-Incident-Meldungen	Alle	Die ESAs erhalten Vorfallmeldungen unter Verwendung einer Vorlage, deren	Die für die Übermittlung von Vorfallmeldungen zuständigen Stellen können berücksichtigen, dass die zuständigen Behörden voraussichtlich die von den ESAs vorgegebenen Vorlagen in englischer Sprache für die Meldung an die ESAs verwenden werden (d. h. Überschriften/Elemente und Werte, die in

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
			Überschriften und Werte in die jeweiligen Landessprachen übersetzt wurden.	geschlossenen Antwortfeldern angegeben werden, basieren auf der Terminologie der englischen Sprachfassung der ITS 2025/302). **Freitextfelder können weiterhin in der jeweils anwendbaren Landessprache ausgefüllt werden.** Quelle: **Operational Instructions der ESAs** (ID 1, Seite 2).
2	Eindeutige Identifizierung eines Vorfalls	1.3a, 1.3b, 2.1	Die in den Feldern 1.3a/1.3b bzw. 2.1 gemeldeten Informationen werden zwischen Erstmeldung, Zwischenmeldung und Abschlussmeldung nicht konsistent fortgeführt.	Vorfälle werden zunächst mittels **Erstmeldung** gemeldet. Je nach weiterer Entwicklung des Vorfalls können anschließend **eine oder mehrere Zwischenmeldungen** übermittelt werden. Der Meldeprozess wird grundsätzlich mit der **Abschlussmeldung** beendet. Ändert sich die Einstufung eines Vorfalls, ist unabhängig vom aktuellen Stand des Meldeprozesses unverzüglich eine **Reklassifizierungsmeldung** einzureichen. Mit der Übermittlung einer Reklassifizierungsmeldung gilt der Meldeprozess als abgeschlossen; eine zusätzliche Abschlussmeldung ist in diesem Fall nicht erforderlich. Damit alle Meldungen während des gesamten Meldezyklus eindeutig demselben Vorfall zugeordnet werden können, verwenden die ESAs bestimmte Identifikationsmerkmale: • die Felder 1.3a bzw. 1.3b mit dem Identifikationscode der meldenden Einrichtung sowie • das Feld 2.1 mit dem von der Finanzinstitution vergebenen Vorfallsreferenzcode. Die in diesen Feldern angegebenen Werte sind von der Erstmeldung bis zur Abschlussmeldung unverändert beizubehalten. Sie dienen der eindeutigen Identifizierung eines Vorfalls über den gesamten Meldezyklus hinweg. Änderungen dieser Angaben können zu einer fehlerhaften Zuordnung von Meldungen oder zu einer irrtümlichen Mehrfacherfassung (Doppelzählung) desselben Vorfalls führen. Quelle: **Operational Instructions der ESAs** (ID 6, Seite 3).

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
3	Angaben bei *type of the affected financial entity*	1.4	Angaben stimmen nicht mit Konzession überein	**Feld 1.4 dient der Angabe des Typs des Finanzunternehmens gemäß Artikel 2 Absatz 1 Buchstaben (a) bis (t) DORA, für das die Meldung erstattet wird.** In der Praxis wurde wiederholt beobachtet, dass in Feld 1.4 der Unternehmenstyp „payment institution“ ausgewählt wurde, obwohl die meldende Einrichtung tatsächlich als „credit institution“ konzessioniert ist. Grundsätzlich ist in diesem Feld jener Unternehmenstyp anzugeben, für den die meldende Einheit über eine **aufsichtsrechtliche Konzession** verfügt. Die korrekte Auswahl ist wesentlich für die rechtliche Einordnung und aufsichtsrechtliche Verarbeitung der Meldung. **Unternehmen mit mehreren Konzessionen** Verfügt ein Finanzunternehmen über mehrere einschlägige Konzessionen, sind in Feld 1.4 sämtliche zutreffenden Unternehmenstypen auszuwählen. Im Fall einer aggregierten Meldung gemäß Artikel 7 der ITS zu Standardformularen, Vorlagen und Verfahren sind alle Typen von Finanzunternehmen anzugeben, die von der aggregierten Meldung erfasst werden (z. B. *payment institution*, *credit institution*). Bei sektorübergreifenden aggregierten Meldungen, die mehrere Kategorien von Finanzunternehmen umfassen (z. B. Kreditinstitute, Versicherungsunternehmen und Wertpapierfirmen), sind die Meldungen sektorweise getrennt einzubringen. Unterschiedliche Sektoren sind nicht in einer gemeinsamen aggregierten Meldung zusammenzufassen.
4	Beschreibung des Vorfalls	2.4	Sehr knappe Beschreibungen	**In Feld 2.4 ist eine möglichst aussagekräftige Beschreibung des Vorfalls bereitzustellen. Der FMA ist bewusst, dass zum Zeitpunkt der Erstmeldung aufgrund des laufenden Vorfalls regelmäßig noch nicht sämtliche Informationen vorliegen.** Sofern die Beschreibung in der Erstmeldung noch unvollständig ist, sind die Angaben in den nachfolgenden Zwischen- und Abschlussmeldungen entsprechend zu ergänzen und zu konkretisieren.

