Úradný vestník
Európskej únie

SK
Séria L

2025/302

20.2.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/302

z 23. októbra 2024,

ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a na oznamovanie významných kybernetických hrozieb

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 ([1]), a najmä na jeho článok 20 štvrtý odsek,

keďže:

(1) S cieľom zabezpečiť, aby finančné subjekty oznamovali závažné incidenty svojim príslušným orgánom konzistentným spôsobom a zabezpečiť, aby týmto orgánom poskytovali údaje dobrej kvality, by sa malo špecifikovať, ktoré dátové polia musia finančné subjekty poskytovať v rôznych fázach nahlasovania uvedeného v článku 19 ods. 4 nariadenia (EÚ) 2022/2554. Je dôležité, aby tieto informácie boli prezentované spôsobom, ktorý umožňuje jednotný prehľad o incidente. Je preto potrebné stanoviť na tieto účely jednotný vzor nahlasovania.

(2) Finančné subjekty by mali vyplniť tie dátové polia vzoru nahlasovania, ktoré zodpovedajú požiadavkám na informácie v príslušnom oznámení alebo správe. Finančné subjekty, ktoré už majú informácie, ktoré majú poskytnúť v neskoršej fáze nahlasovania, t. j. v priebežnej alebo záverečnej správe, by však mali mať možnosť predvídať predloženie údajov.

(3) Keďže viacnásobné alebo opakujúce sa incidenty môžu predstavovať závažný incident, ako sa uvádza v článku 8 delegovaného nariadenia Komisie (EÚ) 2024/1772 ([2]), návrh vzoru nahlasovania a dátových polí by mal finančným subjektom umožniť nahlasovanie takýchto opakujúcich sa incidentov.

(4) S cieľom zabezpečiť presné a aktuálne informácie by sa malo vo vzore nahlasovania umožniť finančným subjektom pri predkladaní priebežnej a záverečnej správy aktualizovať všetky predtým predložené informácie a v prípade potreby preklasifikovať závažné incidenty na menej závažné.

(5) Právna identifikácia subjektov by sa mala zosúladiť s identifikátormi uvedenými vo vykonávacích technických predpisoch prijatých podľa článku 28 ods. 9 nariadenia (EÚ) 2022/2554.

(6) Ak finančné subjekty zveria plnenie nahlasovacích povinností, pokiaľ ide o závažné incidenty súvisiace s IKT, tretej strane formou outsourcingu, príslušné orgány by mali poznať totožnosť nahlasujúcej tretej strany, ktorá podáva správy v mene finančného subjektu, ešte pred predložením prvého oznámenia alebo nahlásenia, aby mohli overiť legitímnosť nahlasujúcej tretej strany.

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

([2]) Delegované nariadenie Komisie (EÚ) 2024/1772 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch (Ú. v. EÚ L 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

(7) V záujme jednoduchej identifikácie vplyvu incidentu, ktorý sa vyskytol u externého poskytovateľa alebo bol spôsobený externým poskytovateľom a ktorý ovplyvňuje viacero finančných subjektov v rámci jedného členského štátu, a v záujme zníženia námahy finančných subjektov pri nahlasovaní by mal vzor nahlasovania umožniť predloženie súhrnnej správy obsahujúcej súhrnné informácie o vplyve incidentu na všetky ovplyvnené finančné subjekty, ktoré incident klasifikovali ako závažný.

(8) Vzor nahlasovania by mal byť navrhnutý technologicky neutrálne, aby ho bolo možné zaviesť do rôznych riešení na nahlasovanie incidentov, ktoré už existujú alebo ktoré môžu byť vyvinuté na účely vykonávania požiadaviek nariadenia (EÚ) 2022/2554.

(9) Návrh vzoru nahlasovania a dátových polí by mal uľahčiť nahlasovanie závažných incidentov súvisiacich s IKT tretími stranami, ktorým finančné subjekty zverili svoju nahlasovaciu povinnosť v súlade s článkom 19 ods. 5 nariadenia (EÚ) 2022/2554 formou outsourcingu.

(10) Toto nariadenie vychádza z návrhu vykonávacích technických predpisov, ktorý Komisii predložili európske orgány dohľadu.

(11) Európske orgány dohľadu uskutočnili otvorené verejné konzultácie k návrhu vykonávacích technických predpisov, z ktorého toto nariadenie vychádza, analyzovali možné súvisiace náklady a prínosy a požiadali o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade s článkom 37 nariadení Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([3]), (EÚ) č. 1094/2010 ([4]) a (EÚ) č. 1095/2010 ([5]).

(12) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([6]) sa uskutočnili konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 22. júla 2024 kladné stanovisko. Akékoľvek spracúvanie osobných údajov v rozsahu pôsobnosti tohto nariadenia by sa malo vykonávať v súlade s platnými zásadami ochrany údajov a ustanoveniami uvedenými v nariadení (EÚ) 2018/1725,

PRIJALA TOTO NARIADENIE:

Článok 1

Vzor nahlasovania závažných incidentov súvisiacich s IKT

1. Finančné subjekty použijú na predloženie počiatočného oznámenia, priebežnej správy a záverečnej správy uvedenej v článku 19 ods. 4 nariadenia (EÚ) 2022/2554 vzor stanovený v prílohe I takto:

a) finančné subjekty, ktoré predkladajú počiatočné oznámenie, vyplnia dátové polia vzoru, ktoré zodpovedajú informáciám, ktoré sa majú poskytnúť v súlade s článkom 2 delegovaného nariadenia Komisie (EÚ) 2025/301 ([7]), a ak už majú tieto informácie, môžu vyplniť tie dátové polia, ktorých vyplnenie sa nevyžaduje pre počiatočné oznámenie, ale vyžaduje sa pre priebežnú alebo záverečnú správu;

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Delegované nariadenie Komisie (EÚ) 2025/301 z 23. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb. (Ú. v. EÚ L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) finančné subjekty, ktoré predkladajú priebežnú správu, vyplnia dátové polia vzoru, ktoré zodpovedajú informáciám, ktoré sa majú poskytnúť v súlade s článkom 3 delegovaného nariadenia (EÚ) 2025/301, a ak už majú príslušné informácie, môžu vyplniť dátové polia, ktorých vyplnenie sa nevyžaduje pre priebežnú správu, ale vyžaduje sa pre záverečnú správu;

c) finančné subjekty, ktoré predkladajú záverečnú správu, vyplnia dátové polia vzoru, ktoré zodpovedajú informáciám, ktoré sa majú poskytnúť v súlade s článkom 4 delegovaného nariadenia (EÚ) 2025/301.

2. Finančné subjekty zabezpečia, aby informácie uvedené v počiatočnom oznámení a v priebežnej a záverečnej správe boli úplné a presné.

3. Finančné subjekty poskytujú odhadované hodnoty založené na iných dostupných údajoch a informáciách v rozsahu, v akom je to možné, ak v čase nahlasovania počiatočného oznámenia alebo priebežnej správy nie sú k dispozícii presné údaje.

4. Pri predkladaní priebežnej alebo záverečnej správy finančné subjekty použijú vzor stanovený v prílohe I na predloženie všetkých požadovaných informácií a v prípade potreby aktualizujú informácie, ktoré boli predtým poskytnuté v počiatočnom oznámení alebo v priebežnej správe.

5. Finančné subjekty pri vypĺňaní vzoru uvedeného v prílohe I postupujú podľa slovníka údajov a pokynov uvedených v prílohe II.

Článok 2

Spoločné predkladanie počiatočného oznámenia, priebežných a záverečných správ

Finančné subjekty môžu skombinovať predloženie počiatočného oznámenia, priebežnej správy a záverečnej správy a predložiť dve alebo všetky tieto správy súčasne, ak sa obnovili pravidelné činnosti alebo sa ukončila analýza základných príčin a za predpokladu, že sa dodržia lehoty stanovené v článku 5 delegovaného nariadenia (EÚ) 2025/301.

Článok 3

Opakujúce sa incidenty súvisiace s IKT

Finančné subjekty, ktoré poskytujú informácie o iných ako závažných opakujúcich sa incidentoch súvisiacich s IKT, ktoré kumulatívne spĺňajú podmienky jedného závažného incidentu súvisiaceho s IKT, ako sa stanovuje v článku 8 ods. 2 delegovaného nariadenia (EÚ) 2024/1772, poskytujú tieto informácie v súhrnnej forme.

Článok 4

Používanie zabezpečených elektronických kanálov

1. Finančné subjekty používajú na predkladanie počiatočného oznámenia a priebežných a záverečných správ zabezpečené elektronické kanály, ktoré im sprístupní ich príslušný orgán.

2. Finančné subjekty, ktoré nemôžu používať zabezpečené elektronické kanály sprístupnené ich príslušným orgánom, informujú svoj príslušný orgán o závažnom incidente súvisiacom s IKT inými bezpečnými prostriedkami po dohode s príslušným orgánom. Ak to požaduje príslušný orgán, finančné subjekty opätovne predložia počiatočné oznámenie alebo priebežnú či záverečnú správu prostredníctvom zabezpečeného elektronického kanála, ktorý im sprístupní ich príslušný orgán, keď tak budú môcť urobiť.

Článok 5

Zmena klasifikácie závažných incidentov súvisiacich s IKT

Ak po ďalšom posúdení finančný subjekt dospeje k záveru, že incident súvisiaci s IKT, ktorý bol predtým nahlásený ako závažný, v žiadnom prípade nespĺňal klasifikačné kritériá a prahové hodnoty stanovené v článku 8 delegovaného nariadenia (EÚ) 2024/1772, finančný subjekt oznámi príslušnému orgánu, že zmenil klasifikáciu incidentu súvisiaceho s IKT zo závažného na menej závažný, a to poskytnutím informácií o tejto zmene klasifikácie vo vzore stanovenom v prílohe II k tomuto nariadeniu v súvislosti s poľami „typ správy“ a „iné informácie“.

Článok 6

Oznámenie o zabezpečovaní nahlasovacích povinností formou outsourcingu

1. Finančné subjekty, ktoré si zabezpečili povinnosť nahlasovať závažné incidenty súvisiace s IKT v súlade s článkom 19 ods. 5 nariadenia (EÚ) 2022/2554 formou outsourcingu, informujú svoj príslušný orgán o tejto dohode o outsourcingu hneď po jej uzavretí a najneskôr pred prvým oznámením alebo nahlasovaním.

2. Finančné subjekty poskytnú príslušnému orgánu názov, kontaktné údaje a identifikačný kód tretej strany, ktorá za ne bude predkladať oznámenia alebo správy o závažných incidentoch súvisiacich s IKT.

3. Finančné subjekty informujú svoj príslušný orgán hneď, ako prestanú zabezpečovať formou outsourcingu svoje nahlasovacie povinnosti uvedené v článku 19 ods. 5 nariadenia (EÚ) 2022/2554.

Článok 7

Súhrnné nahlasovanie

1. Poskytovateľ služieb, ktorý je treťou stranou a na ktorého boli na základe outsourcingu prenesené nahlasovacie povinnosti, ako sa uvádza v článku 19 ods. 5 nariadenia (EÚ) 2022/2554, môže použiť vzor uvedený v prílohe I k tomuto nariadeniu na poskytnutie súhrnných informácií o závažnom incidente súvisiacom s IKT, ktorý má vplyv na viacero finančných subjektov, v jednom oznámení alebo správe a predložiť toto oznámenie alebo správu príslušnému orgánu v mene všetkých ovplyvnených finančných subjektov za predpokladu, že sú splnené všetky tieto podmienky:

a) závažný incident súvisiaci s IKT, ktorý sa má nahlásiť, pochádza od externého poskytovateľa IKT služieb alebo je ním spôsobený;

b) že externý poskytovateľ služieb poskytuje príslušnú IKT službu viac ako jednému finančnému subjektu alebo skupine;

c) každý finančný subjekt, ktorého sa týka súhrnné oznámenie alebo správa, klasifikuje incident súvisiaci s IKT ako závažný;

d) závažný incident súvisiaci s IKT sa týka finančných subjektov v jednom členskom štáte a súhrnná správa sa vzťahuje na finančné subjekty, nad ktorými vykonáva dohľad ten istý príslušný orgán;

e) príslušné orgány výslovne povolili tomuto typu finančných subjektov agregovať svoje správy.

2. Odsek 1 sa neuplatňuje na úverové inštitúcie, ktoré sa považujú za významné, ako sa uvádza v článku 2 bode 16 nariadenia Európskej centrálnej banky (EÚ) č. 468/2014 ([8]), prevádzkovateľov obchodných miest a centrálne protistrany, ktoré používajú vzor uvedený v prílohe I len na individuálne predkladanie oznámení alebo správ o závažných incidentoch súvisiacich s IKT svojmu príslušnému orgánu.

