2025/302

20.2.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/302

ze dne 23. října 2024,

kterým se stanoví prováděcí technické normy pro uplatňování nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o standardní formuláře, vzory a postupy pro hlášení závažného incidentu souvisejícího s IKT a oznamování významné kybernetické hrozby finančními orgány

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 ([1]), a zejména na čl. 20 čtvrtý pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Aby bylo zajištěno, že finanční subjekty budou závažné incidenty hlásit svým příslušným orgánům jednotným způsobem a že těmto orgánům budou poskytovat kvalitní údaje, je vhodné upřesnit, která datová pole musí finanční subjekty v různých fázích hlášení podle čl. 19 odst. 4 nařízení (EU) 2022/2554 poskytnout. Je důležité, aby tyto informace byly předkládány způsobem umožňujícím jednotný přehled o incidentu. Z tohoto důvodu je nezbytné stanovit pro tyto účely jednotný vzor hlášení.

(2) Finanční subjekty by měly vyplnit ta datová pole vzoru hlášení, která odpovídají požadavkům na informace týkajícím se příslušného oznámení nebo zprávy. Pokud ovšem již mají k dispozici informace, které mají být poskytnuty v pozdější fázi hlášení, tj. v průběžné nebo závěrečné zprávě, měly by mít možnost předložit tyto údaje předem.

(3) Vzhledem k tomu, že vícenásobné nebo opakující se incidenty mohou představovat závažný incident podle článku 8 nařízení Komise v přenesené pravomoci (EU) 2024/1772 ([2]), měla by podoba vzoru hlášení a datových polí finančním subjektům umožňovat hlášení těchto opakujících se incidentů.

(4) V zájmu zajištění přesných a aktuálních informací by vzor hlášení měl finančním subjektům umožňovat, aby při předkládání průběžné a závěrečné zprávy veškeré dříve předložené informace aktualizovaly a v případě potřeby překlasifikovaly závažné incidenty na méně závažné.

(5) Právní identifikace subjektů by měla být v souladu s identifikátory uvedenými v prováděcích technických normách přijatých podle čl. 28 odst. 9 nařízení (EU) 2022/2554.

(6) Pokud finanční subjekty zadají zajištění povinného hlášení závažných incidentů souvisejících s IKT třetí straně, měly by příslušné orgány znát totožnost této třetí strany, která hlášení jménem finančního subjektu podává, ještě před předložením prvního oznámení nebo hlášení, aby mohly ověřit její oprávněnost.

([1]) Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Nařízení Komise v přenesené pravomoci (EU) 2024/1772 ze dne 13. března 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, v nichž jsou upřesněna kritéria klasifikace incidentů souvisejících s IKT a kybernetických hrozeb, stanoveny prahové hodnoty významnosti a upřesněny údaje v hlášeních závažných incidentů (Úř. věst. L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) V zájmu snadného zjištění dopadu incidentu, k němuž došlo u poskytovatele z řad třetích stran nebo který byl způsoben poskytovatelem z řad třetích stran a dotýká se více finančních subjektů v rámci jednoho členského státu, a za účelem snížení náročnosti hlášení pro finanční subjekty by vzor hlášení měl umožňovat předložení souhrnného hlášení obsahujícího souhrnné informace o dopadu incidentu na všechny dotčené finanční subjekty, které daný incident klasifikovaly jako závažný.

(8) Vzor hlášení by měl být navržen technologicky neutrálním způsobem, aby se dal implementovat do různých řešení hlášení incidentů, která již existují nebo která mohou být pro účely provádění požadavků nařízení (EU) 2022/2554 vytvořena.

(9) Podoba vzoru hlášení a datových polí by měla usnadnit hlášení závažných incidentů souvisejících s IKT třetími stranami, jimž finanční subjekty zadaly zajištění povinného hlášení závažných incidentů souvisejících s IKT v souladu s čl. 19 odst. 5 nařízení (EU) 2022/2554.

(10) Toto nařízení vychází z návrhu prováděcích technických norem, které Komisi předložily evropské orgány dohledu.

(11) O návrhu prováděcích technických norem, z něhož toto nařízení vychází, vedly evropské orgány dohledu otevřené veřejné konzultace, analyzovaly potenciální související náklady a přínosy a požádaly o stanovisko skupinu subjektů působících v bankovnictví zřízenou podle článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([3]), (EU) č. 1094/2010 ([4]) a (EU) č. 1095/2010 ([5]).

(12) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal kladné stanovisko dne 22. července 2024. Jakékoli zpracování osobních údajů v oblasti působnosti tohoto nařízení by mělo být prováděno v souladu s platnými zásadami ochrany údajů a s ustanoveními nařízení (EU) 2018/1725,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Vzor pro hlášení závažných incidentů souvisejících s IKT

1. Finanční subjekty použijí k předložení prvotního oznámení, průběžné zprávy a závěrečné zprávy podle čl. 19 odst. 4 nařízení (EU) 2022/2554 vzor uvedený v příloze I, a to následovně:

a) finanční subjekty, které předkládají prvotní oznámení, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 2 nařízení Komise v přenesené pravomoci (EU) 2025/301 ([7]), a pokud již mají příslušné informace, mohou vyplnit datová pole, jejichž vyplnění se pro účely prvotního oznámení nevyžaduje, ale vyžaduje se pro účely průběžné nebo závěrečné zprávy;

([3]) Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES (Úř. věst. L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Nařízení Komise v přenesené pravomoci (EU) 2025/301 ze dne 23. října 2024, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, jež stanoví obsah a lhůty pro prvotní oznámení a průběžnou a závěrečnou zprávu o závažných incidentech souvisejících s IKT a obsah dobrovolného oznámení o významných kybernetických hrozbách (Úř. věst. L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) finanční subjekty, které předkládají průběžnou zprávu, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 3 nařízení v přenesené pravomoci (EU) 2025/301, a pokud již mají příslušné informace, mohou vyplnit datová pole, jejichž vyplnění se pro účely průběžné zprávy nevyžaduje, ale vyžaduje se pro účely závěrečné zprávy;

c) finanční subjekty, které předkládají závěrečnou zprávu, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 4 nařízení v přenesené pravomoci (EU) 2025/301

2. Finanční subjekty zajistí, aby informace obsažené v prvotním oznámení a v průběžné a závěrečné zprávě byly úplné a přesné.

3. V případě, že v době podávání prvotního oznámení nebo průběžné zprávy nejsou k dispozici přesné údaje, uvedou finanční subjekty pokud možno odhadované hodnoty vycházející z jiných dostupných údajů a informací.

4. Při předkládání průběžné nebo závěrečné zprávy použijí finanční subjekty vzor stanovený v příloze I k předložení všech požadovaných informací a k případné aktualizaci informací poskytnutých předtím v prvotním oznámení nebo v průběžné zprávě.

5. Při vyplňování vzoru uvedeného v příloze I se finanční subjekty řídí datovým glosářem a pokyny uvedenými v příloze II.

Článek 2

Současné předkládání prvotního oznámení a průběžné a závěrečné zprávy

Finanční subjekty mohou předložení prvotního oznámení, průběžné zprávy a závěrečné zprávy spojit a podat dvě nebo všechny tyto zprávy současně, pokud již došlo k obnovení běžných činností nebo byla dokončena analýza hlavních příčin a pokud jsou dodrženy lhůty stanovené v článku 5 nařízení v přenesené pravomoci (EU) 2025/301

Článek 3

Opakující se incidenty související s IKT

Finanční subjekty, které poskytují informace o opakujících se méně závažných incidentech souvisejících s IKT, jež kumulativně splňují podmínky pro jeden závažný incident související s IKT podle čl. 8 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1772, poskytnou tyto informace v souhrnné podobě.

Článek 4

Používání zabezpečených elektronických kanálů

1. Finanční subjekty použijí k předložení prvotního oznámení a průběžné a závěrečné zprávy zabezpečené elektronické kanály, které jim poskytne příslušný orgán.

2. Finanční subjekty, které nemohou použít zabezpečené elektronické kanály poskytnuté příslušným orgánem, informují svůj příslušný orgán o závažném incidentu souvisejícím s IKT jinými bezpečnými způsoby, na nichž se s příslušným orgánem dohodnou. Pokud to příslušný orgán požaduje, finanční subjekty znovu předloží prvotní oznámení nebo průběžnou či závěrečnou zprávu prostřednictvím zabezpečeného elektronického kanálu poskytnutého příslušným orgánem, jakmile tak mohou učinit.

Článek 5

Překlasifikování závažných incidentů souvisejících s IKT

Pokud finanční subjekt po dalším posouzení dojde k závěru, že incident související s IKT, který byl předtím hlášen jako závažný, v žádném okamžiku nesplnil klasifikační kritéria a prahové hodnoty stanovené v článku 8 nařízení v přenesené pravomoci (EU) 2024/1772, oznámí příslušnému orgánu, že daný incident související s IKT překlasifikoval ze závažného na méně závažný, a to poskytnutím informací o tomto překlasifikování ve vzoru stanoveném v příloze II tohoto nařízení, pokud jde o pole „Druh předkládaného dokumentu" a „Jiné relevantní informace".

Článek 6

Oznámení o externím zajištění povinného hlášení

1. Finanční subjekty, které v souladu s čl. 19 odst. 5 nařízení (EU) 2022/2554 zadají zajištění povinného hlášení závažných incidentů souvisejících s IKT externě, uvědomí svůj příslušný orgán o této dohodě o externím zajištění, jakmile ji uzavřou, nejpozději však před podáním prvního oznámení nebo zprávy.

2. Finanční subjekty poskytnou příslušnému orgánu jméno, kontaktní údaje a identifikační kód třetí strany, která za ně bude oznámení nebo zprávy o závažných incidentech souvisejících s IKT předkládat.

3. Finanční subjekty informují svůj příslušný orgán, jakmile povinné hlášení přestanou mít zajištěno externě podle čl. 19 odst. 5 nařízení (EU) 2022/2554.

Článek 7

Souhrnné hlášení

1. Poskytovatel služeb z řad třetích stran, který externě zajišťuje povinné hlášení podle čl. 19 odst. 5 nařízení (EU) 2022/2554, může použít vzor uvedený v příloze I tohoto nařízení k poskytnutí souhrnných informací o závažném incidentu souvisejícím s IKT, který má dopad na více finančních subjektů, v rámci jediného oznámení nebo zprávy, jež předloží příslušnému orgánu jménem všech dotčených finančních subjektů, pokud jsou splněny všechny tyto podmínky:

a) závažný incident související s IKT, který má být hlášen, vznikl u poskytovatele služeb IKT z řad třetích stran nebo je jím způsoben;

b) tento poskytovatel služeb z řad třetích stran poskytuje příslušné služby IKT více než jednomu finančnímu subjektu nebo skupině;

c) každý finanční subjekt, jehož se souhrnné oznámení nebo zpráva týká, klasifikuje incident související s IKT jako závažný;

d) závažný incident související s IKT se dotýká finančních subjektů v rámci jediného členského státu a souhrnné hlášení se týká finančních subjektů, nad nimiž vykonává dohled stejný příslušný orgán;

e) příslušné orgány tomuto druhu finančních subjektů výslovně povolily podávání souhrnného hlášení.

2. Odstavec 1 se nevztahuje na úvěrové instituce, jež se považují za významné podle čl. 2 bodu 16 nařízení (EU) Evropské centrální banky č. 468/2014 ([8]), provozovatele obchodních systémů a ústřední protistrany, které použijí vzor uvedený v příloze I pouze k individuálnímu předkládání oznámení nebo zpráv o závažných incidentech souvisejících s IKT příslušnému orgánu.