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
				Mit zunehmender Erkenntnislage wird erwartet, dass die Darstellung des Vorfalls laufend aktualisiert und präzisiert wird. Dadurch soll ein möglichst vollständiges Bild des Vorfalls und dessen Entwicklung über den gesamten Meldezyklus hinweg gewährleistet werden. Relevante Informationen können ebenso in Feld 2.10 eingetragen werden.
5	Für die Meldung ausschlaggebende Kriterien	2.5	Keine oder zu wenige ausschlaggebende Kriterien angegeben	**Feld 2.5** erfasst die **Klassifizierungskriterien** gemäß des RTS zu Klassifizierungskriterien, **die zur Einstufung des IKT-bezogenen Vorfalls als schwerwiegend („major“)** und damit zur entsprechenden Meldung und weiteren Berichterstattung geführt haben. Der **Klassifizierungsansatz** für DORA-IKT-Vorfälle gemäß Artikel 8 Absatz 1 des RTS zu Klassifizierungskriterien sieht vor, dass **neben dem Kriterium „Critical Services affected“** entweder ein **böswilliger Zugriff** im Sinne des Artikels 9 Absatz 5 Buchstabe b oder **mindestens zwei weitere Wesentlichkeitsschwellen** erfüllt sein müssen (Artikel 8 Absatz 1 lit. b RTS zu Klassifizierungskriterien). Die Betroffenheit kritischer Dienste stellt somit eine **zwingende Voraussetzung** für die Einstufung eines IKT-bezogenen Vorfalls als schwerwiegend dar. **Aus Gründen der Konsistenz und Vollständigkeit der Meldungen sollte daher bei als schwerwiegend eingestuften Vorfällen das Kriterium „Critical Services affected“ in Feld 2.5 stets ausdrücklich ausgewählt werden.** Daher sind in Feld 2.5 sämtliche Klassifizierungskriterien anzugeben, die für die Meldung des IKT-Vorfalls ausschlaggebend waren. Feld 2.5 ist bei jeder weiteren Meldung (Zwischen- oder Abschlussmeldung) zu **aktualisieren**, sofern sich die maßgeblichen Klassifizierungskriterien geändert haben. Wird festgestellt, dass die zugrunde liegenden Klassifizierungskriterien **zu keinem Zeitpunkt erfüllt waren**, ist die eingebrachte Meldung entsprechend zu reklassifizieren. Quelle: Operational Instructions der ESAs (ID 7, Seite 3).