3. Ak príslušné orgány požadujú informácie o individuálnom vplyve závažného incidentu súvisiaceho s IKT na jeden finančný subjekt, finančný subjekt na žiadosť príslušného orgánu predloží individuálne oznámenie alebo správu o závažnom incidente súvisiacom s IKT.

([8]) Nariadenie Európskej centrálnej banky (EÚ) č. 468/2014 zo 16. apríla 2014 o rámci pre spoluprácu v rámci jednotného mechanizmu dohľadu medzi Európskou centrálnou bankou, príslušnými vnútroštátnymi orgánmi a určenými vnútroštátnymi orgánmi (nariadenie o rámci JMD) (ECB/2014/17) (Ú. v. EÚ L 141, 14.5.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Článok 8

Oznamovanie významných kybernetických hrozieb

1. Finančné subjekty, ktoré oznamujú významné kybernetické hrozby príslušným orgánom v súlade s článkom 19 ods. 2 nariadenia (EÚ) 2022/2554, používajú vzor stanovený v prílohe III k tomuto nariadeniu a dodržiavajú slovník údajov a pokyny stanovené v prílohe IV k tomuto nariadeniu.

2. Finančné subjekty zabezpečia, aby informácie uvedené v oznámení o významných kybernetických hrozbách boli úplné a presné.

Článok 9

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 23. októbra 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA I

VZORY NA NAHLASOVANIE ZÁVAŽNÝCH INCIDENTOV

Číslo poľa	Dátové pole	
Všeobecné informácie o finančnom subjekte		
1.1	Typ predloženia	
1.2	Názov subjektu, ktorý predkladá správu	
1.3	Identifikačný kód subjektu, ktorý predkladá správu	
1.4	Typ ovplyvneného finančného subjektu	
1.5	Názov ovplyvneného finančného subjektu	
1.6	Identifikátor právneho subjektu ovplyvneného finančného subjektu	
1.7	Meno hlavnej kontaktnej osoby	
1.8	E-mail: hlavnej kontaktnej osoby	
1.9	Telefón hlavnej kontaktnej osoby	
1.10	Meno druhej kontaktnej osoby	
1.11	E-mail: druhej kontaktnej osoby	
1.12	Telefón druhej kontaktnej osoby	
1.13	Názov hlavného materského podniku	
1.14	Identifikátor právneho subjektu hlavného materského podniku	
1.15	Mena vykazovania	
Obsah počiatočného oznámenia		
2.1	Referenčný kód incidentu pridelený finančným subjektom	
2.2	Dátum a čas zistenia závažného incidentu súvisiaceho s IKT	
2.3	Dátum a čas klasifikácie incidentu súvisiaceho s IKT ako závažného	
2.4	Opis závažného incidentu súvisiaceho s IKT	
2.5	Klasifikačné kritériá, ktoré viedli k nahláseniu incidentu	
2.6	Prahové hodnoty významnosti pre klasifikačné kritérium „geografické rozloženie“	
2.7	Zistenie závažného incidentu súvisiaceho s IKT	

Číslo poľa	Dátové pole	
2.8	Údaj o tom, či závažný incident súvisiaci s IKT pochádza od externého poskytovateľa alebo iného finančného subjektu	
2.9	Aktivácia plánu kontinuity činnosti, ak je aktivovaný	
2.10	Ďalšie relevantné informácie	
Obsah priebežnej správy		
3.1	Referenčný kód incidentu poskytnutý príslušným orgánom	
3.2	Dátum a čas výskytu závažného incidentu súvisiaceho s IKT	
3.3	Dátum a čas obnovenia služieb, činností alebo operácií	
3.4	Počet ovplyvnených klientov	
3.5	Percentuálny podiel ovplyvnených klientov	
3.6	Počet ovplyvnených finančných protistrán	
3.7	Percentuálny podiel ovplyvnených finančných protistrán	
3.8	Vplyv na príslušných klientov alebo finančné protistrany	
3.9	Počet ovplyvnených transakcií	
3.10	Percentuálny podiel ovplyvnených transakcií	
3.11	Hodnota ovplyvnených transakcií	
3.12	Informácie o tom, či ide o skutočné čísla alebo odhady, alebo či nedošlo k žiadnemu vplyvu	
3.13	Vplyv na dobré meno	
3.14	Kontextové informácie o vplyve na dobré meno	
3.15	Trvanie závažného incidentu súvisiaceho s IKT	
3.16	Výpadok služby	
3.17	Informácie o tom, či sú údaje o dĺžke trvania a čase výpadku služby skutočné alebo odhadované	
3.18	Typy vplyvu v členských štátoch	
3.19	Opis toho, aký vplyv má závažný incident súvisiaci s IKT na ostatné členské štáty.	
3.20	Prahové hodnoty významnosti pre klasifikačné kritérium „straty údajov“	
3.21	Opis strát údajov	

Číslo poľa	Dátové pole	
3.22	Klasifikačné kritérium „kritickosť zasiahnutých služieb“	
3.23	Typ závažného incidentu súvisiaceho s IKT	
3.24	Iné typy incidentov	
3.25	Hrozby a techniky používané aktérom hrozby	
3.26	Iné typy techník	
3.27	Informácie o ovplyvnených funkčných oblastiach a obchodných procesoch	
3.28	Ovplyvnené zložky infraštruktúry podporujúce obchodné procesy	
3.29	Informácie o ovplyvnených zložkách infraštruktúry podporujúcich obchodné procesy	
3.30	Vplyv na finančné záujmy klientov	
3.31	Nahlasovanie iným orgánom	
3.32	Špecifikácia „iných“ orgánov	
3.33	Dočasné kroky/opatrenia, ktoré sa prijali alebo sa plánujú prijať na obnovu po incidente	
3.34	Opis všetkých dočasných činností a opatrení, ktoré sa prijali alebo sa plánujú prijať na obnovu po incidente	
3.35	Ukazovatele ohrozenia	
Obsah záverečnej správy		
4.1	Klasifikácia hlavných príčin incidentu na vysokej úrovni	
4.2	Podrobná klasifikácia hlavných príčin incidentu	
4.3	Dodatočná klasifikácia hlavných príčin incidentu	
4.4	Iné typy hlavných príčin	
4.5	Informácie o hlavných príčinách incidentu	
4.6	Zhrnutie riešenia incidentu	
4.7	Dátum a čas, kedy sa riešila hlavná príčina incidentu	
4.8	Dátum a čas vyriešenia incidentu	
4.9	Informácie, ak sa dátum trvalého riešenia incidentu líši od pôvodne plánovaného dátumu vykonania	
4.10	Posúdenie rizika pre zásadné funkcie na účely riešenia incidentov	
4.11	Informácie relevantné pre orgány pre riešenie krízových situácií	

Číslo poľa	Dátové pole	
4.12	Prahová hodnota významnosti pre klasifikačné kritérium „hospodársky vplyv“	
4.13	Výška hrubých priamych a nepriamych nákladov a strát	
4.14	Výška vrátených finančných prostriedkov	
4.15	Informácie o tom, či sa incidenty, ktoré nie sú závažné, opakujú	
4.16	Dátum a čas výskytu opakujúcich sa incidentov	

PRÍLOHA II

SLOVNÍK ÚDAJOV A POKYNY NA NAHLASOVANIE ZÁVAŽNÝCH INCIDENTOV

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
Všeobecné informácie o finančnom subjekte					
1.1. Typ predloženia	Uveďte typ oznámenia o incidente alebo správy, ktorá sa predkladá príslušnému orgánu.	Áno	Áno	Áno	Pole s možnosťou výberu: — počiatočné oznámenie; — priebežná správa; — záverečná správa; — závažný incident preklasifikovaný na menej závažný.
1.2. Názov subjektu, ktorý predkladá správu	Úplný právny názov subjektu, ktorý predkladá správu.	Áno	Áno	Áno	Alfanumerické
1.3. Identifikačný kód subjektu, ktorý predkladá správu	Identifikačný kód subjektu, ktorý predkladá správu. Ak finančné subjekty predkladajú oznámenie/správu, identifikačným kódom je identifikátor právneho subjektu (LEI), čo je jedinečný 20-miestny alfanumerický kód podľa normy ISO 17442-1:2020. Externý poskytovateľ, ktorý predkladá správu za finančný subjekt, môže použiť identifikačný kód uvedený vo vykonávacích technických predpisoch prijatých podľa článku 28 ods. 9 nariadenia (EÚ) 2022/2554.	Áno	Áno	Áno	Alfanumerické
1.4. Typ ovplyvnených finančného subjektu	Typ subjektu podľa článku 2 ods. 1 písm. a) až t) nariadenia (EÚ) 2022/2554, za ktorý sa správa predkladá. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia sa vyberú rôzne typy finančných subjektov, na ktoré sa súhrnná správa vzťahuje.	Áno	Áno	Áno	Pole s možnosťou výberu (viacnásobný výber): — úverová inštitúcia; — platobná inštitúcia; — oslobodená platobná inštitúcia; — poskytovateľ služieb informovania o účte; — inštitúcia elektronického peňažníctva; — oslobodená inštitúcia elektronického peňažníctva; — investičná spoločnosť; — poskytovateľ služieb kryptoaktív; — emitent tokenov naviazaných na aktíva; — centrálny depozitár cenných papierov; — centrálna protistrana, — obchodné miesto; — archív obchodných údajov;

Dátové pole		Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
						— správca alternatívneho investičného fondu; — správcovská spoločnosť; — poskytovateľ služieb vykazovania údajov; — poisťovňa a zaisťovňa; — sprostredkovateľ poistenia; sprostredkovateľ zaistenia a sprostredkovateľ doplnkového poistenia; — inštitúcia zamestnaneckého dôchodkového zabezpečenia; — ratingová agentúra, — správca kritických referenčných hodnôt; — poskytovateľ služieb hromadného financovania; — archív sekuritizačných údajov.
1.5.	Názov ovplyvneného finančného subjektu	Úplný právny názov finančného subjektu, ktorý je ovplyvnený závažným incidentom súvisiacim s IKT a ktorý je povinný nahlásiť závažný incident svojmu príslušnému orgánu podľa článku 19 nariadenia (EÚ) 2022/2554. V prípade súhrnného nahlasovania: a) zoznam všetkých názvov finančných subjektov, ktoré sú ovplyvnené závažným incidentom súvisiacim s IKT, oddelených bodkočiarkou; b) externý poskytovateľ, ktorý predkladá oznámenie alebo správu o závažnom incidente, alebo súhrnne, ako sa uvádza v článku 7 tohto nariadenia, uvedie názvy všetkých finančných subjektov, ktorých sa incident týka, oddelené bodkočiarkou.	Áno, ak je finančný subjekt, ktorý je ovplyvnený incidentom, odlišný od subjektu, ktorý predkladá správu, a v prípade súhrnného nahlasovania.	Áno, ak je finančný subjekt, ktorý je ovplyvnený incidentom, odlišný od subjektu, ktorý predkladá správu, a v prípade súhrnného nahlasovania.	Áno, ak je finančný subjekt, ktorý je ovplyvnený incidentom, odlišný od subjektu, ktorý predkladá správu, a v prípade súhrnného nahlasovania.	Alfanumerické
1.6.	Identifikátor právneho subjektu ovplyvneného finančného subjektu	Identifikátor právneho subjektu (LEI) finančného subjektu, ktorý je ovplyvnený závažným incidentom súvisiacim s IKT, pridelený v súlade s Medzinárodnou organizáciou pre normalizáciu. V prípade súhrnného nahlasovania: a) zoznam všetkých identifikátorov právneho subjektu finančných subjektov, ktoré sú ovplyvnené závažným incidentom súvisiacim s IKT, oddelených bodkočiarkou;	Áno, ak je finančný subjekt, ktorý je ovplyvnený závažným incidentom súvisiacim s IKT, odlišný	Áno, ak je finančný subjekt, ktorý je ovplyvnený závažným incidentom súvisiacim s IKT, odlišný od subjektu,	Áno, ak je finančný subjekt, ktorý je ovplyvnený závažným incidentom súvisiacim s IKT, odlišný	Jedinečný 20-miestny alfanumerický kód podľa normy ISO 17442-1:2020