3. Pokud příslušné orgány požadují informace o individuálním dopadu závažného incidentu souvisejícího s IKT na jednotlivý finanční subjekt, předloží tento finanční subjekt na žádost příslušného orgánu individuální oznámení nebo zprávu o závažném incidentu souvisejícím s IKT.

([8]) Nařízení Evropské centrální banky (EU) č. 468/2014 ze dne 16. dubna 2014, kterým se stanoví rámec spolupráce Evropské centrální banky s vnitrostátními příslušnými orgány a vnitrostátními pověřenými orgány v rámci jednotného mechanismu dohledu (nařízení o rámci jednotného mechanismu dohledu) (ECB/2014/17) (Úř. věst. L 141, 14.5.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Článek 8

Oznámení o významných kybernetických hrozbách

1. Finanční subjekty, které oznamují příslušným orgánům významné kybernetické hrozby v souladu s čl. 19 odst. 2 nařízení (EU) 2022/2554, použijí vzor stanovený v příloze III tohoto nařízení a řídí se datovým glosářem a pokyny uvedenými v příloze IV tohoto nařízení.

2. Finanční subjekty zajistí, aby informace obsažené v oznámení o významných kybernetických hrozbách byly úplné a přesné.

Článek 9

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 23. října 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

Vzory pro hlášení závažných incidentů

Číslo pole	Datové pole	
Obecné informace o finančním subjektu		
1.1	Druh předkládaného dokumentu	
1.2	Název subjektu, který zprávu předkládá	
1.3	Identifikační kód subjektu předkládajícího zprávu	
1.4	Druh dotčeného finančního subjektu	
1.5	Název dotčeného finančního subjektu	
1.6	Kód LEI dotčeného finančního subjektu	
1.7	Jméno hlavní kontaktní osoby	
1.8	E-mail hlavní kontaktní osoby	
1.9	Telefon hlavní kontaktní osoby	
1.10	Jméno druhé kontaktní osoby	
1.11	E-mail druhé kontaktní osoby	
1.12	Telefon druhé kontaktní osoby	
1.13	Název nejvyšší mateřské společnosti	
1.14	Kód LEI nejvyšší mateřské společnosti	
1.15	Měna hlášení	
Obsah prvotního oznámení		
2.1	Referenční kód incidentu přidělený finančním subjektem	
2.2	Datum a čas zjištění závažného incidentu souvisejícího s IKT	
2.3	Datum a čas klasifikace incidentu souvisejícího s IKT jako závažného	
2.4	Popis závažného incidentu souvisejícího s IKT	
2.5	Klasifikační kritéria, na jejichž základě je incident hlášen	
2.6	Prahy významnosti pro klasifikační kritérium „Územní rozsah“	
2.7	Odhalení závažného incidentu souvisejícího s IKT	

Číslo pole	Datové pole	
2.8	Údaj o tom, zda závažný incident související s IKT pochází od poskytovatele z řad třetích stran nebo od jiného finančního subjektu	
2.9	Aktivace plánu zachování provozu, pokud byl aktivován	
2.10	Jiné relevantní informace	
Obsah průběžné zprávy		
3.1	Referenční kód incidentu poskytnutý příslušným orgánem	
3.2	Datum a čas výskytu závažného incidentu souvisejícího s IKT	
3.3	Datum a čas obnovení služeb, činností nebo operací	
3.4	Počet dotčených klientů	
3.5	Procento dotčených klientů	
3.6	Počet dotčených finančních protistran	
3.7	Procento dotčených finančních protistran	
3.8	Dopad na příslušné klienty nebo finanční protistrany	
3.9	Počet dotčených transakcí	
3.10	Procento dotčených transakcí	
3.11	Hodnota dotčených transakcí	
3.12	Informace o tom, zda se jedná o skutečná čísla nebo odhady, nebo zda nedošlo k žádnému dopadu	
3.13	Poškození dobré pověsti	
3.14	Informace o souvislostech poškození dobré pověsti	
3.15	Doba trvání závažného incidentu souvisejícího s IKT	
3.16	Doba odstávky služby	
3.17	Informace o tom, zda údaje o době trvání a době odstávky služby jsou skutečné nebo odhadované	
3.18	Druhy dopadu v členských státech	
3.19	Popis dopadu závažného incidentu souvisejícího s IKT v jiných členských státech	
3.20	Prahy významnosti pro klasifikační kritérium „Ztráty údajů“	
3.21	Popis ztrát údajů	

Číslo pole	Datové pole	
3.22	Klasifikační kritérium „Dotčené významné služby“	
3.23	Druh závažného incidentu souvisejícího s IKT	
3.24	Jiné druhy incidentů	
3.25	Hrozby a techniky použité aktérem hrozby	
3.26	Jiné druhy technik	
3.27	Informace o dotčených funkčních oblastech a obchodních procesech	
3.28	Dotčené součásti infrastruktury podporující obchodní procesy	
3.29	Informace o dotčených součástech infrastruktury podporujících obchodní procesy	
3.30	Dopad na finanční zájmy klientů	
3.31	Hlášení podávaná jiným orgánům	
3.32	Upřesnění „jiných“ orgánů	
3.33	Dočasná opatření přijatá nebo plánovaná k překonání účinků incidentu	
3.34	Popis všech dočasných opatření přijatých nebo plánovaných k překonání účinků incidentu	
3.35	Ukazatele narušení	
Obsah závěrečné zprávy		
4.1	Vysokoúrovňová klasifikace hlavních příčin incidentu	
4.2	Podrobná klasifikace hlavních příčin incidentu	
4.3	Další klasifikace hlavních příčin incidentu	
4.4	Jiné druhy hlavních příčin	
4.5	Informace o hlavních příčinách incidentu	
4.6	Stručný popis řešení incidentu	
4.7	Datum a čas odstranění hlavní příčiny incidentu	
4.8	Datum a čas vyřešení incidentu	
4.9	Informace o tom, zda se datum trvalého vyřešení incidentu liší od původně plánovaného data provedení	
4.10	Posouzení rizika pro zásadní funkce pro účely řešení krize	
4.11	Informace relevantní pro orgány příslušné k řešení krize	

Číslo pole	Datové pole	
4.12	Práh významnosti pro klasifikační kritérium „Ekonomický dopad“	
4.13	Výše hrubých přímých a nepřímých nákladů a ztrát	
4.14	Výše zpětně získaných finančních prostředků	
4.15	Informace o tom, zda se méně závažné incidenty opakují	
4.16	Datum a čas výskytu opakujících se incidentů	

PŘÍLOHA II

Datový glosář a pokyny pro hlášení závažných incidentů

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
Obecné informace o finančním subjektu						
1.1	Druh předkládaného dokumentu	Uveďte druh oznámení nebo zprávy o incidentu, který se příslušnému orgánu předkládá.	Ano	Ano	Ano	Výběr z možností: — prvotní oznámení — průběžná zpráva — závěrečná zpráva — závažný incident překlasifikován na méně závažný
1.2	Název subjektu, který zprávu předkládá	Úplný právní název subjektu, který hlášení předkládá.	Ano	Ano	Ano	Alfanumerické
1.3	Identifikační kód subjektu předkládajícího zprávu	Identifikační kód subjektu, který zprávu předkládá. Pokud oznámení/zprávu předkládají finanční subjekty, identifikačním kódem je identifikační kód právnické osoby (LEI), což je jedinečný 20místný alfanumerický kód podle normy ISO 17442-1:2020. Poskytovatel z řad třetích stran, který předkládá hlášení za finanční subjekt, může použít identifikační kód uvedený v prováděcích technických normách přijatých podle čl. 28 odst. 9 nařízení (EU) 2022/2554.	Ano	Ano	Ano	Alfanumerické
1.4	Druh dotčeného finančního subjektu	Druh subjektu, za který se hlášení předkládá, podle čl. 2 odst. 1 písm. a) až t) nařízení (EU) 2022/2554. V případě souhrnného hlášení podle článku 7 tohoto nařízení je třeba vybrat jednotlivé druhy finančních subjektů, které jsou do souhrnného hlášení zahrnuty.	Ano	Ano	Ano	Výběr z možností (lze zvolit více možností): — úvěrová instituce, — platební instituce, — vyňatá platební instituce, — poskytovatel služeb informování o účtu, — instituce elektronických peněz, — vyňatá instituce elektronických peněz, — investiční podnik, — poskytovatel služeb souvisejících s kryptoaktivy, — vydavatel tokenů vázaných na aktiva, — centrální depozitář cenných papírů, — ústřední protistrana, — obchodní systém, — registr obchodních údajů,

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
						— správce alternativního investičního fondu, — správcovská společnost, — poskytovatel služeb hlášení údajů, — pojišťovna a zajišťovna, — zprostředkovatel pojištění, zprostředkovatel zajištění a zprostředkovatel doplňkového pojištění, — instituce zaměstnaneckého penzijního pojištění, — ratingová agentura, — správce kritických referenčních hodnot, — poskytovatel služeb skupinového financování, — registr sekuritizací.
1.5	Název dotčeného finančního subjektu	Úplný právní název finančního subjektu dotčeného závažným incidentem souvisejícím s IKT a povinného tento závažný incident hlásit příslušnému orgánu podle článku 19 nařízení (EU) 2022/2554. V případě souhrnného hlášení: a) seznam všech názvů finančních subjektů dotčených závažným incidentem souvisejícím s IKT, oddělených středníkem; b) poskytovatel z řad třetích stran, který předkládá oznámení nebo zprávu o závažném incidentu souhrnným způsobem podle článku 7 tohoto nařízení, uvede názvy všech finančních subjektů, kterých se incident dotýká, oddělené středníkem.	Ano, pokud je finanční subjekt, jehož se incident dotýká, odlišný od subjektu, který předkládá hlášení, a v případě souhrnného hlášení	Ano, pokud je finanční subjekt, jehož se incident dotýká, odlišný od subjektu, který předkládá hlášení, a v případě souhrnného hlášení	Ano, pokud je finanční subjekt, jehož se incident dotýká, odlišný od subjektu, který předkládá hlášení, a v případě souhrnného hlášení	Alfanumerické
1.6	Kód LEI dotčeného finančního subjektu	Identifikační kód právnické osoby (LEI) finančního subjektu, jehož se závažný incident související s IKT dotýká, přidělený podle Mezinárodní organizace pro normalizaci. V případě souhrnného hlášení: a) seznam všech kódů LEI finančních subjektů dotčených závažným incidentem souvisejícím s IKT, oddělených středníkem;	Ano, pokud je finanční subjekt, jehož se závažný incident související s IKT dotýká,	Ano, pokud je finanční subjekt, jehož se závažný incident související s IKT dotýká, odlišný od	Ano, pokud je finanční subjekt, jehož se závažný incident související s IKT dotýká,	Jedinečný 20místný alfanumerický kód podle normy ISO 17442-1:2020