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
6	Ausschluss des Herkunftsmitgliedstaats Feld 2.6 *„Materiality thresholds for the classification criterion 'Geographical spread'"*	2.6	Im Feld 2.6 wird das **Herkunftsland** (in Österreich: AT) des betroffenen Unternehmens in der Liste der Länder zur „geografischen Ausbreitung" angeführt.	Wie in Artikel 4 RTS zu Klassifizierungskriterien festgelegt, bezieht sich die **„geografische Ausbreitung"** auf die Bewertung der Auswirkungen des Vorfalls **auf andere Mitgliedstaaten**. Feld 2.6 dient der Angabe der geografischen Ausbreitung des Vorfalls und erfasst daher ausschließlich jene Länder, in denen der Vorfall **zusätzlich** Auswirkungen hatte. Das Herkunftsland des hauptsächlich betroffenen Finanzunternehmens (in Österreich: AT) darf nicht in Feld 2.6 angegeben werden. Hat der Vorfall **nur Auswirkungen auf Österreich**, so ist das Feld 2.6 **leer zu lassen**. Hatte der Vorfall beispielsweise Auswirkungen in Österreich und Deutschland, so ist nur „DE" im Feld 2.6 anzuführen. Quelle: **Operational Instructions der ESAs** (ID 8, Seite 3).
7	Standardisierte Angaben: Informationen zum Ursprung bei Drittdienstleistern oder anderen Finanzinstituten	2.8	Schwierigkeiten bei der automatisierten Verarbeitung und Analyse der Angaben in **Feld 2.8**.	**Feld 2.8** gibt an, ob der Vorfall von einem **Drittdienstleister (Third-Party Provider, TPP)** oder einem anderen **Finanzunternehmen (Financial Entity, FE)** ausgeht. Sofern dies der Fall ist, sind der Name des betreffenden TPP bzw. der anderen FE, deren Identifikationscode sowie die Art des verwendeten Identifikationscodes (z. B. **LEI** oder **EUID**) anzugeben. Zur Gewährleistung einer konsistenten Berichterstattung empfehlen die **Europäischen Aufsichtsbehörden (ESAs)**, Feld 2.8 in einem **standardisierten Format** zu befüllen. Dabei sind die nachstehenden Elemente durch ein Semikolon („;") voneinander zu trennen und in der angegebenen Reihenfolge anzuführen: 1. Vollständiger rechtlicher Name des TPP bzw. des anderen Finanzunternehmens 2. Identifikationscode des TPP bzw. des anderen Finanzunternehmens (LEI oder EUID) 3. Art des Identifikationscodes (LEI oder EUID) 4. Sonstige als relevant erachtete Informationen **Beispiel bei Ursprung des Vorfalls bei einem TPP oder einem anderen Finanzunternehmen:** *PROVIDER REGISTERED LEGAL NAME;[LEI CODE];LEI;"public statement issued by provider on xxx"*

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
				Beispiel, wenn der Vorfall nicht von einem TPP oder einem anderen Finanzunternehmen ausgeht: *Feld 2.8 ist **leer** zu lassen.* Quelle: Operational Instructions der ESAs (ID 9, Seite 4).
8	Klassifizierungsschwellen nicht erreicht - Einbringung einer Reklassifizierungsmeldung	2.10	Meldungen werden eingebracht, obwohl die Klassifizierungs-schwellen nicht erreicht werden.	In diesem Fall ist **verpflichtend eine Reklassifizierungsmeldung** einzubringen und der Vorfall **als nicht schwerwiegend einzustufen**. Im Tabellenblatt Erstmeldung („initial notification") ist **Feld 2.10 verpflichtend auszufüllen** und mit einer **Begründung für die vorgenommene Reklassifizierung** zu versehen.
9	Angaben für betroffene Kunden, finanzielle Gegenparteien & Transaktionen	3.4 bis 3.11	Unrealistische Werte & Feld 3.11 wird nicht in Tausend EUR angegeben	Erklärungen zu den einzelnen Feldern: - **3.4 Anzahl betroffener Kunden** Anzahl **aller betroffenen Kunden** (natürliche oder juristische Personen), **die den betroffenen Dienst während des Vorfalls nicht nutzen konnten** oder anderweitig negativ betroffen waren. Kann die tatsächliche Zahl nicht bestimmt werden, sind Schätzungen auf Basis verfügbarer Vergleichsdaten zulässig. Einzubeziehen sind auch vertraglich erfasste Dritte sowie Begünstigte des betroffenen Dienstes. - **3.5 Prozentsatz betroffener Kunden** Anteil der **betroffenen Kunden** im **Verhältnis zur Gesamtzahl der Kunden**, die den jeweiligen Dienst nutzen (könnten). Falls erforderlich, sind Schätzungen anzustellen. - **3.6 Anzahl betroffener finanzieller Gegenparteien**