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	b) externý poskytovateľ, ktorý predkladá oznámenie alebo správu o závažnom incidente, alebo súhrnne, ako sa uvádza v článku 7 tohto nariadenia, má uviesť identifikátory právneho subjektu všetkých finančných subjektov, ktoré sú ovplyvnené incidentom, oddelené bodkočiarkou. Poradie výskytu identifikátorov právneho subjektu a názvov finančných subjektov musí byť rovnaké.	od subjektu, ktorý predkladá správu, a v prípade súhrnného nahlasovania.	ktorý predkladá správu, a v prípade súhrnného nahlasovania.	od subjektu, ktorý predkladá správu, a v prípade súhrnného nahlasovania	
1.7. Meno hlavnej kontaktnej osoby	Meno a priezvisko hlavnej kontaktnej osoby finančného subjektu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia meno hlavnej kontaktnej osoby v subjekte, ktorý predkladá súhrnnú správu.	Áno	Áno	Áno	Alfanumerické
1.8. E-mail: hlavnej kontaktnej osoby	E-mailová adresa hlavnej kontaktnej osoby, ktorú môže príslušný orgán použiť na následnú komunikáciu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia e-mail: hlavnej kontaktnej osoby v subjekte, ktorý predkladá súhrnnú správu.	Áno	Áno	Áno	Alfanumerické
1.9. Telefón hlavnej kontaktnej osoby	Telefónne číslo hlavnej kontaktnej osoby, ktoré môže príslušný orgán použiť na následnú komunikáciu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia telefónne číslo hlavnej kontaktnej osoby v subjekte, ktorý predkladá súhrnnú správu. Telefónne číslo sa uvádza so všetkými medzinárodnými predvoľbami (napr. +33XXXXXXXXX)	Áno	Áno	Áno	Alfanumerické
1.10. Meno druhej kontaktnej osoby	Meno a priezvisko druhej kontaktnej osoby alebo názov zodpovedného tímu finančného subjektu alebo subjektu, ktorý predkladá správu v mene finančného subjektu	Áno	Áno	Áno	Alfanumerické
1.11. E-mail: druhej kontaktnej osoby	E-mailová adresa druhej kontaktnej osoby alebo funkčná e-mailová adresa tímu, ktorú môže príslušný orgán použiť na následnú komunikáciu.	Áno	Áno	Áno	Alfanumerické

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

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
1.12. Telefón druhej kontaktnej osoby	Telefónne číslo druhej kontaktnej osoby alebo tímu, ktoré môže príslušný orgán použiť na následnú komunikáciu. Telefónne číslo sa uvádza so všetkými medzinárodnými predvoľbami (napr. +33XXXXXXXXX)	Áno	Áno	Áno	Alfanumerické
1.13. Názov hlavného materského podniku	Názov hlavného materského podniku skupiny, do ktorej patrí ovplyvnený finančný subjekt, v náležitých prípadoch.	Áno, ak finančný subjekt patrí do skupiny.	Áno, ak finančný subjekt patrí do skupiny.	Áno, ak finančný subjekt patrí do skupiny.	Alfanumerické
1.14. Identifikátor právneho subjektu hlavného materského podniku	Identifikátor právneho subjektu hlavného materského podniku skupiny, do ktorej patrí ovplyvnený finančný subjekt, v náležitých prípadoch. Priradený v súlade s Medzinárodnou organizáciou pre normalizáciu.	Áno, ak finančný subjekt patrí do skupiny.	Áno, ak finančný subjekt patrí do skupiny.	Áno, ak finančný subjekt patrí do skupiny.	Jedinečný 20-miestny alfanumerický kód podľa normy ISO 17442-1:2020.
1.15. Mena vykazovania	Mena používaná pri nahlasovaní incidentov	Áno	Áno	Áno	Pole s možnosťou výberu vyplnené pomocou kódov mien podľa normy ISO 4217
Obsah počiatočného oznámenia					
2.1. Referenčný kód incidentu pridelený finančným subjektom	Jedinečný referenčný kód vydaný finančným subjektom, ktorý jednoznačne identifikuje závažný incident súvisiaci s IKT. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia referenčný kód incidentu pridelený externým poskytovateľom.	Áno	Áno	Áno	Alfanumerické
2.2. Dátum a čas zistenia incidentu súvisiaceho s IKT	Dátum a čas, kedy sa finančný subjekt dozvedel o incidente súvisiacom s IKT. V prípade opakujúcich sa incidentov dátum a čas, kedy bol zistený posledný incident súvisiaci s IKT.	Áno	Áno	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
2.3. Dátum a čas klasifikácie incidentu ako závažného	Dátum a čas, kedy bol incident súvisiaci s IKT klasifikovaný ako závažný podľa klasifikačných kritérií stanovených v delegovanom nariadení (EÚ) 2024/1772.	Áno	Áno	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)
2.4. Opis incidentu súvisiaceho s IKT	Opis najdôležitejších aspektov závažného incidentu súvisiaceho s IKT. Finančné subjekty poskytnú prehľad na vysokej úrovni o nasledujúcich informáciách, ako sú možné príčiny, bezprostredné vplyvy, ovplyvnené systémy a iné. Finančné subjekty zahrnú, ak sú známe alebo sa odôvodnene predpokladá, že incident má vplyv na externých poskytovateľov alebo iné finančné subjekty, typ poskytovateľa alebo finančného subjektu, ich názov, príslušné identifikačné kódy a typ identifikačného kódu (napr. LEI alebo EUID). V ďalších správach sa obsah polí môže časom vyvíjať tak, aby sa zohľadňovalo priebežné chápanie incidentu súvisiaceho s IKT a opisovali sa akékoľvek ďalšie relevantné informácie o incidente súvisiacom s IKT, ktoré nie sú zachytené v dátových poliach, vrátane interného hodnotenia závažnosti zo strany finančného subjektu (napr. veľmi nízka, nízka, stredná, vysoká, veľmi vysoká) a uviedla sa úroveň a názov najvyšších rozhodovacích štruktúr, ktoré boli zapojené do reakcie na incident súvisiaci s IKT.	Áno	Áno	Áno	Alfanumerické
2.5. Klasifikačné kritériá, ktoré viedli k nahláseniu incidentu	Klasifikačné kritériá podľa delegovaného nariadenia (EÚ) 2024/1772, na základe ktorých sa incident súvisiaci s IKT určil ako závažný a následne sa oznámil a nahlásil. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia klasifikačné kritériá, na základe ktorých sa incident súvisiaci s IKT určil ako závažný aspoň pre jeden alebo viac finančných subjektov.	Áno	Áno	Áno	Pole s možnosťou výberu (viac možností): — klienti, finančné protistrany a transakcie ovplyvnené incidentom; — vplyv na dobré meno; — trvanie incidentu súvisiaceho s IKT a výpadok služby; — geografické rozloženie; — straty údajov; — kritickosť zasiahnutých služieb; — hospodársky vplyv.
2.6. Prahové hodnoty významnosti pre klasifikačné kritérium „geografické rozloženie“	Členské štáty EHP ovplyvnené závažným incidentom súvisiacim s IKT Pri posudzovaní vplyvu závažného incidentu súvisiaceho s IKT v iných členských štátoch finančné subjekty zohľadňujú články 4 a 12 delegovaného nariadenia (EÚ) 2024/1772.	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“.	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“.	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“.	Pole s možnosťou výberu (viac možností) vyplnené po použití ISO 3166 ALPHA-2 dotknutých krajín

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
2.7. Zistenie závažného incidentu súvisiaceho s IKT	Údaj o tom, ako bol zistený závažný incident súvisiaci s IKT.	Áno	Áno	Áno	Pole s možnosťou výberu: — bezpečnosť informačných technológií; — zamestnanci; — vnútorný audit; — externý audit; — klienti; — finančné protistrany; — externý poskytovateľ; — útočník; — systémy monitorovania; — orgán/agentúra/orgán presadzovania práva; — iné.
2.8. Údaj o tom, či incident pochádza od externého poskytovateľa alebo iného finančného subjektu	Údaj o tom, či závažný incident súvisiaci s IKT pochádza od externého poskytovateľa alebo iného finančného subjektu. Finančné subjekty uvedú, či závažný incident súvisiaci s IKT pochádza od externého poskytovateľa alebo iného finančného subjektu (vrátane finančných subjektov patriacich do rovnakej skupiny ako nahlasujúci subjekt), a názov, identifikačný kód externého poskytovateľa alebo finančného subjektu a typ identifikačného kódu (napr. LEI alebo EUID).	Áno, ak incident pochádza od externého poskytovateľa alebo iného finančného subjektu	Áno, ak incident pochádza od externého poskytovateľa alebo iného finančného subjektu	Áno, ak incident pochádza od externého poskytovateľa alebo iného finančného subjektu	Alfanumerické
2.9. Aktivácia plánu kontinuity činnosti, ak je aktivovaný	Údaj o tom, či došlo k formálnej aktivácii opatrení na zabezpečenie kontinuity činností finančného subjektu.	Áno	Áno	Áno	Booleovské (áno alebo nie)
2.10. Ďalšie relevantné informácie	Akékoľvek ďalšie informácie, ktoré nie sú uvedené vo vzore. Finančné subjekty, ktoré preklasifikovali závažný incident súvisiaci s IKT na iný ako závažný, opíšu dôvody, prečo incident súvisiaci s IKT nespĺňa a ani sa neočakáva, že bude spĺňať kritériá na to, aby sa považoval za závažný incident súvisiaci s IKT.	Áno, ak existujú ďalšie informácie, ktoré nie sú zahrnuté vo	Áno, ak existujú ďalšie informácie, ktoré nie sú zahrnuté vo vzore, alebo ak bol	Áno, ak existujú ďalšie informácie, ktoré nie sú zahrnuté vo	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
		vzore, alebo ak bol závažný incident súvisiaci s IKT preklasifikovaný na menej závažný.	závažný incident súvisiaci s IKT preklasifikovaný na menej závažný	vzore, alebo ak bol závažný incident súvisiaci s IKT preklasifikovaný na menej závažný	
Obsah priebežnej správy					
3.1. Referenčný kód incidentu poskytnutý príslušným orgánom	Jedinečný referenčný kód pridelený príslušným orgánom v čase prijatia prvého oznámenia na jednoznačnú identifikáciu závažného incidentu súvisiaceho s IKT.	Nie	Áno, ak sa uplatňuje	Áno, ak sa uplatňuje	Alfanumerické
3.2. Dátum a čas výskytu incidentu	Dátum a čas, kedy došlo k závažnému incidentu súvisiacemu s IKT, ak sa líši od času, kedy sa finančný subjekt dozvedel o závažnom incidente súvisiacom s IKT. V prípade opakujúcich sa závažných incidentov súvisiacich s IKT dátum a čas, kedy došlo k poslednému závažnému incidentu súvisiacemu s IKT.	Nie	Áno	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)
3.3. Dátum a čas obnovenia služieb, činností alebo operácií	Informácie o dátume a čase obnovenia služieb, činností alebo operácií ovplyvnených závažným incidentom súvisiacim s IKT.	Nie	Áno, ak bolo dátové pole 3.16. „Výpadok služby“ vyplnené	Áno, ak bolo dátové pole 3.16. „Výpadok služby“ vyplnené	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)
3.4. Počet ovplyvnených klientov	Počet klientov ovplyvnených závažným incidentom súvisiacim s IKT, ktorí využívajú služby poskytované finančným subjektom. Pri posudzovaní počtu ovplyvnených klientov finančné subjekty prihliadajú na článok 1 ods. 1 a článok 9 ods. 1 písm. b) delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nedokáže určiť skutočný počet dotknutých klientov, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia celkový počet ovplyvnených klientov vo všetkých finančných subjektoch.	Nie	Áno	Áno	Celé číslo

Dátové pole		Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.5.	Percentuálny podiel ovplyvnených klientov	Percentuálny podiel klientov ovplyvnených závažným incidentom súvisiacim s IKT vo vzťahu k celkovému počtu klientov, ktorí využívajú ovplyvnené služby poskytované finančným subjektom. V prípade viacerých ovplyvnených služieb sa služby poskytujú súhrnne. Finančné subjekty pri posudzovaní zohľadňujú článok 1 ods. 1 a článok 9 ods. 1 písm. a) delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nedokáže určiť skutočný percentuálny podiel ovplyvnených klientov, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančný subjekt vydelí súčet všetkých ovplyvnených klientov celkovým počtom klientov všetkých ovplyvnených finančných subjektov.	Nie	Áno	Áno	Vyjadrené ako percentuálny podiel – akákoľvek hodnota najviac s piatimi číselnými znakmi vrátane najviac jedného desatinného miesta vyjadrená ako percentuálny podiel (napr. 2,4 namiesto 2,4 %). Ak má hodnota po desatinnej čiarke viac ako jednu číslicu, nahlasujúce protistrany posledné miesto zaokrúhlia smerom nahor.
3.6.	Počet ovplyvnených finančných protistrán	Počet finančných protistrán, ktoré boli ovplyvnené závažným incidentom súvisiacim s IKT a ktoré uzavreli zmluvu s finančným subjektom. Pri posudzovaní počtu ovplyvnených finančných protistrán finančné subjekty prihliadajú na článok 1 ods. 2 delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nedokáže určiť skutočný počet ovplyvnených finančných protistrán, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia celkový počet ovplyvnených finančných protistrán vo všetkých finančných subjektoch.	Nie	Áno	Áno	Celé číslo