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
		b) poskytovatel z řad třetích stran, který předkládá oznámení nebo zprávu o závažném incidentu souhrnným způsobem podle článku 7 tohoto nařízení, uvede kódy LEI všech finančních subjektů, kterých se incident dotýká, oddělené středníkem. Pořadí kódů LEI a názvů finančních subjektů musí být stejné.	odlišný od subjektu, který předkládá hlášení, a v případě souhrnného hlášení	subjektu, který předkládá hlášení, a v případě souhrnného hlášení	odlišný od subjektu, který předkládá hlášení, a v případě souhrnného hlášení	
1.7	Jméno hlavní kontaktní osoby	Jméno a příjmení hlavní kontaktní osoby finančního subjektu. V případě souhrnného hlášení podle článku 7 tohoto nařízení jméno hlavní kontaktní osoby v subjektu, který souhrnné hlášení předkládá.	Ano	Ano	Ano	Alfanumerické
1.8	E-mail hlavní kontaktní osoby	E-mailová adresa hlavní kontaktní osoby, kterou může příslušný orgán použít pro následnou komunikaci. V případě souhrnného hlášení podle článku 7 tohoto nařízení e-mailová adresa hlavní kontaktní osoby v subjektu, který souhrnné hlášení předkládá.	Ano	Ano	Ano	Alfanumerické
1.9	Telefon hlavní kontaktní osoby	Telefonní číslo hlavní kontaktní osoby, které může příslušný orgán použít pro následnou komunikaci. V případě souhrnného hlášení podle článku 7 tohoto nařízení telefonní číslo hlavní kontaktní osoby v subjektu, který souhrnné hlášení předkládá. Telefonní číslo se uvádí se všemi mezinárodními předvolbami (např. +33XXXXXXXXX).	Ano	Ano	Ano	Alfanumerické
1.10	Jméno druhé kontaktní osoby	Jméno a příjmení druhé kontaktní osoby nebo jméno odpovědného týmu finančního subjektu nebo subjektu, který předkládá hlášení jménem finančního subjektu.	Ano	Ano	Ano	Alfanumerické
1.11	E-mail druhé kontaktní osoby	E-mailová adresa druhé kontaktní osoby nebo funkční e-mailová adresa týmu, kterou může příslušný orgán použít pro následnou komunikaci.	Ano	Ano	Ano	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
1.12	Telefon druhé kontaktní osoby	Telefonní číslo druhé kontaktní osoby nebo týmu, které může příslušný orgán použít pro následnou komunikaci. Telefonní číslo se uvádí se všemi mezinárodními předvolbami (např. +33XXXXXXXXX).	Ano	Ano	Ano	Alfanumerické
1.13	Název nejvyšší mateřské společnosti	Případný název nejvyšší mateřské společnosti skupiny, do které dotčený finanční subjekt patří.	Ano, pokud finanční subjekt patří do skupiny	Ano, pokud finanční subjekt patří do skupiny	Ano, pokud finanční subjekt patří do skupiny	Alfanumerické
1.14	Kód LEI nejvyšší mateřské společnosti	Případný kód LEI nejvyšší mateřské společnosti skupiny, do které dotčený finanční subjekt patří, přidělený podle Mezinárodní organizace pro normalizaci.	Ano, pokud finanční subjekt patří do skupiny	Ano, pokud finanční subjekt patří do skupiny	Ano, pokud finanční subjekt patří do skupiny	Jedinečný 20místný alfanumerický kód podle normy ISO 17442-1:2020
1.15	Měna hlášení	Měna použitá pro hlášení incidentu.	Ano	Ano	Ano	Zde se uvede kód měny podle normy ISO 4217.
Obsah prvotního oznámení						
2.1	Referenční kód incidentu přidělený finančním subjektem	Jedinečný referenční kód vydaný finančním subjektem, který jednoznačně identifikuje závažný incident související s IKT. V případě souhrnného hlášení podle článku 7 tohoto nařízení referenční kód incidentu přidělený poskytovatelem z řad třetích stran.	Ano	Ano	Ano	Alfanumerické
2.2	Datum a čas zjištění incidentu souvisejícího s IKT	Datum a čas, kdy se finanční subjekt o incidentu souvisejícím s IKT dozvěděl. U opakujících se incidentů datum a čas, kdy byl zjištěn poslední incident související s IKT.	Ano	Ano	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601(RRRR-MM-DD Thh: mm:ss)

	Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
2.3	Datum a čas klasifikace incidentu jako závažného	Datum a čas, kdy byl incident související s IKT klasifikován jako závažný podle klasifikačních kritérií stanovených v nařízení v přenesené pravomoci (EU) 2024/1772.	Ano	Ano	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601(RRRR-MM-DD Thh: mm:ss)
2.4	Popis incidentu souvisejícího s IKT	Popis nejdůležitějších aspektů závažného incidentu souvisejícího s IKT. Finanční subjekty uvedou základní přehled informací, jako jsou možné příčiny, bezprostřední dopady, dotčené systémy a další informace. Pokud je znám nebo lze důvodně očekávat dopad incidentu na poskytovatele z řad třetích stran nebo jiné finanční subjekty, uvedou finanční subjekty druh poskytovatele nebo finančního subjektu, jeho název, příslušné identifikační kódy a typ identifikačního kódu (např. LEI nebo EUID). V následných zprávách se obsah tohoto pole může průběžně vyvíjet, aby odrážel aktuální poznatky o incidentu souvisejícím s IKT a popisoval další relevantní informace o incidentu souvisejícím s IKT, které v datových polích nejsou zachyceny, včetně interního posouzení závažnosti finančním subjektem (např. velmi nízká, nízká, střední, vysoká, velmi vysoká) a uvedení úrovně a názvu nejvyšších rozhodovacích struktur, které byly do reakce na incident související s IKT zapojeny.	Ano	Ano	Ano	Alfanumerické
2.5	Klasifikační kritéria, na jejichž základě je incident hlášen	Klasifikační kritéria podle nařízení v přenesené pravomoci (EU) 2024/1772, jež vedla k označení incidentu souvisejícího s IKT za závažný a k následnému oznámení a zprávám. V případě souhrnného hlášení podle článku 7 tohoto nařízení klasifikační kritéria, na jejichž základě byl incident související s IKT označen za závažný u nejméně jednoho z finančních subjektů.	Ano	Ano	Ano	Výběr z možností (lze zvolit více možností): — dotčení klienti, finanční protistrany a transakce, — dopad na dobrou pověst, — doba trvání incidentu a doba odstávky služby, — územní rozsah, — ztráty údajů, — dotčené významné služby, — ekonomický dopad.
2.6	Prahy významnosti pro klasifikační kritérium „Územní rozsah“	Členské státy EHP, které byly závažným incidentem souvisejícím s IKT dotčeny Při posuzování dopadu závažného incidentu souvisejícího s IKT v jiných členských státech přihlížejí finanční subjekty k článkům 4 a 12 nařízení v přenesené pravomoci (EU) 2024/1772.	Ano, pokud je splněna prahová hodnota pro „Územní rozsah“	Ano, pokud je splněna prahová hodnota pro „Územní rozsah“	Ano, pokud je splněna prahová hodnota pro „Územní rozsah“	Výběr z možností (lze zvolit více možností); uvede se pomocí dvoupísmenných kódů dotčených zemí podle normy ISO 3166

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
2.7	Odhalení závažného incidentu souvisejícího s IKT	Údaj o tom, jak byl závažný incident související s IKT odhalen.	Ano	Ano	Ano	Výběr z možností: — zabezpečení IT, — zaměstnanec, — interní audit, — externí audit, — klienti, — finanční protistrany, — poskytovatel z řad třetích stran, — útočník, — monitorovací systémy, — orgán / agentura / donucovací orgán, — jiná možnost.
2.8	Údaj o tom, zda incident pochází od poskytovatele z řad třetích stran nebo od jiného finančního subjektu	Údaj o tom, zda závažný incident související s IKT pochází od poskytovatele z řad třetích stran nebo od jiného finančního subjektu. Finanční subjekty uvedou, zda závažný incident související s IKT pochází od poskytovatele z řad třetích stran nebo od jiného finančního subjektu (včetně finančních subjektů patřících do téže skupiny jako subjekt podávající hlášení), a název a identifikační kód tohoto poskytovatele z řad třetích stran nebo finančního subjektu a druh identifikačního kódu (např. LEI nebo EUID).	Ano, pokud incident pochází od poskytovatele z řad třetích stran nebo jiného finančního subjektu	Ano, pokud incident pochází od poskytovatele z řad třetích stran nebo jiného finančního subjektu	Ano, pokud incident pochází od poskytovatele z řad třetích stran nebo jiného finančního subjektu	Alfanumerické
2.9	Aktivace plánu zachování provozu, pokud byl aktivován	Údaj o tom, zda došlo k formální aktivaci opatření k zachování provozu finančního subjektu.	Ano	Ano	Ano	Booleovské (ano nebo ne)
2.10	Jiné relevantní informace	Veškeré další informace, které nejsou zahrnuty ve vzoru. Finanční subjekty, které překlasifikovaly závažný incident související s IKT na méně závažný, popíšou důvody, proč incident související s IKT nesplňuje a ani se neočekává, že by splnil kritéria pro to, aby byl považován za závažný incident související s IKT.	Ano, pokud jsou k dispozici další informace, které nejsou	Ano, pokud jsou k dispozici další informace, které nejsou zahrnuty ve vzoru, nebo	Ano, pokud jsou k dispozici další informace, které nejsou	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
			zahrnuty ve vzoru, nebo pokud byl závažný incident související s IKT překlasifikován na méně závažný	pokud byl závažný incident související s IKT překlasifikován na méně závažný	zahrnuty ve vzoru, nebo pokud byl závažný incident související s IKT překlasifikován na méně závažný	
Obsah průběžné zprávy						
3.1	Referenční kód incidentu poskytnutý příslušným orgánem	Jedinečný referenční kód přidělený příslušným orgánem v okamžiku přijetí prvotního oznámení, který jednoznačně identifikuje závažný incident související s IKT.	Ne	Ano, pokud existuje	Ano, pokud existuje	Alfanumerické
3.2	Datum a čas výskytu incidentu	Datum a čas, kdy k závažnému incidentu souvisejícímu s IKT došlo, pokud se liší od okamžiku, kdy se finanční subjekt o závažném incidentu souvisejícím s IKT dozvěděl. U opakujících se závažných incidentů souvisejících s IKT datum a čas, kdy došlo k poslednímu závažnému incidentu souvisejícímu s IKT.	Ne	Ano	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601(RRRR-MM-DD Thh: mm:ss)
3.3	Datum a čas obnovení služeb, činností nebo operací	Informace o datu a čase obnovení služeb, činností nebo operací, které byly závažným incidentem souvisejícím s IKT dotčeny.	Ne	Ano, pokud bylo vyplněno datové pole 3.16 „Doba odstávky služby“	Ano, pokud bylo vyplněno datové pole 3.16 „Doba odstávky služby“	Koordinovaný světový čas (UTC) dle normy ISO 8601(RRRR-MM-DD Thh: mm:ss)
3.4	Počet dotčených klientů	Počet klientů dotčených závažným incidentem souvisejícím s IKT, kteří využívají služby poskytované finančním subjektem. Při posuzování počtu dotčených klientů přihlížejí finanční subjekty k čl. 1 odst. 1 a čl. 9 odst. 1 písm. b) nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečný počet dotčených klientů, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. V případě souhrnného hlášení podle článku 7 tohoto nařízení celkový počet dotčených klientů ve všech finančních subjektech.	Ne	Ano	Ano	Numerické celočíselné

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.5	Procento dotčených klientů	Procentní podíl klientů dotčených závažným incidentem souvisejícím s IKT ve vztahu k celkovému počtu klientů, kteří dotčenou službu poskytovanou finančním subjektem využívají. V případě více dotčených služeb se služby uvedou souhrnně. Finanční subjekty při posuzování přihlížejí k čl. 1 odst. 1 a čl. 9 odst. 1 písm. a) nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečné procento dotčených klientů, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. V případě souhrnného hlášení podle článku 7 tohoto nařízení finanční subjekt vydělí součet všech dotčených klientů celkovým počtem klientů všech dotčených finančních subjektů.	Ne	Ano	Ano	Vyjádřeno v procentech – jakákoli hodnota o nejvýše pěti číselných znacích včetně nejvýše jednoho desetinného místa, vyjádřená v procentech (např. 2,4 namísto 2,4 %). Pokud má hodnota více než jednu číslici za desetinnou čárkou, oznamující strany ji zaokrouhlí nahoru na poloviny.
3.6	Počet dotčených finančních protistran	Počet finančních protistran dotčených závažným incidentem souvisejícím s IKT, které mají s finančním subjektem uzavřenu smlouvu. Při posuzování počtu dotčených finančních protistran přihlížejí finanční subjekty k čl. 1 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečný počet dotčených finančních protistran, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. V případě souhrnného hlášení podle článku 7 tohoto nařízení celkový počet dotčených finančních protistran u všech finančních subjektů.	Ne	Ano	Ano	Numerické celočíselné

	Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.7	Procento dotčených finančních protistran	Procentní podíl finančních protistran dotčených závažným incidentem souvisejícím s IKT ve vztahu k celkovému počtu finančních protistran, které s finančním subjektem uzavřely smlouvu. Při posuzování procenta dotčených finančních protistran přihlížejí finanční subjekty k čl. 1 odst. 1 a čl. 9 odst. 1 písm. c) nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečné procento dotčených finančních protistran, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. V případě souhrnného hlášení podle článku 7 tohoto nařízení uveďte součet všech dotčených finančních protistran vydělený celkovým počtem finančních protistran všech dotčených finančních subjektů.	Ne	Ano	Ano	Vyjádřeno v procentech – jakákoli hodnota o nejvýše pěti číselných znacích včetně nejvýše jednoho desetinného místa, vyjádřená v procentech (např. 2,4 namísto 2,4 %). Pokud má hodnota více než jednu číslici za desetinnou čárkou, oznamující strany ji zaokrouhlí nahoru na poloviny.
3.8	Dopad na příslušné klienty nebo finanční protistrany	Jakýkoli zjištěný dopad na příslušné klienty nebo finanční protistranu podle čl. 1 odst. 3 a čl. 9 odst. 1 písm. f) nařízení v přenesené pravomoci (EU) 2024/1772.	Ne	Ano, pokud je splněna prahová hodnota „Relevance klientů a finančních protistran“	Ano, pokud je splněna prahová hodnota „Relevance klientů a finančních protistran“	Booleovské (ano nebo ne)
3.9	Počet dotčených transakcí	Počet transakcí dotčených závažným incidentem souvisejícím s IKT. Při posuzování dopadu na transakce přihlížejí finanční subjekty k čl. 1 odst. 4 nařízení v přenesené pravomoci (EU) 2024/1772, včetně toho, že všechny dotčené domácí a přeshraniční transakce obsahují peněžní částku a mají alespoň jednu část transakce provedenou v Unii.	Ne	Ano, pokud byla incidentem dotčena jakákoli transakce	Ano, pokud byla incidentem dotčena jakákoli transakce	Numerické celočíselné

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	Finanční subjekt, která není schopen určit skutečný počet dotčených transakcí, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. V případě souhrnného hlášení podle článku 7 tohoto nařízení uveďte celkový počet dotčených transakcí u všech finančních subjektů.				
3.10 Procento dotčených transakcí	Procentní podíl dotčených transakcí ve vztahu k průměrnému dennímu počtu domácích a přeshraničních transakcí prováděných finančním subjektem v souvislosti s dotčenou službou. Finanční subjekty přihlížejí k čl. 1 odst. 4 a čl. 9 odst. 1 písm. d) nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečné procento dotčených transakcí, použije odhady. V případě souhrnného hlášení podle článku 7 tohoto nařízení finanční subjekt sečte počet všech dotčených transakcí a vydělí tento součet celkovým počtem transakcí všech dotčených finančních subjektů.	Ne	Ano, pokud byla incidentem dotčena jakákoli transakce	Ano, pokud byla incidentem dotčena jakákoli transakce	Vyjádřeno v procentech – jakákoli hodnota o nejvýše pěti číselných znacích včetně nejvýše jednoho desetinného místa, vyjádřená v procentech (např. 2,4 namísto 2,4 %). Pokud má hodnota více než jednu číslici za desetinnou čárkou, oznamující strany ji zaokrouhlí nahoru na poloviny.
3.11 Hodnota dotčených transakcí	Celková hodnota transakcí dotčených závažnou událostí související s IKT se posuzuje v souladu s čl. 1 odst. 4 a čl. 9 odst. 1 písm. e) nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekt, který není schopen určit skutečnou hodnotu dotčených transakcí, použije odhady založené na dostupných údajích ze srovnatelných referenčních období. Finanční subjekt uvede tuto peněžní částku jako kladnou hodnotu. V případě souhrnného hlášení podle článku 7 tohoto nařízení celková hodnota dotčených transakcí u všech dotčených subjektů.	Ne	Ano, pokud byla incidentem dotčena jakákoli transakce	Ano, pokud byla incidentem dotčena jakákoli transakce	Peněžní Finanční subjekty uvedou tento datový bod v jednotkách s minimální přesností odpovídající tisícům jednotek (např. 2,5 namísto 2 500 EUR).

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.12 Informace o tom, zda se jedná o skutečná čísla nebo odhady, nebo zda nedošlo k žádnému dopadu	Informace o tom, zda hodnoty uvedené v datových polích 3.4. až 3.11. jsou skutečné nebo odhadované, nebo zda nedošlo k žádnému dopadu.	Ne	Ano	Ano	Výběr z možností (lze zvolit více možností): — skutečné údaje o dotčených klientech, — skutečné údaje o dotčených finančních protistranách, — skutečné údaje o dotčených transakcích, — odhady dotčených klientů, — odhady dotčených finančních protistran, — odhady dotčených transakcí; — žádný dopad na klienty, — žádný dopad na finanční protistrany, — žádný dopad na transakce.
3.13 Poškození dobré pověsti	Informace o poškození dobré pověsti v důsledku závažného incidentu souvisejícího s IKT, jak je uvedeno v článcích 2 a 10 nařízení v přenesené pravomoci (EU) 2024/1772. V případě souhrnného hlášení podle článku 7 tohoto nařízení kategorie poškození dobré pověsti, které se týkají alespoň jednoho finančního subjektu.	Ne	Ano, pokud je splněno kritérium „Poškození dobré pověsti“	Ano, pokud je splněno kritérium „Poškození dobré pověsti“	Výběr z možností (lze zvolit více možností): — závažný incident související s IKT byl zveřejněn v médiích, — závažný incident související s IKT měl za následek, že různí klienti nebo finanční protistrany opakovaně podávali stížnosti týkající se klientských služeb nebo zásadních obchodních vztahů, — finanční subjekt v důsledku závažného incidentu souvisejícího s IKT nebude schopen splnit nebo pravděpodobně nebude schopen splnit regulatorní požadavky, — finanční subjekt v důsledku závažného incidentu souvisejícího s IKT přijde nebo pravděpodobně přijde o klienty nebo finanční protistrany, což bude mít významný dopad na jeho obchodní činnost.
3.14 Informace o souvislostech poškození dobré pověsti	Informace o tom, jak závažný incident související s IKT ovlivnil nebo by mohl ovlivnit dobrou pověst finančního subjektu, včetně porušení právních předpisů, nesplněných regulatorních požadavků, počtu stížností klientů a dalších dopadů.	Ne	Ano, pokud je splněno kritérium „Poškození dobré pověsti“	Ano, pokud je splněno kritérium „Poškození dobré pověsti“	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
		Tyto informace zahrnují druh médií (např. tradiční a digitální média, blogy, streamovací platformy) a mediální pokrytí, včetně dosahu médií (místní, celostátní, mezinárodní). Mediálním pokrytím v této souvislosti není míněno několik negativních komentářů sledujících nebo uživatelů sociálních sítí. Finanční subjekt rovněž uvede, zda medializace upozornila na významná rizika pro jeho klienty v souvislosti se závažným incidentem souvisejícím s IKT, včetně rizika platební neschopnosti finančního subjektu nebo rizika ztráty finančních prostředků. Finanční subjekty dále uvedou, zda médiím poskytly informace, jež posloužily ke spolehlivému informování veřejnosti o závažném incidentu souvisejícím s IKT a jeho důsledcích. Finanční subjekty mohou také uvést, zda se v médiích v souvislosti s incidentem souvisejícím s IKT objevily nepravdivé informace, včetně informací založených na záměrných dezinformacích šířených aktéry hrozeb, nebo informace týkající se defacementu internetových stránek finančního subjektu nebo tento defacement názorně dokládající.				
3.15	Doba trvání incidentu	Finanční subjekty měří dobu trvání závažného incidentu souvisejícího s IKT od okamžiku, kdy k závažnému incidentu souvisejícímu s IKT došlo, do okamžiku, kdy byl vyřešen. Finanční subjekty, které nejsou schopny určit okamžik, kdy k závažnému incidentu souvisejícímu s IKT došlo, měří dobu trvání závažného incidentu souvisejícího s IKT buď od okamžiku, kdy finanční subjekt incident zjistil, nebo od okamžiku, kdy ho zaznamenal v síťových nebo systémových protokolech či jiných zdrojích dat, podle toho, co nastane dříve. Finanční subjekty, které dosud neznají okamžik, kdy bude závažný incident související s IKT vyřešen, použijí odhady. Tato hodnota se vyjadřuje ve dnech, hodinách a minutách. Pokud je v případě souhrnného hlášení podle článku 7 tohoto nařízení doba trvání u jednotlivých finančních subjektů rozdílná, měří finanční subjekty nejdelší dobu trvání závažného incidentu souvisejícího s IKT.	Ne	Ano	Ano	DD:HH:MM

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.16	Doba odstávky služby	Doba odstávky služby měřená od okamžiku, kdy je služba pro klienty, finanční protistrany nebo jiné interní či externí uživatele zcela nebo částečně nedostupná, do okamžiku, kdy jsou běžné činnosti nebo operace obnoveny na úroveň služby poskytovanou před závažným incidentem souvisejícím s IKT. V případě, že v důsledku odstávky byla služba poskytnuta se zpožděním poté, co byly běžné činnosti nebo operace obnoveny, měří finanční subjekty dobu odstávky služby od začátku závažného incidentu souvisejícího s IKT do okamžiku poskytnutí této zpožděné služby. Finanční subjekty, které nejsou schopny určit okamžik, kdy odstávka služby začala, měří odstávku služby buď od okamžiku zjištění incidentu, nebo od okamžiku jeho zaznamenání, podle toho, co nastane dříve. Pokud je v případě souhrnného hlášení podle článku 7 tohoto nařízení doba odstávky služby u jednotlivých finančních subjektů rozdílná, měří finanční subjekty nejdelší dobu odstávky služby.	Ne	Ano, pokud incident způsobil odstávku služby	Ano, pokud incident způsobil odstávku služby	DD:HH:MM
3.17	Informace o tom, zda údaje o době trvání a době odstávky služby jsou skutečné nebo odhadované	Informace o tom, zda jsou hodnoty uvedené v datových polích 3.15 a 3.16. skutečné nebo odhadované.	Ne	Ano, pokud je splněno kritérium „Doba trvání a doba odstávky služby“	Ano, pokud je splněno kritérium „Doba trvání a doba odstávky služby“	Výběr z možností: — skutečné údaje — odhady — skutečné údaje a odhady — informace nejsou k dispozici
3.18	Druhy dopadu v členských státech	Druh dopadu v příslušných členských státech EHP. Údaj o tom, zda závažný incident související s IKT měl dopad na jiné členské státy EHP (jiné než členský stát příslušného orgánu, jemuž se incident přímo hlásí), v souladu s článkem 4 nařízení v přenesené pravomoci (EU) 2024/1772, zejména s ohledem na významnost dopadu ve vztahu k: a) dotčeným klientům a finančním protistranám v jiných členských státech nebo	Ne	Ano, pokud je splněna prahová hodnota „Územní rozsah“	Ano, pokud je splněna prahová hodnota „Územní rozsah“	Výběr z možností (lze zvolit více možností): — klienti — finanční protistrany — pobočka finančního subjektu — finanční subjekty v rámci téže skupiny, které vyvíjejí činnost v příslušném členském státě — infrastruktura finančního trhu — poskytovatelé z řad třetích stran, kteří mohou být společní s jinými finančními subjekty