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
				Anzahl der finanziellen Gegenparteien mit Vertragsbeziehung zum Finanzunternehmen, die vom **Vorfall betroffen** sind. Ist eine exakte Ermittlung nicht möglich, sind Schätzwerte auf Basis vorhandener Referenzdaten zu verwenden. - **3.7 Prozentsatz betroffener finanzieller Gegenparteien** **Anteil** der betroffenen finanziellen Gegenparteien im Verhältnis zur Gesamtzahl der vertraglich gebundenen finanziellen Gegenparteien. Schätzungen sind zulässig, wenn exakte Daten fehlen. - **3.8 Auswirkungen auf relevante Kunden oder finanzielle Gegenparteien** Qualitative Beschreibung identifizierter Auswirkungen auf relevante Kunden oder finanzielle Gegenparteien gemäß den einschlägigen Kriterien des RTS zu Klassifizierungskriterien. - **3.9 Anzahl betroffener Transaktionen** **Anzahl** der durch den IKT-Vorfall beeinträchtigten Transaktionen, einschließlich inländischer und grenzüberschreitender Transaktionen mit Bezug zur Union. Bei fehlenden genauen Daten sind Schätzungen zulässig. - **3.10 Prozentsatz betroffener Transaktionen** **Anteil der betroffenen Transaktionen** im Verhältnis zur durchschnittlichen täglichen Anzahl der vom betroffenen Dienst abgewickelten Transaktionen. Auch hier können **Schätzungen** verwendet werden. - **3.11 Wert der betroffenen Transaktionen** Gesamter monetärer Wert der vom Vorfall betroffenen Transaktionen. **Angabe in Tausendereinheiten der in Feld 1.15 angegebenen Währung**. Der Betrag ist **als positiver Geldwert** anzugeben; bei fehlender Genauigkeit sind Schätzungen auf Basis verfügbarer Vergleichsdaten zulässig.

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
10	Angabe monetärer Werte	3.11, 4.13, 4.14	Inkonsistente Angaben bei monetären Werten (Tausendereinheiten)	Der ITS zu Standardformularen, Vorlagen und Verfahren schreibt vor, dass der Datenpunkt in Einheiten mit einer Mindestgenauigkeit entsprechend Tausendereinheiten zu melden ist. Dementsprechend haben meldende Unternehmen sicherzustellen, dass **alle als monetär gekennzeichneten Felder**, namentlich **Feld 3.11, Feld 4.13 und Feld 4.14**, **ausschließlich in Tausendereinheiten** gemeldet werden. Darüber hinaus sind **alle in diesen Feldern angegebenen monetären Beträge in derselben Währung** auszuweisen wie jene, die in **Feld 1.15** angegeben ist. Quelle: **Operational Instructions der ESAs** (ID 2, Seite 2).
11	Auswirkungen auf die Reputation	3.13 & 3.14	Die Felder 3.13 und 3.14 werden beinahe immer befüllt.	Die Felder 3.13 und 3.14 sind nur dann zu befüllen, wenn „*Reputational impact*“ im Feld 2.5 als für die Meldung einschlägiges Klassifizierungskriterium angegeben wurde. Stellt sich nachträglich heraus, dass ein Reputationsschaden im Sinne des Artikel 2 des RTS zu Klassifizierungskriterien gegeben ist, muss das entsprechende Kriterium **„Reputational impact“** auch in **Feld 2.5** berücksichtigt werden.
12	Dauer und Ausfallzeiten	3.15 & 3.16	Derzeit scheint nicht vollständig klar, welche Angaben zur Dauer des Vorfalls vorzunehmen sind.	Die Wesentlichkeitsschwelle für das Klassifizierungskriterium **„Duration and Service Downtime“** gilt als erreicht, wenn mindestens eine der folgenden Bedingungen erfüllt ist: • der IKT-bezogene Vorfall dauert **länger als 24 Stunden** (Feld 3.15), oder • die **Ausfallzeit von IKT-Diensten zur Unterstützung kritischer oder wichtiger Funktionen** beträgt **mehr als zwei Stunden** (Feld 3.16). **Feld 3.15 („Duration“)** ist stets anzugeben und bezeichnet den Zeitraum vom Beginn eines schwerwiegenden IKT-bezogenen Vorfalls bis zu dessen vollständiger Behebung.