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.7. Percentuálny podiel ovplyvnených finančných protistrán	Percentuálny podiel finančných protistrán ovplyvnených závažným incidentom súvisiacim s IKT vo vzťahu k celkovému počtu finančných protistrán, ktoré uzavreli zmluvu s finančným subjektom. Pri posudzovaní percentuálneho podielu ovplyvnených finančných protistrán finančné subjekty prihliadajú na článok 1 ods. 1 a článok 9 ods. 1 písm. c) delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nedokáže určiť skutočný percentuálny podiel ovplyvnených finančných protistrán, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia uveďte súčet všetkých ovplyvnených finančných protistrán vydelený celkovým počtom finančných protistrán všetkých ovplyvnených finančných subjektov.	Nie	Áno	Áno	Vyjadrené ako percentuálny podiel – akákoľvek hodnota najviac s piatimi číselnými znakmi vrátane najviac jedného desatinného miesta vyjadrená ako percentuálny podiel (napr. 2,4 namiesto 2,4 %). Ak má hodnota po desatinnej čiarke viac ako jednu číslicu, nahlasujúce protistrany posledné miesto zaokrúhlia smerom nahor.
3.8. Vplyv na príslušných klientov alebo finančné protistrany	Akýkoľvek zistený vplyv na príslušných klientov alebo finančné protistrany, ako sa uvádza v článku 1 ods. 3 a článku 9 ods. 1 písm. f) delegovaného nariadenia (EÚ) 2024/1772.	Nie	Áno, ak je splnená prahová hodnota kritéria „relevantnosť klientov a finančných protistrán“	Áno, ak je splnená prahová hodnota kritéria „relevantnosť klientov a finančných protistrán“	Booleovské (áno alebo nie)
3.9. Počet ovplyvnených transakcií	Počet transakcií ovplyvnených závažným incidentom súvisiacim s IKT. Pri posudzovaní vplyvu na transakcie finančné subjekty zohľadňujú článok 1 ods. 4 delegovaného nariadenia (EÚ) 2024/1772 vrátane všetkých ovplyvnených domácich a cezhraničných transakcií obsahujúcich peňažnú sumu, ktoré majú aspoň jednu časť transakcie vykonanú v Únii.	Nie	Áno, ak incident ovplyvnil nejakú transakciu	Áno, ak incident ovplyvnil nejakú transakciu	Celé číslo

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	Finančný subjekt, ktorý nedokáže určiť skutočný počet ovplyvnených transakcií, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia uviesť celkový počet ovplyvnených transakcií vo všetkých finančných subjektoch.				
3.10. Percentuálny podiel ovplyvnených transakcií	Percentuálny podiel ovplyvnených transakcií vo vzťahu k priemernému dennému počtu domácich a cezhraničných transakcií vykonaných finančným subjektom v súvislosti s ovplyvnenou službou. Finančné subjekty zohľadňujú článok 1 ods. 4 a článok 9 ods. 1 písm. d) delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nemôže určiť skutočný percentuálny podiel ovplyvnených transakcií, použije odhady. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančný subjekt spočíta počet všetkých ovplyvnených transakcií a súčet vydelí celkovým počtom transakcií všetkých ovplyvnených finančných subjektov.	Nie	Áno, ak incident ovplyvnil nejakú transakciu	Áno, ak incident ovplyvnil nejakú transakciu	Vyjadrené ako percentuálny podiel – akákoľvek hodnota najviac s piatimi číselnými znakmi vrátane najviac jedného desatinného miesta vyjadrená ako percentuálny podiel (napr. 2,4 namiesto 2,4 %). Ak má hodnota po desatinnej čiarke viac ako jednu číslicu, nahlasujúce protistrany posledné miesto zaokrúhlia smerom nahor.
3.11. Hodnota ovplyvnených transakcií	Celková hodnota transakcií ovplyvnených závažným incidentom súvisiacim s IKT sa posudzuje v súlade s článkom 1 ods. 4 a článkom 9 ods. 1 písm. e) delegovaného nariadenia (EÚ) 2024/1772. Finančný subjekt, ktorý nedokáže určiť skutočnú hodnotu ovplyvnených transakcií, použije odhady založené na dostupných údajoch z porovnateľných referenčných období. Finančný subjekt vykazuje peňažnú sumu ako kladnú hodnotu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia celková hodnota ovplyvnených transakcií vo všetkých finančných subjektoch.	Nie	Áno, ak incident ovplyvnil nejaké transakcie	Áno, ak incident ovplyvnil nejakú transakciu	Peňažná suma Finančné subjekty vykazujú údajový bod v jednotkách s minimálnou presnosťou zodpovedajúcou tisícom jednotiek (napr. 2,5 namiesto 2 500 EUR).

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.12. Informácie o tom, či ide o skutočné čísla alebo odhady, alebo či nedošlo k žiadnemu vplyvu	Informácie o tom, či hodnoty vykázané v dátových poliach 3.4 až 3.11 sú skutočné alebo odhadované, alebo či nedošlo k žiadnemu vplyvu.	Nie	Áno	Áno	Pole s možnosťou výberu (viac možností): — skutočné údaje o ovplyvnených klientoch; — skutočné údaje o ovplyvnených finančných protistranách; — skutočné údaje o ovplyvnených transakciách; — odhady o ovplyvnených klientoch; — odhady o ovplyvnených finančných protistranách; — odhady o ovplyvnených transakciách; — žiadny vplyv na klientov; — žiadny vplyv na finančné protistrany; — žiadny vplyv na transakcie.
3.13. Vplyv na dobré meno	Informácie o vplyve na dobré meno v dôsledku závažného incidentu súvisiaceho s IKT, ako sa uvádza v článkoch 2 a 10 delegovaného nariadenia (EÚ) 2024/1772. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia kategórie vplyvu na dobré meno, ktoré sa vzťahujú aspoň na jeden finančný subjekt.	Nie	Áno, ak je splnené kritérium „vplyv na dobré meno“	Áno, ak je splnené kritérium „vplyv na dobré meno“	Pole s možnosťou výberu (viac možností): — závažný incident súvisiaci s IKT bol predmetom mediálneho spravodajstva; — závažný incident súvisiaci s IKT viedol k opakovaným sťažnostiam rôznych klientov alebo finančných protistrán, ktoré sa týkali služieb vyžadujúcich si priamy kontakt so zákazníkom alebo kritických obchodných vzťahov; — finančný subjekt si v dôsledku závažného incidentu súvisiaceho s IKT nebude môcť alebo pravdepodobne nebude môcť splniť regulačné požiadavky; — finančný subjekt v dôsledku závažného incidentu súvisiaceho s IKT stratí alebo pravdepodobne stratí klientov alebo finančné protistrany, čo môže mať významný vplyv na jeho obchodnú činnosť.
3.14. Kontextové informácie o vplyve na dobré meno	Informácie opisujúce, ako závažný incident súvisiaci s IKT ovplyvnil alebo by mohol ovplyvniť dobré meno finančného subjektu vrátane porušenia právnych predpisov, nesplnených regulačných požiadaviek, počtu sťažností klientov a iných.	Nie	Áno, ak je splnené kritérium „vplyv na dobré meno“.	Áno, ak je splnené kritérium „vplyv na dobré meno“.	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	Kontextové informácie zahŕňajú typ médií (napr. tradičné a digitálne médiá, blogy, streamovacie platformy) a mediálne pokrytie vrátane dosahu médií (miestne, národné, medzinárodné). Medializácia v tomto kontexte neznamená niekoľko negatívnych komentárov sledovateľov alebo používateľov sociálnych sietí. Finančný subjekt takisto uvedie, či medializácia poukázala na významné riziká pre jeho klientov v súvislosti so závažným incidentom súvisiacim s IKT vrátane rizika platobnej neschopnosti finančného subjektu alebo rizika straty finančných prostriedkov. Finančné subjekty takisto uvedú, či poskytli médiám informácie, ktoré slúžili na spoľahlivé informovanie verejnosti o závažnom incidente súvisiacom s IKT a jej dôsledkoch. Finančné subjekty môžu takisto uviesť, či sa v médiách v súvislosti s incidentom súvisiacim s IKT objavili nepravdivé informácie vrátane informácií založených na úmyselných dezinformáciách šírených aktérmi hrozieb alebo informácií týkajúcich sa poškodenia webového sídla finančného subjektu alebo zobrazujúcich takéto poškodenie.				
3.15. Dĺžka trvania incidentu	Finančné subjekty merajú trvanie závažného incidentu súvisiaceho s IKT od okamihu, keď došlo k závažnému incidentu súvisiacemu s IKT, do okamihu, keď bol incident vyriešený. Finančné subjekty, ktoré nemôžu určiť okamih, kedy prišlo k závažnému incidentu súvisiacemu s IKT, merajú trvanie závažného incidentu súvisiaceho s IKT od skoršieho okamihu medzi okamihom, keď finančný subjekt zistil incident, a okamihom, keď finančný subjekt zaznamenal incident v sieťových alebo systémových protokoloch alebo iných zdrojoch údajov. Finančné subjekty, ktoré ešte nevedia, kedy bude vyriešený závažný incident súvisiaci s IKT, použijú odhady. Hodnota sa vyjadruje v dňoch, hodinách a minútach. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančné subjekty merajú najdlhšie trvanie závažného incidentu súvisiaceho s IKT v prípade rozdielov medzi finančnými subjektmi.	Nie	Áno	Áno	DD:HH:MM

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.16. Výpadok služby	Výpadok služby meraný od okamihu, keď je služba úplne alebo čiastočne nedostupná pre klientov, finančné protistrany alebo iných interných alebo externých používateľov, až do okamihu, keď sa pravidelné činnosti alebo operácie obnovia na úroveň služby, ktorá bola poskytovaná pred závažným incidentom súvisiacim s IKT. Ak výpadok služby spôsobí omeškanie pri poskytovaní služby po obnovení bežných činností alebo operácií, finančné protistrany merajú výpadok od začiatku závažného incidentu súvisiaceho s IKT do momentu, keď sa uvedená meškajúca služba poskytuje. Finančné subjekty, ktoré nemôžu určiť okamih začatia výpadku služby, merajú výpadok služby od skoršieho okamihu medzi zistením incidentu a okamihom jeho zaznamenania. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančné subjekty merajú najdlhšie trvanie výpadku služby v prípade rozdielov medzi finančnými subjektmi.	Nie	Áno, ak incident spôsobil výpadok služby	Áno, ak incident spôsobil výpadok služby	DD:HH:MM
3.17. Informácie o tom, či sú údaje o dĺžke trvania a čase výpadku služby skutočné alebo odhadované	Informácia o tom, či hodnoty uvedené v dátových poliach 3.15 a 3.16 sú skutočné alebo odhadované.	Nie	Áno, ak je splnené kritérium „trvanie incidentu súvisiaceho s IKT a výpadok služby“	Áno, ak je splnené kritérium „trvanie incidentu súvisiaceho s IKT a výpadok služby“	Pole s možnosťou výberu: — skutočné údaje; — odhady; — skutočné údaje a odhady; — žiadne dostupné informácie.
3.18. Typy vplyvu v členských štátoch	Typ vplyvu v príslušných členských štátoch EHP. Údaj o tom, či závažný incident súvisiaci s IKT mal vplyv v iných členských štátoch EHP (okrem členského štátu príslušného orgánu, ktorému bol incident priamo nahlásený) v súlade s článkom 4 delegovaného nariadenia (EÚ) 2024/1772, a to najmä s ohľadom na význam vplyvu vo vzťahu k: a) ovplyvneným klientom a finančným protistranám v iných členských štátoch, alebo	Nie	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“	Pole s možnosťou výberu (viac možností): — klienti; — finančné protistrany; — pobočka finančného subjektu; — finančné subjekty v rámci skupiny vykonávajúce činnosti v príslušných členských štátoch; — infraštruktúra finančného trhu; — externí poskytovatelia, ktorí môžu byť spoloční s inými finančnými subjektmi.