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	b) pobočkám či jiným finančním subjektům v rámci téže skupiny, které vyvíjejí činnost v jiných členských státech, nebo c) infrastrukturám finančních trhů nebo poskytovatelům z řad třetích stran, kde se může dotýkat finančních subjektů v jiných členských státech, jimž poskytují služby.				
3.19 Popis dopadu incidentu na jiné členské státy	Popis dopadu a závažnosti závažného incidentu souvisejícího s IKT v jednotlivých dotčených členských státech, včetně posouzení dopadu a závažnosti, pokud jde o: a) klienty; b) finanční protistrany; c) pobočky finančního subjektu; d) jiné finanční subjekty v rámci téže skupiny, které vyvíjejí činnost v příslušném členském státě; e) infrastruktury finančních trhů; f) poskytovatele z řad třetích stran, kteří mohou být společní s jinými finančními subjekty, pokud je to v jiném členském státě nebo státech relevantní.	Ne	Ano, pokud je splněna prahová hodnota „Územní rozsah“	Ano, pokud je splněna prahová hodnota „Územní rozsah“	Alfanumerické
3.20 Prahy významnosti pro klasifikační kritérium „Ztráty údajů“	Druh ztrát údajů, které závažný incident související s IKT způsobil, pokud jde o dostupnost, hodnověrnost, integritu nebo důvěrnost údajů. Finanční subjekty při posuzování přihlížejí k článkům 5 a 13 nařízení v přenesené pravomoci (EU) 2024/1772. V případě souhrnného hlášení podle článku 7 tohoto nařízení ztráty údajů, jež postihly alespoň jeden finanční subjekt.	Ne	Ano, pokud je splněno kritérium „Ztráty údajů“	Ano, pokud je splněno kritérium „Ztráty údajů“	Výběr z možností (lze zvolit více možností): — dostupnost — hodnověrnost — integrita — důvěrnost
3.21 Popis ztrát údajů	Popis dopadu závažného incidentu souvisejícího s IKT na dostupnost, hodnověrnost, integritu a důvěrnost kritických údajů v souladu s články 5 a 13 nařízení v přenesené pravomoci (EU) 2024/1772. Informace o dopadu na realizaci obchodních cílů finančního subjektu nebo na plnění regulatorních požadavků. V rámci poskytovaných informací finanční subjekty uvedou, zda dotčenými údaji jsou údaje klientů, údaje jiných subjektů (např. finančních protistran) nebo údaje samotného finančního subjektu.	Ne	Ano, pokud je splněno kritérium „Ztráty údajů“	Ano, pokud je splněno kritérium „Ztráty údajů“	Alfanumerické

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	Finanční subjekt může také uvést druh údajů, jichž se incident týká – zejména zda jde o důvěrné údaje a o jaký typ důvěrnosti se jedná (např. obchodní důvěrnost/tajemství, osobní údaje, profesní tajemství: bankovní tajemství, pojišťovací tajemství, tajemství platebních služeb atd.). Informace mohou zahrnovat také možná rizika spojená se ztrátami údajů, například zda údaje dotčené incidentem mohou být použity k identifikaci osob a mohly by být aktérem hrozby použity k získání úvěru nebo půjčky bez jejich souhlasu, k provedení phishingových útoků nebo ke zveřejnění informací. V případě souhrnného hlášení podle článku 7 tohoto nařízení obecný popis dopadu incidentu na dotčené finanční subjekty. Pokud je dopad rozdílný, musí popis dopadu jasně uvádět konkrétní dopad na jednotlivé finanční subjekty.				
3.22 Klasifikační kritérium „Dotčené významné služby“	Informace týkající se kritéria „Dotčené významné služby“. Finanční subjekty při posuzování přihlížejí k článku 6 nařízení v přenesené pravomoci (EU) 2024/1772, včetně informací o: — dotčených službách nebo činnostech. které vyžadují povolení nebo registraci nebo nad nimiž vykonávají dohled příslušné orgány, nebo — službách nebo síti IKT a informačních systémech, které podporují zásadní nebo důležité funkce finančního subjektu, a — povaze zlovolného a neoprávněného přístupu do sítě a informačních systémů finančního subjektu. V případě souhrnného hlášení podle článku 7 tohoto nařízení dopad na významné služby týkající se alespoň jednoho finančního subjektu.	Ne	Ano	Ano	Alfanumerické

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.23 Druh incidentu	Klasifikace incidentů podle druhu.	Ne	Ano	Ano	Výběr z možností (lze zvolit více možností): — incident související s kybernetickou bezpečností — selhání procesu — Porucha systému — externí událost — incident související s platbami — jiný incident (upřesněte)
3.24 Jiné druhy incidentů	Jiné druhy incidentů souvisejících s IKT: finanční subjekty, které v datovém poli 3.23 zvolily typ incidentu „Jiný incident“, druh incidentu souvisejícího s IKT upřesní.	Ne	Ano, pokud je v datovém poli 3.23 zvolen typ incidentu „Jiný incident“	Ano, pokud je v datovém poli 3.23 zvolen typ incidentu „Jiný incident“	Alfanumerické
3.25 Hrozby a techniky použité aktérem hrozby	Uveďte hrozby a techniky použité aktérem hrozby, například: a) sociální inženýrství, včetně phishingu; b) útok (D)DoS; c) krádež identity; d) šifrování dat s dopadem, včetně ransomwaru; e) únos zdrojů; f) exfiltrace dat a manipulace s daty, s výjimkou krádeže identity; g) zničení dat; h) nahrazení originálního obsahu podvrhem (defacement); i) útok na dodavatelský řetězec; j) jiné (upřesněte).	Ne	Ano, pokud je v poli 3.23 uveden typ incidentu souvisejícího s IKT „Incident související s kybernetickou bezpečností“	Ano, pokud je v poli 3.23 uveden typ incidentu souvisejícího s IKT „Incident související s kybernetickou bezpečností“	Výběr z možností (lze zvolit více možností): — Sociální inženýrství (včetně phishingu) — útok (D)DoS — krádež identity — šifrování dat za účelem dopadu, včetně ransomwaru — únos zdrojů — exfiltrace dat a manipulace s daty, včetně krádeže identity — zničení dat — nahrazení originálního obsahu podvrhem (defacement) — útok na dodavatelský řetězec — jiný incident (upřesněte)
3.26 Jiné druhy technik	Jiné druhy technik Finanční subjekty, které v datovém poli 3.25 zvolily druh technik „Jiné“, druh techniky upřesní.	Ne	Ano, pokud je v datovém poli 3.25 zvolen typ incidentu „Jiný incident“	Ano, pokud je v datovém poli 3.25 zvolen typ incidentu „Jiný incident“	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.27	Informace o dotčených funkčních oblastech a obchodních procesech	Vymezení funkčních oblastí a obchodních procesů, které jsou incidentem dotčeny, včetně produktů a služeb. Funkční oblasti zahrnují mimo jiné: a) marketing a rozvoj podnikání; b) zákaznické služby; c) řízení produktů; d) dodržování předpisů; e) řízení rizik; f) finance a účetnictví; g) lidské zdroje a obecné služby; h) informační technologie. Obchodní procesy zahrnují mimo jiné: — informování o účtu, — pojistněmatematické služby, — akceptace platebních transakcí, — ověřování/autorizace, — onboarding — nových orgánů/klientů, — správa požitků, — řízení výplat požitků, — nákup a prodej balíčků pojištění mezi pojišťovnami, — platby kartou, — řízení hotovosti, — vložení nebo výběry hotovosti, — správa pojistných plnění, — pojištění procesu pojistných událostí, — zúčtování, — konglomeráty podnikových úvěrů, — kolektivní pojištění, — úhrady, — úschova a uložení aktiv, — onboarding zákazníků, — přijímání dat, — zpracování dat, — inkasa, — vývozní pojištění, — finalizace obchodů/prodejů, — umístění finančních nástrojů, — účetnictví fondů,	Ne	Ano	Ano	Alfanumerické

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	— valuty a devizy, — investiční poradenství, — správa investic, — vydávání platebních prostředků, — řízení úvěrů, — proces plateb životního pojištění, — poukazování peněz, — výpočet čistých aktiv, — příkaz, — iniciování platby, — upisování pojištění, — správa portfolií, — výběr pojistného/zajistného, — příjem/předávání/provádění, — zajištění, — vypořádání, — sledování transakcí. V případě souhrnného hlášení podle článku 7 tohoto nařízení dotčené funkční oblasti a obchodní procesy alespoň u jednoho finančního subjektu.				
3.28 Dotčené součásti infrastruktury podporující obchodní procesy	Informace o tom, zda byly závažným incidentem souvisejícím s IKT dotčeny součásti infrastruktury (servery, operační systémy, software, aplikační servery, middleware, síťové komponenty a další), které podporují obchodní procesy.	Ne	Ano	Ano	Výběr z možností: — Ano — Ne — Informace nejsou k dispozici
3.29 Informace o dotčených součástech infrastruktury podporujících obchodní procesy	Popis dopadu závažného incidentu souvisejícího s IKT na součásti infrastruktury podporující obchodní procesy včetně hardwaru a softwaru. Hardware zahrnuje servery, počítače, datová centra, přepínače, směrovače, rozbočovače. Software zahrnuje operační systémy, aplikace, databáze, bezpečnostní nástroje, síťové komponenty a další. V těchto popisech je třeba dotčené součásti nebo systémy infrastruktury popsat nebo vyjmenovat, a pokud jsou k dispozici, je třeba uvést: a) informace o verzi; b) zda jde o infrastrukturu interní / zčásti zajištěnou externě / plně zajištěnou externě – název poskytovatele z řad třetích stran;	Ne	Ano, pokud incident ovlivnil součásti infrastruktury podporující obchodní procesy	Ano, pokud incident ovlivnil součásti infrastruktury podporující obchodní procesy	Alfanumerické

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	c) zda je infrastruktura využívaná / sdílená pro více obchodních funkcí; d) příslušná zavedená opatření pro zajištění odolnosti/ kontinuity/obnovy/zastupitelnosti.				
3.30 Dopad na finanční zájmy klientů	Informace o tom, zda měl závažný incident související s IKT dopad na finanční zájmy klientů.	Ne	Ano	Ano	Výběr z možností: — Ano — Ne — Informace nejsou k dispozici
3.31 Hlášení podávaná jiným orgánům	Upřesnění, které orgány byly o závažném incidentu souvisejícím s IKT informovány. S ohledem na rozdíly vyplývající z vnitrostátních právních předpisů členských států musí být pojem donucovací orgány chápán finančními subjekty široce jako zahrnující orgány veřejné správy oprávněné stíhat kybernetickou kriminalitu, včetně policie, donucovacích orgánů a státních zástupců.	Ne	Ano	Ano	Výběr z možností (lze zvolit více možností): — Policie a donucovací orgány — Tým pro reakce na počítačové bezpečnostní incidenty (CSIRT) — Úřad pro ochranu osobních údajů — Národní agentura pro kybernetickou bezpečnost — Žádný orgán — Jiný orgán (upřesněte)
3.32 Upřesnění „jiných“ orgánů	Upřesnění jiných druhů orgánů, které byly o závažném incidentu souvisejícím s IKT informovány. Pokud je zvoleno datové pole 3.31 „Jiný orgán“, musí popis obsahovat podrobnější informace o orgánu, jemuž finanční subjekt informace o závažném incidentu souvisejícím s IKT předložil.	Ne	Ano, pokud finanční subjekt informoval o závažném incidentu souvisejícím s IKT jiný druh orgánů	Ano, pokud finanční subjekt informoval o závažném incidentu souvisejícím s IKT jiný druh orgánů	Alfanumerické
3.33 Dočasná opatření přijatá nebo plánovaná k překonání účinků incidentu	Údaj o tom, zda finanční subjekt provedl (nebo hodlá provést) dočasná opatření, která byla přijata (nebo jejichž přijetí se plánuje) k překonání účinků závažného incidentu souvisejícího s IKT.	Ne	Ano	Ano	Booleovské (ano nebo ne)

