EVROPSKÁ
KOMISE

V Bruselu dne 23.10.2024
C(2024) 7277 final

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) …/...

ze dne 23.10.2024,

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

(Text s významem pro EHP)

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) …/...

ze dne 23.10.2024,

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

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

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

vzhledem k těmto důvodům:

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

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

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

(4) V zájmu zajištění přesných a aktuálních informací by vzor hlášení měl finančním subjektům umožňovat, aby při předkládání průběžné a závěrečné zprávy veškeré dříve

[1] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

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

předložené informace aktualizovaly a v případě potřeby překlasifikovaly závažné incidenty na méně závažné.

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

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

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

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

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

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

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

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

---

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

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

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

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

nařízení by mělo být prováděno v souladu s platnými zásadami ochrany údajů a s ustanoveními nařízení 2018/1725,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1
Vzor pro hlášení závažných incidentů souvisejících s IKT

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

   a) finanční subjekty, které předkládají prvotní oznámení, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 2 nařízení Komise v přenesené pravomoci (EU) 2024/xxx [C(2024) 6901][7], a pokud již mají příslušné informace, mohou vyplnit datová pole, jejichž vyplnění se pro účely prvotního oznámení nevyžaduje, ale vyžaduje se pro účely průběžné nebo závěrečné zprávy;

   b) finanční subjekty, které předkládají průběžnou zprávu, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 3 nařízení v přenesené pravomoci (EU) 2024/xxx [C(2024) 6901], a pokud již mají příslušné informace, mohou vyplnit datová pole, jejichž vyplnění se pro účely průběžné zprávy nevyžaduje, ale vyžaduje se pro účely závěrečné zprávy;

   c) finanční subjekty, které předkládají závěrečnou zprávu, vyplní datová pole vzoru, která odpovídají informacím, jež mají být poskytnuty v souladu s článkem 4 nařízení v přenesené pravomoci (EU) 2024/xxx [C(2024) 6901].

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

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

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

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

[7] Nařízení Komise v přenesené pravomoci (EU) 2024/xxx, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, jež stanoví obsah a lhůty pro prvotní oznámení a průběžnou a závěrečnou zprávu o závažných incidentech souvisejících s IKT a obsah dobrovolného oznámení o významných kybernetických hrozbách. (Úř. věst. L, xxx/xxx, ELI: xxx). [Úřad pro publikace: vložte odkaz na C(2024) 6901]

Článek 2

Současné předkládání prvotního oznámení a průběžné a závěrečné zprávy

Finanční subjekty mohou předložení prvotního oznámení, průběžné zprávy a závěrečné zprávy spojit a podat dvě nebo všechny tyto zprávy současně, pokud již došlo k obnovení běžných činností nebo byla dokončena analýza hlavních příčin a pokud jsou dodrženy lhůty stanovené v článku 5 nařízení Komise v přenesené pravomoci (EU) 2024/xxx [C(2024) 6901].

Článek 3

Opakující se incidenty související s IKT

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

Článek 4

Používání zabezpečených elektronických kanálů

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

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

Článek 5

Překlasifikování závažných incidentů souvisejících s IKT

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

Článek 6

Oznámení o externím zajištění povinného hlášení

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

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

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

Článek 7
Souhrnné hlášení

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

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

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

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

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

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

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

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

Článek 8
Oznámení o významných kybernetických hrozbách

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

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

[8] NAŘÍZENÍ EVROPSKÉ CENTRÁLNÍ BANKY (EU) č. 468/2014 ze dne 16. dubna 2014, kterým se stanoví rámec spolupráce Evropské centrální banky s vnitrostátními příslušnými orgány a vnitrostátními pověřenými orgány v rámci jednotného mechanismu dohledu (Úř. věst. L 141, 14.5.2014, s. 1).

Článek 9
Vstup v platnost

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

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

V Bruselu dne 23.10.2024

Za Komisi
předsedkyně
Ursula VON DER LEYEN