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	b) pobočkám alebo iným finančným subjektom v rámci skupiny vykonávajúce činnosti v iných členských štátoch, alebo c) infraštruktúram finančného trhu alebo externým poskytovateľom, ktorí môžu ovplyvniť finančné subjekty v iných členských štátoch, ktorým poskytujú služby				
3.19. Opis toho, aký vplyv má incident na ostatné členské štáty	Opis vplyvu a závažnosti závažného incidentu súvisiaceho s IKT v každom ovplyvnenom členskom štáte vrátane posúdenia vplyvu a závažnosti na: a) klientov; b) finančné protistrany; c) pobočky finančného subjektu; d) iné finančné subjekty v rámci skupiny vykonávajúce činnosti v príslušných členských štátoch; e) infraštruktúry finančných trhov; f) externých poskytovateľov, ktorí môžu byť spoloční s inými finančnými subjektmi, ako sa uplatňuje v inom členskom štáte (členských štátoch).	Nie	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“	Áno, ak je splnená prahová hodnota pre kritérium „geografické rozloženie“	Alfanumerické
3.20. Prahové hodnoty významnosti pre klasifikačné kritérium „straty údajov“	Typ strát údajov, ktoré závažný incident súvisiaci s IKT prináša v súvislosti s dostupnosťou, pravosťou, integritou a dôvernosťou údajov. Finančné subjekty pri posudzovaní zohľadňujú články 5 a 13 delegovaného nariadenia (EÚ) 2024/1772. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia sa straty údajov týkajú aspoň jedného finančného subjektu.	Nie	Áno, ak je splnené kritérium „straty údajov“	Áno, ak je splnené kritérium „straty údajov“	Pole s možnosťou výberu (viac možností): — dostupnosť; — pravosť; — integrita; — dôvernosť.
3.21. Opis strát údajov	Opis vplyvu závažného incidentu súvisiaceho s IKT na dostupnosť, pravosť, integritu a dôvernosť kritických údajov v súlade s článkami 5 a 13 delegovaného nariadenia (EÚ) 2024/1772. Informácie o vplyve na plnenie obchodných cieľov finančného subjektu alebo na plnenie regulačných požiadaviek. Finančné subjekty v rámci poskytovaných informácií uvedú, či sú ovplyvnené údaje klientov, údaje iných subjektov (napr. finančných protistrán) alebo údaje samotného finančného subjektu.	Nie	Áno, ak je splnené kritérium „straty údajov“	Áno, ak je splnené kritérium „straty údajov“	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	Finančný subjekt môže uviesť aj typ údajov, ktorých sa incident týka – najmä či ide o dôverné údaje a o aký typ dôvernosti ide (napr. obchodné/podnikateľské tajomstvo, osobné údaje, služobné tajomstvo): bankové tajomstvo, poisťovacie tajomstvo, tajomstvo platobných služieb atď.). Informácie môžu zahŕňať aj možné riziká spojené so stratou údajov, napríklad či údaje ovplyvnené incidentom možno použiť na identifikáciu osôb a či ich môže aktér hrozby použiť na získanie úveru alebo pôžičky bez ich súhlasu, na uskutočnenie útokov typu cielené neoprávnené získavanie údajov (spear phishing) s cieľom zverejniť informácie. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia všeobecný opis vplyvu incidentu na ovplyvnené finančné subjekty. V prípade rozdielneho vplyvu sa v opise vplyvu jasne uvedie konkrétny vplyv na jednotlivé finančné subjekty.				
3.22. Klasifikačné kritérium „kritickosť zasiahnutých služieb“	Informácie týkajúce sa kritéria „kritickosť zasiahnutých služieb“. Finančné subjekty pri posudzovaní zohľadňujú článok 6 delegovaného nariadenia (EÚ) 2024/1772 vrátane informácií o: — ovplyvnených službách alebo činnostiach, ktoré si vyžadujú povolenie, registráciu alebo ktoré sú pod dohľadom príslušných orgánov, alebo — IKT službách alebo sieti a informačných systémoch, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu, a — charaktere škodlivého a neoprávneného prístupu do siete a informačných systémov finančného subjektu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia vplyv na kritické služby, ktoré sa vzťahujú aspoň na jeden finančný subjekt.	Nie	Áno	Áno	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.23. Typ incidentu	Klasifikácia incidentov podľa typu.	Nie	Áno	Áno	Pole s možnosťou výberu (viac možností): — súvisiace s kybernetickou bezpečnosťou; — zlyhanie procesu; — porucha systému; — externá udalosť; — súvisiace s platbou; — iné (uveďte).
3.24. Iné typy incidentov	Iné typy incidentov súvisiacich s IKT: finančné subjekty, ktoré v dátovom poli 3.23 vybrali typ incidentu „iné“, uvedú typ incidentu súvisiaceho s IKT	Nie	Áno, ak je v dátovom poli 3.23 vybraný typ incidentu „iné“.	Áno, ak je v dátovom poli 3.23 vybraný typ incidentu „iné“.	Alfanumerické
3.25. Hrozby a techniky používané aktérom hrozby	Uveďte hrozby a techniky, ktoré aktér hrozby používa vrátane: a) sociálneho inžinierstva vrátane phishingu; b) (D)DoS; c) krádeže totožnosti; d) šifrovania údajov s cieľom dosiahnuť vplyv vrátane ransomvéru; e) únosu zdrojov; f) exfiltrácie a manipulácie s údajmi s výnimkou krádeže identity; g) zničenia údajov; h) znehodnotenia; i) útoku na dodávateľský reťazec; j) iné (uveďte).	Nie	Áno, ak je typ incidentu súvisiaceho s IKT v poli 3.23 „súvisiaci s kybernetickou bezpečnosťou“.	Áno, ak je typ incidentu súvisiaceho s IKT v poli 3.23 „súvisiaci s kybernetickou bezpečnosťou“.	Pole s možnosťou výberu (viac možností): — sociálne inžinierstvo (vrátane phishingu); — (D)DoS; — krádež totožnosti; — šifrovanie údajov s cieľom dosiahnuť vplyv vrátane ransomvéru; — únos zdrojov; — exfiltrácia a manipulácia s údajmi s výnimkou krádeže identity; — zničenie údajov; — znehodnotenie; — útok na dodávateľský reťazec; — iné (uveďte).
3.26. Iné typy techník	Iné typy techník Finančné subjekty, ktoré si v dátovom poli 3.25 vybrali typ techník „iné“, uvedú typ techniky.	Nie	Áno, ak je v dátovom poli 3.25 vybraný typ techník „iné“.	Áno, ak je v dátovom poli 3.25 vybraný typ techník „iné“.	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.27. Informácie o ovplyvnených funkčných oblastiach a obchodných procesoch	Uvedenie funkčných oblastí a obchodných procesov, ktorých sa incident týka, vrátane produktov a služieb. Funkčné oblasti zahŕňajú okrem iného: a) marketing a rozvoj podnikania; b) služby zákazníkom; c) riadenie produktu; d) dodržiavanie predpisov; e) riadenie rizík; f) financie a účtovníctvo; g) HR a všeobecné služby; h) informačné technológie. Obchodné procesy zahŕňajú okrem iného: — informovanie o účte, — poistno-matematické služby, — prijímanie platobných transakcií, — autentifikáciu/autorizáciu, — orgán, — získavanie nových klientov, — správu dávok, — riadenie platieb dávok, — nákup a predaj štrukturalizovaných poistných zmlúv medzi poisťovňami, — platby kartou, — hospodárenie s hotovosťou, — vklady alebo výbery hotovosti, — riadenie poistných udalostí, — proces poistenia pohľadávok, — zúčtovanie, — konglomeráty podnikových úverov, — kolektívne poistenie, — úhrady, — úschovu a ochranu majetku, — získavanie nových zákazníkov, — prijímanie údajov, — spracovanie údajov, — inkaso, — vývozné poistenie, — finalizácia obchodov/obchodných dohôd, — umiestnenie finančných nástrojov, — účtovníctvo fondov,	Nie	Áno	Áno	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	— devízové prostriedky, — investičné poradenstvo, — riadenie investícií, — vydávanie platobných nástrojov, — riadenie pôžičiek, — proces platieb životného poistenia, — poukazovanie peňazí, — výpočet čistých aktív, — príkaz, — iniciovanie platby, — upisovanie poistenia, — riadenie portfólia, — správu prémií, — príjem/odosielanie/vykonávanie, — zaistenie, — vyrovnanie, — monitorovanie transakcií. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia ovplyvnené funkčné oblasti a obchodné procesy aspoň v jednom finančnom subjekte.				
3.28. Ovplyvnené zložky infraštruktúry podporujúce obchodné procesy	Informácie o tom, či zložky infraštruktúry (servery, operačné systémy, softvér, aplikačné servery, midlvér, sieťové komponenty a iné) podporujúce obchodné procesy boli ovplyvnené závažným incidentom súvisiacim s IKT.	Nie	Áno	Áno	Pole s možnosťou výberu: — Áno; — Nie; — Informácie nie sú k dispozícii.
3.29. Informácie o ovplyvnených zložkách infraštruktúry podporujúcich obchodné procesy	Opis vplyvu závažného incidentu súvisiaceho s IKT na zložky infraštruktúry podporujúce obchodné procesy vrátane hardvéru a softvéru. Hardvér zahŕňa servery, počítače, dátové centrá, prepínače, smerovače, rozbočovače. Softvér zahŕňa operačné systémy, aplikácie, databázy, bezpečnostné nástroje, sieťové komponenty a iné. V opisoch sa opíšu alebo pomenujú ovplyvnené zložky alebo systémy infraštruktúry, a ak sú k dispozícii: a) informácie o verzii; b) interná infraštruktúra/čiastočne outsourcovaná/plne outsourcovaná – názov externého poskytovateľa;	Nie	Áno, ak incident ovplyvnil zložky infraštruktúry podporujúce obchodné procesy	Áno, ak incident ovplyvnil zložky infraštruktúry podporujúce obchodné procesy	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	c) či je infraštruktúra používaná alebo zdieľaná viacerými obchodnými funkciami; d) zavedené príslušné opatrenia týkajúce sa odolnosti/kontinuity/obnovy/nahraditeľnosti.				
3.30. Vplyv na finančné záujmy klientov	Informácie o tom, či závažný incident súvisiaci s IKT ovplyvnil finančné záujmy klientov.	Nie	Áno	Áno	Pole s možnosťou výberu: — Áno; — Nie; — Informácie nie sú k dispozícii.
3.31. Nahlasovanie iným orgánom	Špecifikácia orgánov, ktoré boli informované o závažnom incidente súvisiacom s IKT. S prihliadnutím na rozdiely vyplývajúce z vnútroštátnych právnych predpisov členských štátov chápu finančné subjekty pojem orgány presadzovania práva v širšom zmysle ako orgány verejnej moci oprávnené stíhať počítačovú kriminalitu vrátane polície, orgánov presadzovania práva a prokuratúry.	Nie	Áno	Áno	Pole s možnosťou výberu (viac možností): — polícia/presadzovanie práva; — jednotka CSIRT; — orgán na ochranu osobných údajov; — národná agentúra pre kybernetickú bezpečnosť; — žiaden; — iný (uveďte).
3.32. Špecifikácia „iných“ orgánov	Špecifikácia „iných“ typov orgánov, ktoré boli informované o závažnom incidente súvisiacom s IKT. Ak je vybraná možnosť v dátovom poli 3.31. „Iné“, opis obsahuje podrobnejšie informácie o orgáne, ktorému finančný subjekt predložil informácie o závažnom incidente súvisiacom s IKT.	Nie	Áno, ak finančný subjekt informoval orgány typu „iné“ o závažnom incidente súvisiacom s IKT.	Áno, ak finančný subjekt informoval orgány typu „iné“ o závažnom incidente súvisiacom s IKT	Alfanumerické
3.33. Dočasné kroky/opatrenia, ktoré sa prijali alebo sa plánujú prijať na obnovu po incidente	Údaj o tom, či finančný subjekt vykonal (alebo plánuje vykonať) akékoľvek dočasné opatrenia, ktoré boli prijaté (alebo sa plánujú prijať) na obnovu po závažnom incidente súvisiacom s IKT.	Nie	Áno	Áno	Booleovské (áno alebo nie)