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
3.34 Popis všech dočasných opatření přijatých nebo plánovaných k překonání účinků incidentu	Tato informace musí popisovat bezprostředně přijatá opatření, včetně izolace incidentu na úrovni sítě, aktivovaných postupů pro obejití, zablokovaných portů USB, aktivace místa pro obnovu po havárii a veškeré další dočasně zavedené dodatečné bezpečnostní kontroly. Finanční subjekty uvedou datum a čas provedení dočasných opatření a předpokládané datum návratu na primární místo. U všech dočasných opatření, která dosud nebyla provedena, ale stále jsou plánována, uveďte datum, do kdy se jejich provedení předpokládá. Pokud nebyla přijata žádná dočasná opatření, uveďte důvod.	Ne	Ano, pokud byla přijata dočasná opatření nebo se jejich přijetí plánuje (datové pole 3.33)	Ano, pokud byla přijata dočasná opatření nebo se jejich přijetí plánuje (datové pole 3.33)	Alfanumerické
3.35 Ukazatele narušení	Případné informace týkající se závažného incidentu souvisejícího s IKT, které mohou přispět k identifikaci nepřátelské činnosti v síti nebo informačním systému (ukazatele narušení). Toto pole se v příslušných případech týká pouze těch finančních subjektů, které spadají do oblasti působnosti směrnice Evropského parlamentu a Rady (EU) 2022/2555 ([1]), a těch finančních subjektů, které jsou podle vnitrostátních předpisů, jimiž se provádí článek 3 směrnice (EU) 2022/2555, označeny za základní nebo důležité subjekty. Ukazatel narušení poskytnutý finančním subjektem zahrnuje tyto kategorie údajů: a) IP adresy; b) URL adresy; c) domény; d) hashe souborů; e) údaje o malwaru (název malwaru, názvy souborů a jejich umístění, konkrétní klíče registru spojené s činností malwaru); f) údaje o činnosti sítě (porty, protokoly, adresy, referery, řetězce user agent, hlavičky, konkrétní protokoly nebo charakteristické vzorce síťového provozu); g) údaje e-mailové zprávy (odesílatel, příjemce, předmět, záhlaví, obsah);	Ne	Ano, pokud je v datovém poli 3.23 jako druh incidentu vybrána možnost „Incident související s kybernetickou bezpečností“	Ano, pokud je v datovém poli 3.23 jako druh incidentu vybrána možnost „Incident související s kybernetickou bezpečností“	Alfanumerické

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	h) požadavky systému DNS a konfigurace registru; i) činnosti uživatelských účtů (přihlašování, činnost privilegovaných uživatelských účtů, zvyšování oprávnění); j) databázový provoz (čtení/zápis), požadavky na stejný soubor. V praxi může tento druh informací zahrnovat údaje týkající se například ukazatelů popisujících vzorce síťového provozu, které odpovídají známým útokům/komunikaci v rámci botnetu, IP adresy počítačů infikovaných malwarem (botů), údaje týkající se „řídicích a kontrolních“ serverů používaných malwarem (obvykle domény nebo IP adresy) a adresy URL týkající se phishingových stránek nebo internetových stránek, na nichž byl pozorován malware nebo exploit kity.				
Obsah závěrečné zprávy					
4.1 Vysokoúrovňová klasifikace hlavních příčin incidentu	Vysokoúrovňová klasifikace hlavní příčiny závažného incidentu souvisejícího s IKT podle druhu incidentu, zahrnující tyto základní kategorie: a) zlovolné jednání; b) selhání procesu; c) selhání/porucha systému; d) lidská chyba; e) externí událost.	Ne	Ne	Ano	Výběr z možností (lze zvolit více možností): — zlovolné jednání, — selhání procesu, — selhání/porucha systému, — lidská chyba, — externí událost.
4.2 Podrobná klasifikace hlavních příčin incidentu	Podrobná klasifikace hlavních příčin závažného incidentu souvisejícího s IKT podle druhu incidentu, zahrnující tyto podrobné kategorie spojené s vysokoúrovňovými kategoriemi uvedenými v datovém poli 4.1: 1. **Zlovolné jednání** (je-li zvoleno, vyberte nejméně jednu z následujících možností): a) úmyslné vnitřní zásahy; b) úmyslné fyzické poškození / manipulace / krádež; c) podvodné jednání. 2. **Selhání procesu** (je-li zvoleno, vyberte nejméně jednu z následujících možností): a) nedostatečné monitorování nebo selhání monitorování a kontroly;	Ne	Ne	Ano	Výběr z možností (lze zvolit více možností): — zlovolné jednání: úmyslné vnitřní zásahy, — zlovolné jednání: úmyslné fyzické poškození / manipulace / krádež; — zlovolné jednání: podvodné jednání, — selhání procesu: nedostatečné monitorování nebo selhání monitorování a kontroly, — selhání procesu: nedostatečné/nejasné úlohy a odpovědnosti, — selhání procesu: selhání procesu řízení rizik IKT, — selhání procesu: nedostatečné nebo neúspěšné operace IKT a bezpečnostní operace IKT,

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	b) nedostatečné/nejasné úlohy a odpovědnosti; c) selhání procesu řízení rizik IKT; d) nedostatečné nebo neúspěšné operace IKT a bezpečnostní operace IKT; e) nedostatečné nebo neúspěšné řízení projektů IKT; f) nevhodné interní zásady, postupy a dokumentace; g) nevhodné pořizování, vývoj nebo údržba systémů IKT; h) jiné (upřesněte). 3. **Porucha/nefunkčnost systému** (je-li zvoleno, vyberte nejméně jednu z následujících možností): a) kapacita a výkonnost hardwaru: závažné incidenty související s IKT způsobené hardwarovými prostředky, které se ukážou být z hlediska kapacity nebo výkonnosti nedostatečné ke splnění požadavků příslušných právních předpisů; b) údržba hardwaru: závažné incidenty související s IKT, které jsou důsledkem nevhodné nebo nedostatečné údržby hardwarových komponentů, jiné než „zastaralost/stárnutí hardwaru“; c) zastaralost/stárnutí hardwaru: tento druh hlavní příčiny se týká závažných incidentů souvisejících s IKT, které jsou důsledkem zastaralých nebo stárnoucích hardwarových komponentů; d) kompatibilita/konfigurace softwaru: závažné incidenty související s IKT způsobené softwarovými komponenty, které jsou nekompatibilní s jiným softwarem nebo systémovými konfiguracemi, včetně závažných incidentů souvisejících s IKT v důsledku konfliktů softwaru, nesprávných nastavení nebo chybně nakonfigurovaných parametrů, které ovlivňují celkovou funkčnost systému; e) výkonnost softwaru: závažné incidenty související s IKT, které jsou důsledkem softwarových komponentů vykazujících nízkou výkonnost nebo neefektivitu z jiných důvodů, než jsou uvedeny v rámci „kompatibility/konfigurace softwaru“, včetně závažných incidentů souvisejících s IKT způsobených pomalou dobou odezvy, nadměrnou spotřebou zdrojů nebo neefektivním prováděním dotazů, které mají dopad na výkonnost softwaru nebo systému;				— selhání procesu: nedostatečné nebo neúspěšné řízení projektů IKT; — selhání procesu: nevhodnost interních zásad, postupů a dokumentace, — selhání procesu: nevhodné pořizování, vývoj a údržba systémů IKT, — selhání procesu: jiná možnost (upřesněte), — porucha systému: kapacita a výkonnost hardwaru, — porucha systému: údržba hardwaru, — porucha systému: zastaralost/stárnutí hardwaru, — porucha systému: kompatibilita/konfigurace softwaru, — porucha systému: výkonnost softwaru, — porucha systému: konfigurace sítě, — porucha systému: fyzické poškození, — porucha systému: jiná možnost (upřesněte), — lidská chyba: opomenutí, — — lidská chyba: omyl, — lidská chyba: dovednosti a znalosti, — lidská chyba: nedostatečné lidské zdroje, — lidská chyba: chyba v komunikaci, — lidská chyba: jiná možnost (upřesněte), — externí událost: přírodní katastrofy / vyšší moc, — externí událost: selhání třetích stran, — externí událost: jiné (upřesněte).

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	f) konfigurace sítě: závažné incidenty související s IKT, které jsou důsledkem nesprávného nebo chybného nastavení sítě nebo infrastruktury, včetně závažných incidentů souvisejících s IKT způsobených chybami v konfiguraci sítě, problémy se směrováním, chybnou konfigurací brány firewall nebo jinými problémy souvisejícími se sítí, které ovlivňují konektivitu nebo komunikaci; g) fyzické poškození: závažné incidenty související s IKT způsobené fyzickým poškozením infrastruktury IKT, které vedou k selhání systému; h) jiné (upřesněte). 4. **Lidská chyba** (je-li zvoleno, vyberte nejméně jednu z následujících možností): a) opomenutí (neúmyslné); b) omyl; c) dovednosti a znalosti: závažné incidenty související s IKT, které jsou důsledkem nedostatečných odborných znalostí nebo způsobilosti při zacházení se systémy nebo procesy IKT, jež mohou být způsobeny nevhodnou odbornou přípravou, nedostatečnými znalostmi nebo nedostatky v dovednostech potřebných k provádění konkrétních úkolů nebo řešení technických problémů; d) nedostatečné lidské zdroje: závažné incidenty související s IKT způsobené nedostatkem potřebných zdrojů, včetně hardwaru, softwaru, infrastruktury nebo pracovníků a včetně situací, kdy nedostatečné zdroje vedou k provozní neefektivitě, selhání systému nebo neschopnosti plnit obchodní požadavky; e) chyba v komunikaci; f) jiné (upřesněte). 5. **Externí událost** (je-li zvoleno, vyberte nejméně jednu z následujících možností) a) přírodní katastrofy / vyšší moc; b) selhání třetích stran;				