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
				Feld 3.16 („Service Downtime“) bezeichnet den Zeitraum der vollständigen oder teilweisen Nichtverfügbarkeit eines Dienstes. Hatte der Vorfall keine Auswirkungen auf die Ausfallzeit (*Service Downtime*), kann Feld 3.16 freigelassen werden. Das Feld ist im Format **DD:HH:MM** auszufüllen.
13	Voraussetzungen für die Meldung von Feld 3.17 “*Information on whether the numbers for duration and service downtime are actual or estimates”*	3.17	Feld 3.17 ist für Zwischen- und Abschlussmeldungen als verpflichtend definiert, sofern das Kriterium „*Duration and service downtime*“ erfüllt ist.	**Feld 3.17** gibt an, ob die in **Feld 3.15 („Duration“)** und **Feld 3.16 („Service Downtime“)** gemeldeten Werte tatsächliche Werte oder Schätzungen sind. Da die Angabe von **Feld 3.15 („Duration“)** sowohl in Zwischenmeldungen als auch in Abschlussmeldungen verpflichtend ist, wird erwartet, dass auch **Feld 3.17** in Zwischen- und Abschlussmeldungen ausgefüllt wird und nicht nur dann, wenn das Kriterium **„Duration and Service Downtime“** in **Feld 2.5** als maßgebliches Klassifizierungskriterium gemeldet wird. Dadurch wird sichergestellt, dass die gemeldete Dauer des Vorfalls korrekt interpretiert werden kann. Quelle: **Operational Instructions der ESAs** (ID 10, Seite 4).
14	Ausführungen zum verpflichtenden Kriterium “Critical services affected“	3.22	Feld wird nicht richtig befüllt.	Das Kriterium **„Critical services affected“** ist bei **jeder Vorfallsmeldung verpflichtend anzugeben** (Artikel 8 iVm Artikel 6 der RTS zu den Klassifizierungskriterien) und daher **immer in Feld 2.5** zu erfassen. Siehe bereits oben. Zusätzlich sind in **Feld 3.22 nachvollziehbare und konkrete Angaben** zu machen, **aus welchen Gründen** das Kriterium „Critical services affected“ erfüllt ist. Dabei ist wie folgt vorzugehen: **1. Auswahl der einschlägigen Litera** Es ist anzugeben, **welche der folgenden Litera zutrifft**:

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
				a) Beeinträchtigung von IKT-Diensten oder Netzwerk- und Informationssystemen, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen oder unterstützt haben; b) Beeinträchtigung von Finanzdienstleistungen des Finanzunternehmens, die einer Zulassung oder Registrierung bedürfen oder von den zuständigen Behörden beaufsichtigt werden; c) Erfolgreicher, böswilliger und unbefugter Zugriff auf die Netzwerk- und Informationssysteme des Finanzunternehmens. **2. Konkrete Begründung** Zusätzlich ist **konkret darzulegen**, warum die ausgewählte Litera zutrifft, insbesondere: bei **Lit. a)**: Welche IKT-Dienste oder Systeme waren betroffen? bei **Lit. b)**: Welche konkrete Finanzdienstleistung war beeinträchtigt? bei **Lit. c)**: Lag ein erfolgreicher, böswilliger und unbefugter Zugriff vor? Falls ja, auf welche Systeme bzw. Daten erstreckte sich dieser Zugriff?
15	*Type* of the major ICT-related incident und *High-level classification* of root causes of the incident	3.23 & 4.1	*Type of the major ICT-related incident* (Feld 3.23) und *High-level classification of root causes of the incident* (Feld 4.1) - plausibler Zusammenhang zwischen Vorfall und Ursache	**Feld 3.23 „Type of major ICT-related incident“** und **Feld 4.1 „High-level classification of root causes“** betrachten einen schwerwiegenden IKT-bezogenen Vorfall aus unterschiedlichen Perspektiven. Während **Feld 3.23** die Art bzw. Erscheinungsform des Vorfalls beschreibt und damit die Frage beantwortet, *welcher Vorfall eingetreten ist*, dient **Feld 4.1** der Klassifizierung der zugrunde liegenden Ursache und beantwortet die Frage, *warum der Vorfall eingetreten ist*. Eine formale Übereinstimmung der Angaben in den beiden Feldern ist daher nicht erforderlich. Entscheidend ist vielmehr, dass zwischen dem gemeldeten Incident Type und Root Cause ein sachlich plausibler und nachvollziehbarer Zusammenhang besteht. Die Beurteilung dieses Zusammenhangs sollte insbesondere anhand der in **Feld 4.5** dargestellten Ereignis- und Ursachenkette sowie der in **Feld 4.6** beschriebenen Maßnahmen und Kontrollen erfolgen.

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
16	Abweichende Wortlaute zwischen Beschreibung und Auswahlliste	3.25	Unterschiedliche Wortlaute in der **Beschreibung** gegenüber der **Auswahlliste (Field Type list)** für eine der vordefinierten Optionen in Feld 3.25.	Der ITS zu Standardformularen, Vorlagen und Verfahren enthält für eine der vordefinierten Optionen in Feld 3.25 zwei widersprüchliche Formulierungen: - **Beschreibung:** *"(f) data exfiltration and manipulation, <u>excluding</u> identity theft;"* - **Auswahlliste:** *"– Data exfiltration and manipulation, <u>including</u> identity theft"* Für die Befüllung von **Feld 3.25** ist der in der **Beschreibung** angeführte Wortlaut, nämlich **„***data exfiltration and manipulation, <u>excluding</u> identity theft***"**, als maßgeblich heranzuziehen. Der Auswahllisteneintrag ist aktuell irrtümlich im Template falsch bezeichnet. Bis dieses Template seitens der ESAs ausgetauscht wird, ist das entsprechende Auswahlfeld als „*<u>excluding</u> identity theft*" zu verstehen, zumal „identity theft" als eigene Auswahloption vorgesehen ist (und nicht wie angegeben „*<u>including</u> identity theft*"). Quelle: **Operational Instructions der ESAs** (ID 11, Seite 4 f).
17	Informationen für die Abwicklungs-behörde	4.10	Bei einigen Meldungen wurden **Feld 4.10 und Feld 4.11 ausgefüllt, obwohl sie nicht anwendbar sind** (z. B. mit Angaben wie „none", „not applicable" usw.).	Dieses Feld darf **NUR** ausgefüllt werden, wenn festgestellt wurde, dass **der Vorfall ein Risiko für kritische Funktionen von Finanzunternehmen im Sinne des Artikels 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellt** (wie in im ITS zu Standardformularen, Vorlagen und Verfahren definiert). Ergibt die Bewertung, dass der Vorfall kein solches Risiko darstellt, oder sind die Informationen für das betroffene Finanzunternehmen nicht einschlägig, **ist dieses Feld leer zu lassen**. Quelle: **Operational Instructions der ESAs** (ID 12, Seite 5).
18	Informationen für die Abwicklungs-behörde	4.11	Bei einigen Meldungen sind **Feld 4.10 und Feld 4.11 ausgefüllt, obwohl sie nicht**	Dieses Feld darf **NUR** ausgefüllt werden, wenn festgestellt wurde, dass **der Vorfall die Abwicklungsfähigkeit („Resolvability") des Unternehmens oder der Gruppe beeinträchtigt hat**. Ergibt die Bewertung, dass der Vorfall die Abwicklungsfähigkeit nicht beeinträchtigt hat oder die

	Beschreibung	Relevante Felder	Beobachtung	Erwartungshaltung
			anwendbar sind (z. B. mit Angaben wie „none“, „not applicable“ usw.).	Informationen für das betroffene Finanzunternehmen nicht einschlägig sind, **ist dieses Feld leer zu lassen**. Quelle: **Operational Instructions der ESAs** (ID 13, Seite 5).