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
3.34. Opis všetkých dočasných činností a opatrení, ktoré sa prijali alebo sa plánujú prijať na obnovu po incidente	V informáciách sa opíšu prijaté okamžité opatrenia vrátane izolácie incidentu na úrovni siete, aktivovaných postupov na obídenie incidentu, zablokovaných portov USB, aktivovanej lokality na obnovu po havárii a akýchkoľvek ďalších dočasne zavedených dodatočných bezpečnostných kontrol. Finančné subjekty uvedú dátum a čas vykonania dočasných opatrení a predpokladaný dátum návratu na primárne miesto. Pri všetkých dočasných opatreniach, ktoré neboli vykonané, ale sú stále plánované, uveďte dátum, do ktorého sa očakáva ich vykonanie. Ak neboli prijaté žiadne dočasné opatrenia, uveďte dôvod.	Nie	Áno, ak boli prijaté alebo sa plánujú prijať dočasné opatrenia (dátové pole 3.33)	Áno, ak boli prijaté alebo sa plánujú prijať dočasné opatrenia (dátové pole 3.33)	Alfanumerické
3.35. Ukazovatele ohrozenia	Informácie týkajúce sa závažného incidentu súvisiaceho s IKT, ktoré môžu pomôcť identifikovať škodlivú činnosť v sieti alebo informačnom systéme (ukazovatele ohrozenia), v náležitých prípadoch. Toto pole sa vzťahuje len na tie finančné subjekty, ktoré patria do rozsahu pôsobnosti smernice Európskeho parlamentu a Rady (EÚ) 2022/2555 ([1]), a na tie finančné subjekty, ktoré sú podľa vnútroštátnych predpisov, ktorými sa transponuje článok 3 smernice (EÚ) 2022/2555, v relevantných prípadoch identifikované ako kľúčové alebo dôležité subjekty. Ukazovatele narušenia poskytnuté finančným subjektom obsahujú tieto kategórie údajov: a) IP adresu; b) URL adresu; c) oblasti; d) hašované súbory; e) údaje o škodlivom softvéri (názov škodlivého softvéru, názvy súborov a ich umiestnenie, konkrétne kľúče registra súvisiace s činnosťou škodlivého softvéru); f) údaje o sieťovej aktivite (porty, protokoly, adresy, odkazovače, používateľskí agenti, hlavičky, špecifické protokoly alebo charakteristické vzory sieťovej prevádzky); g) údaje e-mailovej správy (odosielateľ, príjemca, predmet, hlavičku, obsah);	Nie	Áno, ak je v dátovom poli 3.23 vybraný typ incidentu súvisiaci s kybernetickou bezpečnosťou	Áno, ak je v dátovom poli 3.23 vybraný typ incidentu súvisiaci s kybernetickou bezpečnosťou	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	h) požiadavky DNS a konfiguráciu registra; i) činnosti používateľského účtu (prihlásenie, činnosť používateľského účtu s oprávnením, zvýšenie oprávnení); j) prevádzka databázy (čítanie/zápis), požiadavky na ten istý súbor. V praxi môže tento typ informácií zahŕňať údaje týkajúce sa *inter alia* ukazovateľov opisujúcich vzorce sieťovej prevádzky zodpovedajúce známym útokom/komunikácii botnetu, IP adresy počítačov infikovaných škodlivým softvérom (botmi), údaje týkajúce sa „príkazových a riadiacich" serverov používaných škodlivým softvérom (zvyčajne domény alebo IP adresy) a URL adresy týkajúce sa phishingových stránok alebo webových sídel, na ktorých bol pozorovaný škodlivý softvér alebo exploit kity.				
Obsah záverečnej správy					
4.1. Klasifikácia hlavných príčin incidentu na vysokej úrovni	Klasifikácia hlavnej príčiny závažného incidentu súvisiaceho s IKT na vysokej úrovni v rámci typov incidentov vrátane týchto kategórií na vysokej úrovni: a) zlomyseľného konania; b) zlyhania procesu; c) poruchy/nefunkčnosti systému; d) chyby spôsobenej človekom; e) externej udalosti.	Nie	Nie	Áno	Pole s možnosťou výberu (viac možností): — zlomyseľné konanie; — zlyhanie procesu; — porucha/nefunkčnosť systému; — chyba spôsobená človekom; — externá udalosť.
4.2. Podrobná klasifikácia hlavných príčin incidentu	Podrobná klasifikácia hlavných príčin závažných incidentov súvisiacich s IKT v rámci typov incidentov vrátane nasledujúcich podrobných kategórií spojených s kategóriami na vysokej úrovni, ktoré sú uvedené v dátovom poli 4.1.: 1. **Zlomyseľné konanie** (ak je vybrané, vyberte jednu alebo viacero nasledujúcich možností): a) zámerné vnútorné činnosti; b) úmyselné fyzické poškodenie/manipulácia/krádež; c) podvodné konanie. 2. **Zlyhanie procesu** (ak je vybrané, vyberte jednu alebo viacero nasledujúcich možností): a) nedostatočné monitorovanie alebo zlyhanie monitorovania a kontroly;	Nie	Nie	Áno	Pole s možnosťou výberu (viac možností): — zlomyseľné konanie: zámerné vnútorné činnosti; — zlomyseľné konanie: úmyselné fyzické poškodenie/manipulácia/krádež; — zlomyseľné konanie: podvodné konanie; — zlyhanie procesu: nedostatočné monitorovanie alebo zlyhanie monitorovania a kontroly; — zlyhanie procesu: nedostatočné/ nevyjasnené úlohy a povinnosti; — zlyhanie procesu: zlyhanie procesu riadenia IKT rizík, — zlyhanie procesu: nedostatočné alebo neúspešné operácie IKT a bezpečnostné operácie IKT;

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	b) nedostatočné/nevyjasnené úlohy a povinnosti; c) zlyhanie procesu riadenia IKT rizík; d) nedostatočné alebo neúspešné operácie IKT a bezpečnostné operácie IKT; e) nedostatočné alebo neúspešné riadenie projektov IKT; f) nedostatočné interné pravidlá, postupy a dokumentácia; g) nedostatočné nadobudnutie, vývoj alebo údržba IKT systémov; h) iné (uveďte). 3. **Porucha/nefunkčnosť systému** (ak je vybraná, vyberte jednu alebo viacero nasledujúcich možností): a) kapacita a výkon hardvéru: závažné incidenty súvisiace s IKT spôsobené hardvérovými zdrojmi, ktoré sa ukážu ako nedostatočné z hľadiska kapacity alebo výkonu na splnenie platných legislatívnych požiadaviek; b) údržba hardvéru: závažné incidenty súvisiace s IKT vyplývajúce z nevhodnej alebo nedostatočnej údržby hardvérových komponentov, iné ako „zastarávanie/ starnutie hardvéru“; c) zastarávanie/starnutie hardvéru: tento typ hlavnej príčiny zahŕňa závažné incidenty súvisiace s IKT, ktoré sú dôsledkom zastaraných alebo starnúcich hardvérových komponentov; d) kompatibilita/konfigurácia softvéru: závažné incidenty súvisiace s IKT spôsobené softvérovými komponentmi, ktoré sú nekompatibilné s iným softvérom alebo konfiguráciami systému, vrátane závažných incidentov súvisiacich s IKT vyplývajúcich z konfliktov softvéru, nesprávnych nastavení alebo nesprávne nakonfigurovaných parametrov, ktoré ovplyvňujú celkovú funkčnosť systému; e) výkonnosť softvéru: závažné incidenty súvisiace s IKT vyplývajúce zo softvérových komponentov, ktoré vykazujú nízku výkonnosť alebo neefektívnosť z iných dôvodov, ako sú uvedené v časti „kompatibilita/ konfigurácia softvéru“, vrátane závažných incidentov súvisiacich s IKT spôsobených pomalou odozvou, nadmernou spotrebou zdrojov alebo neefektívnym vykonávaním dotazov, ktoré majú vplyv na výkonnosť softvéru alebo systému;				— zlyhanie procesu: nedostatočné alebo neúspešné riadenie projektov IKT; — zlyhanie procesu: nedostatočné interné pravidlá, postupy a dokumentácia; — zlyhanie procesu: nedostatočné nadobudnutie, vývoj a údržba IKT systémov; — zlyhanie procesu: iné (uveďte), — poruchy systému; kapacita a výkon hardvéru; — poruchy systému; údržba hardvéru; — poruchy systému; zastarávanie/starnutie hardvéru; — poruchy systému; kompatibilita/ konfigurácia softvéru; — poruchy systému; výkonnosť softvéru; — poruchy systému; konfigurácia siete; — poruchy systému; fyzické poškodenie; — poruchy systému; iné (uveďte); — chyba spôsobená človekom: opomenutie; — chyba spôsobená človekom: chyba, — chyba spôsobená človekom: zručnosti a vedomosti; — chyba spôsobená človekom: nedostatočné ľudské zdroje; — chyba spôsobená človekom: nesprávna komunikácia; — chyba spôsobená človekom: iné (uveďte); — externá udalosť: prírodné katastrofy/ vyššia moc; — externá udalosť: zlyhania tretích strán; — externá udalosť: iné (uveďte).

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	f) konfigurácia siete: závažné incidenty súvisiace s IKT vyplývajúce z nesprávnych alebo chybne nakonfigurovaných sieťových nastavení alebo infraštruktúry vrátane závažných incidentov súvisiacich s IKT spôsobených chybami v konfigurácii siete, problémami so smerovaním, chybnou konfiguráciou brány firewall alebo inými problémami súvisiacimi so sieťou, ktoré ovplyvňujú pripojiteľnosť alebo komunikáciu; g) fyzické poškodenie: závažné incidenty súvisiace s IKT spôsobené fyzickým poškodením infraštruktúry IKT, ktoré vedú k poruche systému; h) iné (uveďte). 4. **Chyba spôsobená človekom** (ak je vybraná, vyberte jednu alebo viacero nasledujúcich možností): a) opomenutie (neúmyselné); b) chyba; c) zručnosti a vedomosti: závažné incidenty súvisiace s IKT vyplývajúce z nedostatku odborných znalostí alebo zručností pri zaobchádzaní so systémami alebo procesmi IKT, ktoré môžu byť spôsobené neprimeranou odbornou prípravou, nedostatočnými vedomosťami alebo nedostatkami v zručnostiach potrebných na vykonávanie konkrétnych úloh alebo riešenie technických problémov; d) nedostatočné ľudské zdroje: závažné incidenty súvisiace s IKT spôsobené nedostatkom potrebných zdrojov vrátane hardvéru, softvéru, infraštruktúry alebo personálu, vrátane situácií, keď nedostatočné zdroje vedú k prevádzkovej neefektívnosti, poruchám systému alebo neschopnosti splniť obchodné požiadavky; e) nesprávna komunikácia; f) iné (uveďte). 5. **Externá udalosť** (ak je vybraná, vyberte jednu alebo viacero nasledujúcich možností): a) prírodné katastrofy/vyššia moc; b) zlyhania tretích strán;				

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	c) iné (uveďte). Finančné subjekty zohľadňujú, že v prípade opakujúcich sa závažných incidentov súvisiacich s IKT sa berie do úvahy konkrétna zjavná hlavná príčina incidentu, a nie rozsiahle kategórie zahrnuté v tejto oblasti.				
4.3. Dodatočná klasifikácia hlavných príčin incidentu	Dodatočná klasifikácia hlavných príčin závažného incidentu súvisiaceho s IKT v rámci typu incidentu vrátane týchto dodatočných klasifikačných kategórií spojených s podrobnými kategóriami, ktoré sa majú uvádzať v dátovom poli 4.2. Pole je povinné pre záverečnú správu, ak sa v dátovom poli 4.2 uvádzajú špecifické kategórie, ktoré si vyžadujú ďalšiu granularitu. 2a) **Nedostatočné monitorovanie alebo zlyhanie monitorovania a kontroly:** a) monitorovanie dodržiavania politiky; b) monitorovanie externých poskytovateľov služieb; c) monitorovanie a overovanie nápravy zraniteľných miest; d) riadenie identity a prístupu; e) šifrovanie a kryptografia; f) vedenie záznamov. 2c) **Zlyhanie procesu riadenia IKT rizík:** a) zlyhanie pri určovaní presných úrovní tolerancie rizika; b) nedostatočné posúdenie zraniteľnosti a hrozieb; c) neprimerané opatrenia na ošetrenie rizík; d) nedostatočné riadenie zvyškových IKT rizík. 2d) **Nedostatočné alebo neúspešné operácie IKT a bezpečnostné operácie IKT:** a) riadenie zraniteľnosti a opráv; b) riadenie zmien; c) riadenie kapacít a výkonnosti; d) správa IKT aktív a klasifikácia informácií;	Nie	Nie	Áno	Pole s možnosťou výberu (viac možností): — monitorovanie dodržiavania politiky; — monitorovanie externých poskytovateľov služieb; — monitorovanie a overovanie nápravy zraniteľných miest; — riadenie identity a prístupu; — šifrovanie a kryptografia; — vedenie záznamov; — zlyhanie pri určovaní presných úrovní tolerancie rizika; — nedostatočné posúdenie zraniteľnosti a hrozieb; — neprimerané opatrenia na ošetrenie rizík; — nedostatočné riadenie zvyškových IKT rizík; — riadenie zraniteľnosti a opráv; — riadenie zmien; — riadenie kapacít a výkonnosti; — správa IKT aktív a klasifikácia informácií; — zálohovanie a obnovenie; — spracovanie chýb; — nedostatočné nadobudnutie; vývoj a údržba IKT systémov; — nedostatočné testovanie softvéru alebo jeho zlyhanie.