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	c) jiné (upřesněte). Finanční subjekty vezmou v úvahu, že v případě opakujících se závažných incidentů souvisejících s IKT se bere v potaz konkrétní zjevná hlavní příčina incidentu, a nikoli obecné kategorie uvedené v tomto poli.				
4.3 Další klasifikace hlavních příčin incidentu	Další klasifikace hlavních příčin závažného incidentu souvisejícího s IKT podle druhu incidentu, zahrnující následující další klasifikační kategorie spojené s podrobnými kategoriemi, které se uvedou v datovém poli 4.2. Toto pole je pro závěrečnou zprávu povinné, pokud jsou v datovém poli 4.2 uvedeny určité kategorie, které vyžadují další rozčlenění. 2a) **Nedostatečné nebo selhávající sledování a kontrola:** a) sledování dodržování zásad; b) sledování poskytovatelů služeb z řad třetích stran; c) sledování a ověřování nápravy zranitelností; d) správa identit a řízení přístupu; e) šifrování a kryptografie; f) vedení protokolů. 2c) **Selhání procesu řízení rizik IKT:** a) selhání při stanovení správných úrovní tolerance rizik; b) nedostatečné posouzení zranitelnosti a hrozeb; c) nevhodná opatření k řešení rizik; d) špatné řízení zbytkových rizik v oblasti IKT. 2d) **Nedostatečné nebo neúspěšné operace IKT a bezpečnostní operace IKT:** a) řízení zranitelností a dočasných oprav; b) řízení změn; c) řízení kapacity a výkonu; d) řízení aktiv a klasifikace informací v rámci IKT;	Ne	Ne	Ano	Výběr z možností (lze zvolit více možností): — sledování dodržování zásad; — sledování poskytovatelů služeb z řad třetích stran; — sledování a ověřování nápravy zranitelností; — správa identit a řízení přístupu; — šifrování a kryptografie; — vedení protokolů; — selhání při stanovení správných úrovní tolerance rizik; — nedostatečné posouzení zranitelnosti a hrozeb; — nevhodná opatření k řešení rizik; — špatné řízení zbytkových rizik v oblasti IKT; — řízení zranitelností a dočasných oprav; — řízení změn; — řízení kapacity a výkonu; — řízení aktiv a klasifikace informací v rámci IKT; — zálohování a obnovení; — řešení chyb; — nevhodné pořizování, vývoj a údržba systémů IKT; — nedostatečné testování softwaru nebo selhání testování softwaru

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
		e) zálohování a obnovení; f) řešení chyb. 2 **g) Nevhodné pořizování, vývoj a údržba systémů IKT** a) nevhodné pořizování, vývoj a údržba systémů IKT; b) nedostatečné testování softwaru nebo selhání testování softwaru.				
4.4	Jiné druhy hlavních příčin	Finanční subjekty, které v datovém poli 4.2. zvolily jako druh hlavní příčiny „Jinou možnost“, tyto jiné druhy hlavních příčin upřesní.	Ne	Ne	Ano, pokud je v datovém poli 4.2 zvolena jako druh hlavní příčiny „Jiná možnost“	Alfanumerické
4.5	Informace o hlavních příčinách incidentu	Popis sledu událostí, které k závažnému incidentu souvisejícímu s IKT vedly, a pokud je incident klasifikován jako opakující se incident, popis toho, jak má tento závažný incident související s IKT podobnou zjevnou hlavní příčinu, včetně stručného popisu všech základních důvodů a hlavních faktorů, které k výskytu závažného incidentu souvisejícího s IKT přispěly. V případě, že došlo ke zlovolnému jednání, popis způsobu provedení zlovolného zásahu, včetně použitých taktik, technik a postupů, jakož i vstupního vektoru závažného incidentu souvisejícího s IKT, včetně případného popisu vyšetřování a analýzy, které vedly k určení hlavních příčin.	Ne	Ne	Ano	Alfanumerické
4.6	Řešení incidentu	Další informace o přijatých/plánovaných opatřeních k trvalému vyřešení závažného incidentu souvisejícího s IKT a k zabránění jeho opakování. Zkušenosti získané ze závažného incidentu souvisejícího s IKT.	Ne	Ne	Ano	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
		Popis musí obsahovat tyto body: 1. **Popis opatření k řešení** a) opatření přijatá k trvalému vyřešení závažného incidentu souvisejícího s IKT (kromě dočasných opatření); b) u každého přijatého opatření uveďte případné zapojení poskytovatele z řad třetích stran a finančního subjektu; c) uveďte, zda byly po závažném incidentu souvisejícím s IKT upraveny postupy; d) uveďte veškerá další kontrolní opatření, která byla zavedena nebo jsou plánována, a příslušný časový plán jejich provádění. Případné zjištěné problémy týkající se odolnosti dotčených IT systémů a/nebo z hlediska zavedených postupů nebo kontrolních opatření. Finanční subjekty jasně uvedou, jakým způsobem plánovaná nápravná opatření odstraní zjištěné hlavní příčiny a kdy se předpokládá trvalé vyřešení závažného incidentu souvisejícího s IKT. 2. **Získané zkušenosti** Finanční subjekty popíšou zjištění z přezkumu provedeného po incidentu.				
4.7	Datum a čas odstranění hlavní příčiny incidentu	Datum a čas, kdy byla hlavní příčina incidentu odstraněna.	Ne	Ne	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601 (RRRR-MM-DD Thh: mm:ss)
4.8	Datum a čas vyřešení incidentu	Datum a čas, kdy byl incident vyřešen.	Ne	Ne	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601 (RRRR-MM-DD Thh: mm:ss)

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
4.9	Informace o tom, zda se datum trvalého vyřešení incidentů liší od původně plánovaného data provedení	Případně popis důvodu, proč se datum trvalého vyřešení závažných incidentů souvisejících s IKT liší od původně plánovaného data provedení.	Ne	Ne	Ano	Alfanumerické
4.10	Posouzení rizika pro zásadní funkce pro účely řešení krize	Posouzení, zda závažný incident související s IKT představuje riziko pro zásadní funkce ve smyslu čl. 2 odst. 1 bodu 35 směrnice Evropského parlamentu a Rady 2014/59/EU ([2]). Subjekty uvedené v čl. 1 odst. 1 směrnice 2014/59/EU uvedou, zda incident představuje riziko pro zásadní funkce ve smyslu čl. 2 odst. 1 bodu 35 směrnice 2014/59/EU, jež se vykazuje podle vzoru Z 07.01 prováděcího nařízení Komise (EU) 2018/1624 ([3]) a přiřazuje se ke konkrétnímu subjektu podle vzoru Z 07.02.	Ne	Ne	Ano, pokud incident představuje riziko pro zásadní funkce finančních subjektů podle čl. 2 odst. 1 bodu 35 směrnice 2014/59/EU	Alfanumerické
4.11	Informace relevantní pro orgány příslušné k řešení krize	Popis toho, zda a případně jak závažný incident související s IKT ovlivnil způsobilost subjektu nebo skupiny k řešení krize. Subjekty uvedené v čl. 1 odst. 1 směrnice 2014/59/EU poskytnou informace o tom, zda a případně jak závažný incident související s IKT ovlivnil způsobilost subjektu nebo skupiny k řešení krize. Tyto subjekty rovněž uvedou, zda má závažný incident související s IKT dopad na platební schopnost nebo likviditu finančního subjektu, a případnou kvantifikaci tohoto dopadu. Tyto subjekty poskytnou rovněž informace o dopadu na kontinuitu provozu, dopadu na způsobilost subjektu k řešení krize a případném dodatečném dopadu na náklady a ztráty způsobeném závažným incidentem souvisejícím s IKT, včetně dopadu na kapitálovou pozici finančního subjektu, a o tom, zda jsou smluvní ujednání o využívání služeb IKT stále spolehlivá a plně vymahatelná v případě řešení krize subjektu.	Ne	Ne	Ano, pokud incident ovlivnil způsobilost subjektu nebo skupiny k řešení krize	Alfanumerické

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
4.12	Práh významnosti pro klasifikační kritérium „Ekonomický dopad“	Podrobné informace o prahových hodnotách, jichž závažný incident související s IKT nakonec dosáhl v souvislosti s kritériem „Ekonomický dopad“ podle článků 7 a 14 nařízení v přenesené pravomoci (EU) 2024/1772.	Ne	Ne	Ano	Alfanumerické
4.13	Výše hrubých přímých a nepřímých nákladů a ztrát	Celková výše hrubých přímých a nepřímých nákladů a ztrát, které finančnímu subjektu v důsledku závažného incidentu souvisejícího s IKT vznikly, včetně: a) výše vyvlastněných finančních prostředků nebo finančních aktiv, za něž je finanční subjekt odpovědný; b) výše nákladů na výměnu nebo přemístění softwaru, hardwaru nebo infrastruktury; c) výše nákladů na zaměstnance, včetně nákladů spojených s výměnou nebo přeložením zaměstnanců, náborem dalších zaměstnanců, odměnou za práci přesčas a obnovou pozbytých nebo zhoršených dovedností zaměstnanců; d) výše poplatků vzniklých v důsledku nedodržení smluvních závazků; e) výše nákladů na odškodnění zákazníků a náhradu škody; f) výše ztrát v důsledku ušlých příjmů; g) výše nákladů spojených s interní a externí komunikací; h) výše nákladů na poradenství, včetně nákladů spojených s právním poradenstvím, forenzními službami a službami k zajištění nápravy; i) výše ostatních nákladů a ztrát, jež zahrnují: i) přímé zaúčtování nákladů, včetně nákladů ze snížení hodnoty a vypořádání, do výsledovky a odpisy způsobené závažným incidentem souvisejícím s IKT; ii) rezervy nebo opravné položky zaúčtované ve výsledovce proti pravděpodobným ztrátám souvisejícím s významným incidentem souvisejícím s IKT;	Ne	Ne	Ano	Peněžní

Datové pole		Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
		iii) nezaúčtované ztráty ve formě ztrát plynoucích z významného incidentu souvisejícího s IKT, které jsou dočasně zaneseny do přechodných nebo průběžných položek a nejsou dosud odraženy ve výsledovce a jejichž zahrnutí se plánuje ve lhůtě přiměřené velikosti a stáří nezaúčtované položky; iv) podstatné nezinkasované výnosy související se smluvními povinnostmi sjednanými s třetími stranami, včetně rozhodnutí poskytnout klientovi po závažném incidentu souvisejícím s IKT náhradu prostřednictvím úpravy výnosů formou zřeknutí se nebo snížení smluvních poplatků po určité budoucí období, a nikoli formou refundace nebo přímé platby; v) časově vázané ztráty, pokud zahrnují více než jeden rok finančního účetnictví a způsobují právní riziko. Finanční subjekty při posuzování přihlížejí k čl. 7 odst. 1 a 2 nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekty do tohoto čísla nezahrnou žádné finanční prostředky získané zpět. Finanční subjekty uvedou tuto peněžní částku jako kladnou hodnotu. V případě souhrnného hlášení podle článku 7 tohoto nařízení finanční subjekty zohlední celkovou výši nákladů a ztrát u všech finančních subjektů. Finanční subjekty uvedou tento datový bod v jednotkách s minimální přesností odpovídající tisícům jednotek.				
4.14	Výše zpětně získaných finančních prostředků	Celková výše zpětně získaných finančních prostředků. Zpětné získání finančních prostředků se vztahuje k původní ztrátě způsobené incidentem, a to nezávisle na okamžiku zpětného získání finančních prostředků ve formě financí nebo přílivu ekonomických přínosů.	Ne	Ne	Ano	Peněžní Finanční subjekty uvedou tento datový bod v jednotkách s minimální přesností odpovídající tisícům jednotek.