Dátové pole		Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
		e) zálohovanie a obnovenie; f) spracovanie chýb. 2g) **Nedostatočné nadobudnutie, vývoj a údržba IKT systémov:** a) nedostatočné nadobudnutie, vývoj a údržba IKT systémov; b) nedostatočné testovanie softvéru alebo zlyhanie testovania softvéru.				
4.4.	Iné typy hlavných príčin	Finančné subjekty, ktoré v dátovom poli 4.2. zvolili „iný“ typ hlavnej príčiny, uvedú iné typy typov hlavných príčin	Nie	Nie	Áno, ak je v dátovom poli 4.2. vybraný typ hlavnej príčiny „iné“.	Alfanumerické
4.5.	Informácie o hlavných príčinách incidentu	Opis postupnosti udalostí, ktoré viedli k závažnému incidentu súvisiacemu s IKT, a opis toho, ako má závažný incident súvisiaci s IKT podobnú zjavnú hlavnú príčinu, ak je tento incident klasifikovaný ako opakujúci sa incident, vrátane stručného opisu všetkých základných dôvodov a primárnych faktorov, ktoré prispeli k výskytu závažného incidentu súvisiaceho s IKT. V prípade, že došlo k zlomyseľnému konaniu, opis spôsobu vykonania zlomyseľného konania vrátane použitých taktík, techník a postupov, ako aj vstupného vektora závažného incidentu súvisiaceho s IKT vrátane prípadného opisu vyšetrovania a analýzy, ktoré viedli k identifikácii hlavných príčin.	Nie	Nie	Áno	Alfanumerické
4.6.	Riešenie incidentu	Ďalšie informácie týkajúce sa prijatých/plánovaných opatrení na trvalé vyriešenie závažného incidentu súvisiaceho s IKT a na zabránenie jeho opakovaniu. Poznatky získané zo závažného incidentu súvisiaceho s IKT.	Nie	Nie	Áno	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	Opis musí obsahovať tieto body: 1. **Opis opatrení na riešenie** a) opatrenia prijaté na trvalé vyriešenie závažného incidentu súvisiaceho s IKT (okrem dočasných opatrení); b) pri každom prijatom opatrení uveďte prípadnú účasť externého poskytovateľa a finančného subjektu; c) uveďte, či boli po závažnom incidente súvisiacom s IKT upravené postupy; d) uveďte všetky ďalšie kontroly, ktoré boli zavedené alebo ktoré sa plánujú, spolu so súvisiacim časovým harmonogramom vykonávania. Prípadné zistené problémy týkajúce sa spoľahlivosti ovplyvnených IT systémov a/alebo z hľadiska zavedených postupov alebo kontrol. Finančné subjekty jasne uvedú, ako budú plánované nápravné opatrenia riešiť identifikované hlavné príčiny a kedy sa očakáva trvalé vyriešenie závažného incidentu súvisiaceho s IKT. 2. **Získané poznatky** Finančné subjekty opíšu zistenia z preskúmania po incidente.				
4.7. Dátum a čas, kedy sa riešila hlavná príčina incidentu	Dátum a čas, kedy sa riešila hlavná príčina incidentu.	Nie	Nie	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)
4.8. Dátum a čas vyriešenia incidentu	Dátum a čas vyriešenia incidentu.	Nie	Nie	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh:mm.ss)

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
4.9. Informácie, ak sa dátum trvalého riešenia incidentov líši od pôvodne plánovaného dátumu vykonania	Opisy dôvodov, prečo sa dátum trvalého riešenia závažných incidentov súvisiacich s IKT líši od pôvodne plánovaného dátumu vykonania, v náležitých prípadoch.	Nie	Nie	Áno	Alfanumerické
4.10. Posúdenie rizika pre zásadné funkcie na účely riešenia incidentov	Posúdenie, či závažný incident súvisiaci s IKT predstavuje riziko pre zásadné funkcie v zmysle článku 2 ods. 1 bodu 35 smernice Európskeho parlamentu a Rady 2014/59/EÚ ([2]). Subjekty uvedené v článku 1 ods. 1 smernice 2014/59/EÚ uvedú, či incident predstavuje riziko pre zásadné funkcie v zmysle článku 2 ods. 1 bodu 35 smernice 2014/59/EÚ, a nahlásia ho vo vzore Z07.01 vykonávacieho nariadenia Komisie (EÚ) 2018/1624 ([3]) a priradia ku konkrétnemu subjektu vo vzore Z07.02.	Nie	Nie	Áno, ak incident predstavuje riziko pre zásadné funkcie finančných subjektov podľa článku 2 ods. 1 bodu 35 smernice 2014/59/EÚ.	Alfanumerické
4.11. Informácie relevantné pre orgány pre riešenie krízových situácií	Opis toho, či a ak áno, ako závažný incident súvisiaci s IKT ovplyvnil riešiteľnosť krízovej situácie subjektu alebo skupiny. Subjekty uvedené v článku 1 ods. 1 smernice 2014/59/EÚ poskytujú informácie o tom, či a prípadne ako závažný incident súvisiaci s IKT ovplyvnil riešiteľnosť krízovej situácie subjektu alebo skupiny. Tieto subjekty takisto uvedú, či závažný incident súvisiaci s IKT ovplyvňuje platobnú schopnosť alebo likviditu finančného subjektu, a potenciálnu kvantifikáciu vplyvu. Tieto subjekty poskytnú aj informácie o vplyve na prevádzkovú kontinuitu, vplyve na možnosť riešenia krízových situácií subjektu, každom dodatočnom vplyve na náklady a straty vyplývajúceho zo závažného incidentu súvisiaceho s IKT vrátane vplyvu na kapitálovú pozíciu finančného subjektu, ako aj o tom, či sú zmluvné dojednania o využívaní IKT služieb stále spoľahlivé a plne vynútiteľné v prípade riešenia krízovej situácie subjektu.	Nie	Nie	Áno, ak incident ovplyvnil riešiteľnosť krízovej situácie subjektu alebo skupiny.	Alfanumerické

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
4.12. Prahová hodnota významnosti pre klasifikačné kritérium „hospodársky vplyv“	Podrobné informácie o prahových hodnotách, ktoré nakoniec dosiahla závažný incident súvisiaci s IKT vo vzťahu ku kritériu „hospodársky vplyv“ uvedeným v článkoch 7 a 14 delegovaného nariadenia (EÚ) 2024/1772.	Nie	Nie	Áno	Alfanumerické
4.13. Výška hrubých priamych a nepriamych nákladov a strát	Celková výška hrubých priamych a nepriamych nákladov a strát, ktoré vznikli finančnému subjektu v dôsledku závažného incidentu súvisiaceho s IKT vrátane: a) výšky vyvlastnených finančných prostriedkov alebo finančných aktív, za ktoré finančný subjekt zodpovedá; b) výšky nákladov na výmenu alebo premiestnenie softvéru, hardvéru alebo infraštruktúry; c) výšky nákladov na zamestnancov vrátane nákladov spojených s nahradením alebo premiestnením zamestnancov, prijatím ďalších zamestnancov, odmeňovaním nadčasov a obnovou stratených alebo zhoršených zručností zamestnancov; d) výšky poplatkov z dôvodu nedodržania zmluvných záväzkov; e) výšky nákladov na nápravu a odškodnenie zákazníkov; f) výšky strát v dôsledku ušlých príjmov; g) výšky nákladov spojených s vnútornou a vonkajšou komunikáciou; h) výšky nákladov na poradenstvo vrátane nákladov spojených s právnym poradenstvom, forenznými a sanačnými službami; i) výšky ostatných nákladov a strát vrátane: i) priamych nákladov vrátane zníženia hodnoty a nákladov na vyrovnanie účtovaných do výkazu ziskov a strát a do odpisov v dôsledku závažného incidentu súvisiaceho s IKT; ii) rezerv alebo opravných položiek účtovaných do výkazu ziskov a strát na krytie pravdepodobných strát súvisiacich so závažným incidentom súvisiacim s IKT;	Nie	Nie	Áno	Peňažná suma

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	iii) nezaúčtovaných strát vo forme strát z udalosti závažného incidentu súvisiaceho s IKT, ktoré sa dočasne zaúčtujú v tranzitných alebo prechodných účtoch a ktoré sa ešte nepremietli do výsledku hospodárenia, ktoré sa plánujú zahrnúť v časovom období zodpovedajúcom veľkosti a veku nezaúčtovanej položky; iv) významných nevybratých príjmov súvisiacich so zmluvnými povinnosťami s tretími stranami vrátane rozhodnutia namiesto náhrady alebo priamej platby kompenzovať klienta po udalosti závažného incidentu súvisiaceho s IKT, a to prostredníctvom úpravy príjmu, ktorou sa upustí od zmluvných poplatkov na špecifické budúce časové obdobie alebo ktorou sa takéto poplatky znížia; v) strát z načasovania, keď trvajú viac než jeden účtovný rok a vedú k právnemu riziku. Finančné subjekty zohľadňujú vo svojom posúdení článok 7 ods. 1 a 2 delegovaného nariadenia (EÚ) 2024/1772. Finančné subjekty do tohto údaju nezahŕňajú žiadny typ finančnej náhrady. Finančné subjekty vykazujú peňažnú sumu ako kladnú hodnotu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančné subjekty zohľadňujú celkovú výšku nákladov a strát vo všetkých finančných subjektoch. Finančné subjekty vykazujú údajový bod v jednotkách s minimálnou presnosťou rovnajúcou sa tisícom jednotiek.				
4.14. Výška vrátených finančných prostriedkov	Celková výška vrátených finančných prostriedkov. Finančné náhrady sa vzťahujú na pôvodnú stratu spôsobenú incidentom, a to nezávisle od času, keď sa získajú finančné náhrady vo forme finančných prostriedkov alebo prílevu hospodárskych úžitkov.	Nie	Nie	Áno	Peňažná suma Finančné subjekty vykazujú údajový bod v jednotkách s minimálnou presnosťou rovnajúcou sa tisícom jednotiek

Dátové pole	Opis	Povinné v prípade počiatočného oznámenia	Povinné v prípade priebežnej správy	Povinné v prípade záverečnej správy	Druh poľa
	Finančné subjekty vykazujú peňažnú sumu ako kladnú hodnotu. V prípade súhrnného nahlasovania uvedeného v článku 7 tohto nariadenia finančné subjekty zohľadňujú celkovú výšku finančných náhrad vo všetkých finančných subjektoch.				
4.15. Informácie o tom, či sa incidenty, ktoré nie sú závažné, opakujú	Informácie o tom, či sa opakovane vyskytol viac ako jeden menej závažný incident súvisiaci s IKT, ktorý sa spoločne považuje za závažný incident v zmysle článku 8 ods. 2 delegovaného nariadenia (EÚ) 2024/1772. Finančné subjekty uvedú, či sa menej závažné incidenty súvisiace s IKT opakovali a či sa spoločne považujú za jeden závažný incident súvisiaci s IKT. Finančné subjekty uvedú aj počet výskytov týchto menej závažných incidentov súvisiacich s IKT.	Nie	Nie	Áno, ak závažný incident zahŕňa viac ako jeden menej závažný opakujúci sa incident.	Alfanumerické
4.16. Dátum a čas výskytu opakujúcich sa incidentov	Ak finančné subjekty hlásia opakujúce sa incidenty súvisiace s IKT, dátum a čas, kedy sa vyskytol prvý incident súvisiaci s IKT.	Nie	Nie	Áno, v prípade opakujúcich sa incidentov	Norma ISO 8601 UTC (RRRR-MM-DD hh.mm.ss)

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) Smernica Európskeho parlamentu a Rady 2014/59/EÚ z 15. mája 2014, ktorou sa stanovuje rámec pre ozdravenie a riešenie krízových situácií úverových inštitúcií a investičných spoločností a ktorou sa mení smernica Rady 82/891/EHS a smernice Európskeho parlamentu a Rady 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EÚ, 2012/30/EÚ a 2013/36/EÚ a nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 a (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Vykonávacie nariadenie Komisie (EÚ) 2018/1624 z 23. októbra 2018, ktorým sa stanovujú vykonávacie technické predpisy, pokiaľ ide o postupy, štandardné formy a vzory na poskytovanie informácií na účely plánov riešenia krízových situácií pre úverové inštitúcie a investičné spoločnosti podľa smernice Európskeho parlamentu a Rady 2014/59/EÚ, a ktorým sa zrušuje vykonávacie nariadenie Komisie (EÚ) 2016/1066 (Ú. v. EÚ L 277, 7.11.2018, s. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

PRÍLOHA III

VZORY NA OZNAMOVANIE VÝZNAMNÝCH KYBERNETICKÝCH HROZIEB

Číslo poľa	Dátové pole	
1	Názov subjektu, ktorý predkladá oznámenie	
2	Identifikačný kód subjektu, ktorý predkladá oznámenie	
3	Typ finančného subjektu, ktorý predkladá oznámenie	
4	Názov finančného subjektu	
5	Identifikátor právneho subjektu finančného subjektu	
6	Meno hlavnej kontaktnej osoby	
7	E-mail: hlavnej kontaktnej osoby	
8	Telefón hlavnej kontaktnej osoby	
9	Meno druhej kontaktnej osoby	
10	E-mail: druhej kontaktnej osoby	
11	Telefón druhej kontaktnej osoby	
12	Dátum a čas zistenia kybernetickej hrozby	
13	Opis významnej kybernetickej hrozby	
14	Informácie o potenciálnom vplyve	
15	Klasifikačné kritériá potenciálnych incidentov	
16	Stav kybernetickej hrozby	
17	Opatrenia prijaté na zabránenie naplneniu	
18	Oznámenie ostatným zainteresovaným stranám	
19	Ukazovatele ohrozenia	
20	Ďalšie relevantné informácie	

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

PRÍLOHA IV

SLOVNÍK ÚDAJOV A POKYNY NA OZNAMOVANIE VÝZNAMNÝCH KYBERNETICKÝCH HROZIEB

Dátové pole	Opis	Povinné pole	Druh poľa
1. Názov subjektu, ktorý predkladá oznámenie	Úplný právny názov subjektu, ktorý predkladá oznámenie.	Áno	Alfanumerické
2. Identifikačný kód subjektu, ktorý predkladá oznámenie	Identifikačný kód subjektu, ktorý predkladá oznámenie. Ak finančné subjekty predkladajú oznámenie/správu, identifikačným kódom je identifikátor právneho subjektu (LEI), čo je jedinečný 20-miestny alfanumerický kód podľa normy ISO 17442-1:2020. Ak externý poskytovateľ predkladá správu za finančný subjekt, môže použiť identifikačný kód uvedený vo vykonávacích technických predpisoch prijatých podľa článku 28 ods. 9 nariadenia (EÚ) 2022/2554.	Áno	Alfanumerické
3. Typ finančného subjektu, ktorý predkladá správu	Typ subjektu podľa článku 2 ods. 1 písm. a) až t) nariadenia (EÚ) 2022/2554, ktorý predkladá správu.	Áno, ak správu neposkytuje priamo ovplyvnený finančný subjekt.	Pole s možnosťou výberu (viacnásobný výber): — úverová inštitúcia; — platobná inštitúcia; — oslobodená platobná inštitúcia; — poskytovateľ služieb informovania o účte; — inštitúcia elektronického peňažníctva; — oslobodená inštitúcia elektronického peňažníctva; — investičná spoločnosť; — poskytovateľ služieb kryptoaktív; — emitent tokenov naviazaných na aktíva; — centrálny depozitár cenných papierov; — centrálna protistrana; — obchodné miesto; — archív obchodných údajov; — správca alternatívneho investičného fondu; — správcovská spoločnosť; — poskytovateľ služieb vykazovania údajov;

Dátové pole		Opis	Povinné pole	Druh poľa
				— poisťovňa a zaisťovňa; — sprostredkovateľ poistenia, sprostredkovateľ zaistenia a sprostredkovateľ doplnkového poistenia; — inštitúcia zamestnaneckého dôchodkového zabezpečenia; — ratingová agentúra; — správca kritických referenčných hodnôt; — poskytovateľ služieb hromadného financovania; — archív sekuritizačných údajov.
4.	Názov finančného subjektu	Úplný právny názov finančného subjektu, ktorý oznamuje významnú kybernetickú hrozbu.	Áno, ak je finančný subjekt iný ako subjekt, ktorý predkladá oznámenie.	Alfanumerické
5.	Identifikátor právneho subjektu finančného subjektu	Identifikátor právneho subjektu (LEI) finančného subjektu, ktorý oznamuje významnú kybernetickú hrozbu, pridelený v súlade s Medzinárodnou organizáciou pre normalizáciu.	Áno, ak je finančný subjekt oznamujúci významnú kybernetickú hrozbu odlišný od subjektu, ktorý predkladá správu	Jedinečný alfanumerický 20-znakový kód podľa normy ISO 17442-1:2020
6.	Meno hlavnej kontaktnej osoby	Meno a priezvisko hlavnej kontaktnej osoby finančného subjektu.	Áno	Alfanumerické
7.	E-mail: hlavnej kontaktnej osoby	E-mailová adresa hlavnej kontaktnej osoby, ktorú môže príslušný orgán použiť na následnú komunikáciu.	Áno	Alfanumerické
8.	Telefón hlavnej kontaktnej osoby	Telefónne číslo hlavnej kontaktnej osoby, ktoré môže príslušný orgán použiť na následnú komunikáciu. Telefónne číslo sa uvádza so všetkými medzinárodnými predvoľbami (napr. +33XXXXXXXXX)	Áno	Alfanumerické
9.	Meno druhej kontaktnej osoby	Meno a priezvisko druhej kontaktnej osoby finančného subjektu alebo subjektu, ktorý predkladá oznámenie v mene finančného subjektu, ak je k dispozícii.	Áno, ak je k dispozícii meno a priezvisko druhej kontaktnej osoby finančného subjektu alebo subjektu, ktorý predkladá oznámenie za finančný subjekt.	Alfanumerické

Dátové pole	Opis	Povinné pole	Druh poľa
10. E-mail: druhej kontaktnej osoby	E-mailová adresa druhej kontaktnej osoby alebo funkčná e-mailová adresa tímu, ktorú môže príslušný orgán použiť na následnú komunikáciu, ak je k dispozícii.	Áno, ak je k dispozícii e-mailová adresa druhej kontaktnej osoby alebo funkčná e-mailová adresa tímu, ktorú môže príslušný orgán použiť na následnú komunikáciu.	Alfanumerické
11. Telefón druhej kontaktnej osoby	Telefónne číslo druhej kontaktnej osoby, ktoré môže príslušný orgán použiť na následnú komunikáciu, ak je k dispozícii. Telefónne číslo sa uvádza so všetkými medzinárodnými predvoľbami (napr. +33XXXXXXXXX)	Áno, ak je k dispozícii telefónne číslo druhej kontaktnej osoby, ktoré môže príslušný orgán použiť na následnú komunikáciu.	Alfanumerické
12. Dátum a čas zistenia kybernetickej hrozby	Dátum a čas, kedy sa finančný subjekt dozvedel o významnej kybernetickej hrozbe.	Áno	Norma ISO 8601 UTC (RRRR-MM-DD hh: mm.ss)
13. Opis významnej kybernetickej hrozby	Opis najdôležitejších aspektov významnej kybernetickej hrozby. Finančné subjekty poskytujú: a) prehľad najdôležitejších aspektov významnej kybernetickej hrozby na vysokej úrovni; b) súvisiace riziká, ktoré z nej vyplývajú, vrátane potenciálnych zraniteľností systémov finančného subjektu, ktoré môžu byť zneužité; c) informácie o pravdepodobnosti naplnenia významnej kybernetickej hrozby a d) informácie o zdroji informácií o kybernetickej hrozbe.	Áno	Alfanumerické
14. Informácie o potenciálnom vplyve	Informácie o potenciálnom vplyve kybernetickej hrozby na finančný subjekt, jeho klientov alebo finančné protistrany, ak sa kybernetická hrozba naplnila	Áno	Alfanumerické
15. Klasifikačné kritériá potenciálnych incidentov	Klasifikačné kritériá, ktoré by mohli viesť k nahláseniu závažného incidentu, ak by sa kybernetická hrozba naplnila.	Áno	Pole s možnosťou výberu (viac možností): — klienti, finančné protistrany a transakcie ovplyvnené incidentom; — vplyv na dobré meno; — trvanie incidentu súvisiaceho s IKT a výpadok služby; — geografické rozloženie; — straty údajov; — kritickosť zasiahnutých služieb; — hospodársky vplyv.

Dátové pole		Opis	Povinné pole	Druh poľa
16.	Stav kybernetickej hrozby	Informácie o stave kybernetickej hrozby pre finančný subjekt a o tom, či došlo k nejakým zmenám v aktivite hrozby. Ak kybernetická hrozba prestala komunikovať s informačnými systémami finančného subjektu, jej stav možno označiť ako neaktívny. Ak má finančný subjekt informácie, že hrozba je naďalej aktívna voči iným stranám alebo finančnému systému ako celku, stav sa označí ako aktívny.	Áno	Pole s možnosťou výberu: — aktívna; — neaktívna.
17.	Opatrenia prijaté na zabránenie naplneniu	Prípadné informácie na vysokej úrovni o opatreniach, ktoré finančný subjekt prijal s cieľom zabrániť naplneniu významných kybernetických hrozieb.	Áno	Alfanumerické
18.	Oznámenie ostatným zainteresovaným stranám	Informácie o oznámení kybernetickej hrozby iným finančným subjektom alebo orgánom.	Áno, ak boli o kybernetickej hrozbe informované iné finančné subjekty alebo orgány.	Alfanumerické
19.	Ukazovatele ohrozenia	Informácie týkajúce sa významnej hrozby, ktoré môžu pomôcť identifikovať škodlivú činnosť v sieti alebo informačnom systéme (ukazovatele ohrozenia), v náležitých prípadoch. Ukazovatele narušenia poskytované finančným subjektom môžu zahŕňať tieto kategórie údajov, nie však výlučne: a) IP adresu; b) URL adresu; c) oblasti; d) hašované súbory; e) údaje o škodlivom softvéri (názov škodlivého softvéru, názvy súborov a ich umiestnenie, konkrétne kľúče registra súvisiace s činnosťou škodlivého softvéru); f) údaje o sieťovej aktivite (porty, protokoly, adresy, odkazovače, používateľskí agenti, hlavičky, špecifické protokoly alebo charakteristické vzory sieťovej prevádzky); g) údaje e-mailovej správy (odosielateľ, príjemca, predmet, hlavičku, obsah); h) požiadavky DNS a konfiguráciu registra; i) činnosti používateľského účtu (prihlásenie, činnosť používateľského účtu s oprávnením, zvýšenie oprávnení); j) prevádzku databázy (čítanie/zápis), požiadavky na ten istý súbor. Tento typ informácií môže zahŕňať údaje týkajúce sa ukazovateľov opisujúcich vzorce sieťovej prevádzky zodpovedajúce známym útokom/komunikácii botnetu, IP adresy počítačov infikovaných škodlivým softvérom (botmi), údaje týkajúce sa „príkazových a riadiacich“ serverov používaných škodlivým softvérom (zvyčajne domény alebo IP adresy) a URL adresy týkajúce sa phishingových stránok alebo webových sídel, na ktorých bol pozorovaný škodlivý softvér alebo exploit kity.	Áno, ak sú k dispozícii informácie o ukazovateľoch ohrozenia súvisiacich s kybernetickou hrozbou.	Alfanumerické
20.	Ďalšie relevantné informácie	Akékoľvek ďalšie relevantné informácie o významnej kybernetickej hrozbe	Áno, v náležitých prípadoch a ak sú k dispozícii ďalšie informácie, ktoré nie sú uvedené vo vzore.	Alfanumerické

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