Datové pole	Popis	Povinné pro první oznámení	Povinné pro průběžnou zprávu	Povinné pro závěrečnou zprávu	Typ pole
	Finanční subjekty uvedou tuto peněžní částku jako kladnou hodnotu. V případě souhrnného hlášení podle článku 7 tohoto nařízení finanční subjekty zohlední celkovou výši zpětně získaných finančních prostředků u všech finančních subjektů.				
4.15 Informace o tom, zda se méně závažné incidenty opakují	Informace o tom, zda se opakovaně vyskytl více než jeden méně závažný incident související s IKT a zda se tyto incidenty společně považují za závažný incident ve smyslu čl. 8 odst. 2 nařízení v přenesené pravomoci (EU) 2024/1772. Finanční subjekty uvedou, zda se méně závažné incidenty související s IKT opakují a zda se společně považují za jeden závažný incident související s IKT. Finanční subjekty uvedou rovněž četnost výskytů těchto méně závažných incidentů souvisejících s IKT.	Ne	Ne	Ano, pokud závažný incident sestává z více než jednoho méně závažného opakujícího se incidentu.	Alfanumerické
4.16 Datum a čas výskytu opakujících se incidentů	Pokud finanční subjekty hlásí opakující se incidenty související s IKT, datum a čas, kdy došlo k prvnímu incidentu souvisejícímu s IKT.	Ne	Ne	Ano, v případě opakujících se incidentů	Koordinovaný světový čas (UTC) dle normy ISO 8601 (RRRR-MM-DD Thh: mm:ss)

([1]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Směrnice Evropského parlamentu a Rady 2014/59/EU ze dne 15. května 2014, kterou se stanoví rámec pro ozdravné postupy a řešení krize úvěrových institucí a investičních podniků a kterou se mění směrnice Rady 82/891/EHS, směrnice Evropského parlamentu a Rady 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU a 2013/36/EU a nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 a (EU) č. 648/2012 (Úř. věst. L 173, 12.6.2014, s. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Prováděcí nařízení Komise (EU) 2018/1624 ze dne 23. října 2018, kterým se podle směrnice Evropského parlamentu a Rady 2014/59/EU stanoví prováděcí technické normy, pokud jde o postupy, standardní formuláře a vzory k poskytování informací pro účely plánů řešení krize úvěrových institucí a investičních podniků, a zrušuje prováděcí nařízení Komise (EU) 2016/1066 (Úř. věst. L 277, 7.11.2018, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

PŘÍLOHA III

VZORY PRO OZNAMOVÁNÍ VÝZNAMNÝCH KYBERNETICKÝCH HROZEB

Číslo pole	Datové pole	
1	Název subjektu předkládajícího oznámení	
2	Identifikační kód subjektu předkládajícího oznámení	
3	Druh finančního subjektu předkládajícího oznámení	
4	Název finančního subjektu	
5	Kód LEI finančního subjektu	
6	Jméno hlavní kontaktní osoby	
7	E-mail hlavní kontaktní osoby	
8	Telefon hlavní kontaktní osoby	
9	Jméno druhé kontaktní osoby	
10	E-mail druhé kontaktní osoby	
11	Telefon druhé kontaktní osoby	
12	Datum a čas zjištění kybernetické hrozby	
13	Popis významné kybernetické hrozby	
14	Informace o potenciálním dopadu	
15	Potenciální kritéria klasifikace incidentu	
16	Stav kybernetické hrozby	
17	Opatření přijatá k zabránění naplnění hrozby	
18	Oznámení jiným zúčastněným stranám	
19	Ukazatele narušení	
20	Jiné relevantní informace	

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

PŘÍLOHA IV

DATOVÝ GLOSÁŘ A POKYNY PRO OZNAMOVÁNÍ VÝZNAMNÝCH KYBERNETICKÝCH HROZEB

Datové pole	Popis	Povinné pole	Typ pole
1. Název subjektu předkládajícího oznámení	Úplný právní název subjektu, který oznámení předkládá.	Ano	Alfanumerické
2. Identifikační kód subjektu předkládajícího oznámení	Identifikační kód subjektu, který oznámení předkládá. Pokud oznámení/zprávu předkládají finanční subjekty, identifikačním kódem je identifikační kód právnické osoby (LEI), což je jedinečný 20místný alfanumerický kód podle normy ISO 17442-1:2020. Pokud zprávu za finanční subjekt předkládá poskytovatel z řad třetích stran, může použít identifikační kód uvedený v prováděcích technických normách přijatých podle čl. 28 odst. 9 nařízení (EU) 2022/2554.	Ano	Alfanumerické
3. Druh finančního subjektu, který zprávu předkládá	Druh subjektu, který zprávu předkládá, podle čl. 2 odst. 1 písm. a) až t) nařízení (EU) 2022/2554.	Ano, pokud zprávu nepředkládá přímo dotčený finanční subjekt.	Výběr z možností (lze zvolit více možností): — úvěrová instituce, — platební instituce, — vyňatá platební instituce, — poskytovatel služeb informování o účtu, — instituce elektronických peněz, — vyňatá instituce elektronických peněz, — investiční podnik, — poskytovatel služeb souvisejících s kryptoaktivy, — vydavatel tokenů vázaných na aktiva, — centrální depozitář cenných papírů, — ústřední protistrana, — obchodní systém, — registr obchodních údajů, — správce alternativního investičního fondu, — správcovská společnost, — poskytovatel služeb hlášení údajů,

Datové pole		Popis	Povinné pole	Typ pole
				— pojišťovna a zajišťovna, — zprostředkovatel pojištění, zprostředkovatel zajištění a zprostředkovatel doplňkového pojištění, — instituce zaměstnaneckého penzijního pojištění, — ratingová agentura, — správce kritických referenčních hodnot, — poskytovatel služeb skupinového financování, — registr sekuritizací.
4.	Název finančního subjektu	Úplný právní název finančního subjektu, který významnou kybernetickou hrozbu oznamuje.	Ano, pokud je finanční subjekt odlišný od subjektu předkládajícího oznámení.	Alfanumerické
5.	Kód LEI finančního subjektu	Identifikátor právního subjektu (LEI) finančního subjektu, který významnou kybernetickou hrozbu oznamuje, přidělený podle Mezinárodní organizace pro normalizaci.	Ano, pokud je finanční subjekt oznamující významnou kybernetickou hrozbu odlišný od subjektu, který zprávu předkládá	Jedinečný 20místný alfanumerický kód podle normy ISO 17442-1:2020
6.	Jméno hlavní kontaktní osoby	Jméno a příjmení hlavní kontaktní osoby finančního subjektu.	Ano	Alfanumerické
7.	E-mail hlavní kontaktní osoby	E-mailová adresa hlavní kontaktní osoby, kterou může příslušný orgán použít pro následnou komunikaci.	Ano	Alfanumerické
8.	Telefon hlavní kontaktní osoby	Telefonní číslo hlavní kontaktní osoby, které může příslušný orgán použít pro následnou komunikaci. Telefonní číslo se uvádí se všemi mezinárodními předvolbami (např. +33XXXXXXXXX).	Ano	Alfanumerické
9.	Jméno druhé kontaktní osoby	Jméno a příjmení druhé kontaktní osoby finančního subjektu nebo subjektu, který oznámení jménem finančního subjektu předkládá, pokud je k dispozici.	Ano, pokud je k dispozici jméno a příjmení druhé kontaktní osoby finančního subjektu nebo subjektu, který oznámení za finanční subjekt předkládá	Alfanumerické

Datové pole		Popis	Povinné pole	Typ pole
10.	E-mail druhé kontaktní osoby	E-mailová adresa druhé kontaktní osoby nebo funkční e-mailová adresa týmu, kterou může příslušný orgán použít pro následnou komunikaci, pokud je k dispozici.	Ano, pokud je k dispozici e-mailová adresa druhé kontaktní osoby nebo funkční e-mailová adresa týmu, kterou může příslušný orgán použít pro následnou komunikaci	Alfanumerické
11.	Telefon druhé kontaktní osoby	Telefonní číslo druhé kontaktní osoby, které může příslušný orgán použít pro následnou komunikaci, pokud je k dispozici. Telefonní číslo se uvádí se všemi mezinárodními předvolbami (např. +33XXXXXXXXX).	Ano, pokud je k dispozici telefonní číslo druhé kontaktní osoby, které může příslušný orgán použít pro následnou komunikaci	Alfanumerické
12.	Datum a čas zjištění kybernetické hrozby	Datum a čas, kdy se finanční subjekt o významné kybernetické hrozbě dozvěděl.	Ano	Koordinovaný světový čas (UTC) dle normy ISO 8601 (RRRR-MM-DD Thh: mm:ss)
13.	Popis významné kybernetické hrozby	Popis nejdůležitějších aspektů významné kybernetické hrozby. Finanční subjekty uvedou: a) základní přehled nejdůležitějších aspektů významné kybernetické hrozby; b) související rizika, která z ní vyplývají, včetně potenciálních zranitelností systémů finančního subjektu, které mohou být zneužity; c) informace o pravděpodobnosti naplnění významné kybernetické hrozby a d) informace o zdroji informací o kybernetické hrozbě.	Ano	Alfanumerické
14.	Informace o potenciálním dopadu	Informace o potenciálním dopadu kybernetické hrozby na finanční subjekt, jeho klienty nebo finanční protistrany, pokud by se kybernetická hrozba naplnila.	Ano	Alfanumerické
15.	Potenciální kritéria klasifikace incidentu	Klasifikační kritéria, která by mohla vést k hlášení závažného incidentu, pokud by se kybernetická hrozba naplnila.	Ano	Výběr z možností (lze zvolit více možností): — dotčení klienti, finanční protistrany a transakce, — dopad na dobrou pověst, — doba trvání incidentu a doba odstávky služby, — územní rozsah, — ztráty údajů, — dotčené významné služby, — ekonomický dopad.

Datové pole	Popis	Povinné pole	Typ pole
16. Stav kybernetické hrozby	Informace o stavu kybernetické hrozby pro finanční subjekt a o tom, zda došlo ke změnám v její aktivitě. Pokud kybernetická hrozba přestala s informačními systémy finančního subjektu komunikovat, lze její stav označit jako neaktivní. Pokud má finanční subjekt informace o tom, že hrozba je nadále aktivní vůči jiným stranám nebo finančnímu systému jako celku, označí se její stav jako aktivní.	Ano	Výběr z možností: — aktivní — neaktivní
17. Opatření přijatá k zabránění naplnění hrozby	Základní informace o případných opatřeních, která finanční subjekt přijal, aby zabránil naplnění významných kybernetických hrozeb.	Ano	Alfanumerické
18. Oznámení jiným zúčastněným stranám	Informace o oznámení kybernetické hrozby jiným finančním subjektům nebo orgánům.	Ano, pokud byly o kybernetické hrozbě informovány jiné finanční subjekty nebo orgány	Alfanumerické
19. Ukazatele narušení	Případné informace týkající se závažné hrozby, které mohou přispět k identifikaci nepřátelské činnosti v síti nebo informačním systému (ukazatele narušení). Ukazatel narušení uvedený finančním subjektem může zahrnovat například tyto kategorie údajů: a) IP adresy; b) URL adresy; c) domény; d) hashe souborů; e) údaje o malwaru (název malwaru, názvy souborů a jejich umístění, konkrétní klíče registru spojené s činností malwaru); f) údaje o činnosti sítě (porty, protokoly, adresy, referery, řetězce user agent, hlavičky, konkrétní protokoly nebo charakteristické vzorce síťového provozu); g) údaje e-mailové zprávy (odesílatel, příjemce, předmět, záhlaví, obsah); h) požadavky systému DNS a konfigurace registru; i) činnosti uživatelských účtů (přihlašování, činnost privilegovaných uživatelských účtů, zvyšování oprávnění); j) databázový provoz (čtení/zápis), požadavky na stejný soubor. Tento druh informací může zahrnovat údaje týkající se ukazatelů, které popisují vzorce síťového provozu odpovídající známým útokům / komunikaci v rámci botnetu, IP adresy počítačů napadených malwarem (botů), údaje týkající se „řídicích a kontrolních“ serverů používaných malwarem (obvykle domény nebo IP adresy) a adresy URL související s phishingovými stránkami nebo webovými stránkami, na nichž byl pozorován malware nebo exploit kity.	Ano, pokud jsou k dispozici informace o ukazatelích narušení spojených s kybernetickou hrozbou	Alfanumerické
20. Jiné relevantní informace	Jakékoli další relevantní informace o významné kybernetické hrozbě	Ano, pokud je to relevantní a pokud jsou k dispozici další informace, které nejsou zahrnuty ve vzoru.	Alfanumerické

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj