2025/301

20.2.2025

NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2025/301

ze dne 23. října 2024,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy, jež stanoví obsah a lhůty pro prvotní oznámení a průběžnou a závěrečnou zprávu o závažných incidentech souvisejících s IKT a obsah dobrovolného oznámení o významných kybernetických hrozbách

(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 třetí pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) V zájmu zajištění harmonizace a zjednodušení požadavků na podávání oznámení a zpráv o závažných incidentech souvisejících s IKT podle čl. 19 odst. 4 nařízení (EU) 2022/2554 by lhůty pro hlášení závažných incidentů souvisejících s IKT měly být stanoveny tak, aby byl zachován jednotný přístup pro všechny druhy finančních subjektů. Z těchto důvodů by přístup ke stanovení uvedených lhůt měl být rovněž v co největším souladu s požadavky stanovenými ve směrnici Evropského parlamentu a Rady (EU) 2022/2555 ([2]), s nimiž by co do účinku měly být přinejmenším rovnocenné.

(2) Aby se předešlo nepřiměřené zátěži spojené s podáváním zpráv pro finanční subjekty v době, kdy incident související s IKT řeší, měl by se obsah prvotního oznámení omezovat na nejpodstatnější informace. Mají-li příslušné orgány být schopny přijmout náležitá opatření v oblasti dohledu, musí obdržet informace o závažných incidentech souvisejících s IKT pokud možno co nejdříve poté, co finanční subjekt klasifikoval incident související s IKT jako závažný. Lhůta pro předložení prvotního oznámení podle čl. 19 odst. 4 písm. a) nařízení (EU) 2022/2554 poté, co byl incident související s IKT klasifikován jako závažný, by tedy měla být pokud možno co nejkratší, ale zároveň by měla umožňovat flexibilitu, zejména v případě obchodních modelů služeb, které nejsou časově nijak zvlášť časově kritické, pokud finanční subjekty potřebují na zpracování incidentu souvisejícího s IKT poté, co se o něm dozvěděly, více času.

(3) Po obdržení prvotního oznámení by příslušné orgány měly obdržet podrobnější informace o incidentu souvisejícím s IKT v průběžné zprávě a veškeré relevantní informace v závěrečné zprávě. Informace obsažené v těchto zprávách by měly příslušným orgánům umožňovat další posouzení incidentu souvisejícího s IKT a vyhodnocení opatření v oblasti dohledu, která případně budou chtít přijmout.

(4) Lhůty pro hlášení uvedené v čl. 20 prvním pododstavci písm. a) bodě ii) nařízení (EU) 2022/2554 by proto měly vyvažovat potřebu příslušných orgánů obdržet informace rychle a potřebu poskytnout finančním subjektům dostatek času na získání úplných a přesných informací.

(5) S ohledem na kritéria stanovená v čl. 20 prvním pododstavci písm. a) nařízení (EU) 2022/2554 by lhůty pro hlášení neměly představovat nepřiměřenou zátěž pro mikropodniky a jiné finanční subjekty, které se nepovažují za významné. Aby se nadto zabránilo nepřiměřenému zatížení finančních subjektů, měly by lhůty pro hlášení brát v úvahu víkendy a státní svátky.

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

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

(6) Vzhledem k tomu, že oznamování významných kybernetických hrozeb má být dobrovolné, neměl by obsah těchto oznámení představovat pro finanční subjekty zátěž a ve srovnání s informacemi požadovanými v případě závažných incidentů souvisejících s IKT by měl být omezenější.

(7) Toto nařízení vychází z návrhů regulačních technických norem, které Komisi předložily evropské orgány dohledu.

(8) O návrhu regulačních technických norem, z něhož toto nařízení vychází, vedly evropské orgány dohledu otevřené veřejné konzultace, analyzovaly potenciální související náklady a přínosy a požádaly o radu skupinu subjektů zřízenou v souladu s článkem 37 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([3]), (EU) č. 1094/2010 ([4]) a (EU) č. 1095/2010 ([5]).

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Obecné informace, které mají být uvedeny v prvotních oznámeních a průběžných a závěrečných zprávách o závažných incidentech souvisejících s IKT

Finanční subjekty uvedou v prvotním oznámení, průběžné zprávě a závěrečné zprávě podle čl. 19 odst. 4 nařízení (EU) 2022/2554 tyto obecné informace:

a) druh předkládaného dokumentu (prvotní oznámení, průběžná zpráva nebo závěrečná zpráva);

b) název finančního subjektu, jeho identifikační kód právnické osoby (LEI) a druh finančního subjektu podle čl. 2 odst. 1 nařízení (EU) 2022/2554;

c) název a identifikační kód subjektu, který předkládá prvotní oznámení nebo průběžnou či závěrečnou zprávu za finanční subjekt;

d) případně názvy a kódy LEI všech finančních subjektů zahrnutých do souhrnného prvotního oznámení nebo průběžné či závěrečné zprávy;

e) kontaktní údaje osob odpovědných za komunikaci s příslušným orgánem ohledně závažné události související s IKT;

f) případně identifikaci mateřského podniku skupiny, do níž finanční subjekt patří;

g) v případě peněžního dopadu měnu, v níž jsou částky vyčísleny.

([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).

Článek 2

Konkrétní informace, které mají být uvedeny v prvotních oznámeních

Prvotní oznámení podle čl. 19 odst. 4 písm. a) nařízení (EU) 2022/2554 musí obsahovat přinejmenším všechny tyto konkrétní informace:

a) referenční kód incidentu přidělený finančním subjektem;

b) datum zjištění, čas zjištění a klasifikaci incidentu podle článku 8 nařízení Komise v přenesené pravomoci (EU) 2024/1772 ([7]);

c) popis incidentu souvisejícího s IKT;

d) kritéria stanovená v článcích 1 až 8 nařízení v přenesené pravomoci (EU) 2024/1772, na jejichž základě finanční subjekt klasifikoval incident související s IKT jako závažný;

e) členské státy, které jsou incidentem souvisejícím s IKT dotčeny;

f) informace o tom, jak byl incident související s IKT odhalen;

g) informace o původu incidentu souvisejícího s IKT, pokud jsou k dispozici;

h) informace o tom, zda finanční subjekt aktivoval plán zachování provozu;

i) případně informace o překlasifikování incidentu souvisejícího s IKT ze závažného na méně závažný;

j) případné další relevantní informace.

Článek 3

Konkrétní informace, které mají být uvedeny v průběžných zprávách

Průběžné zprávy podle čl. 19 odst. 4 písm. b) nařízení (EU) 2022/2554 musí obsahovat přinejmenším všechny tyto konkrétní informace:

a) případný referenční kód incidentu poskytnutý příslušným orgánem;

b) datum a čas výskytu incidentu souvisejícího s IKT;

c) případně datum a čas, kdy finanční subjekt obnovil své běžné činnosti;

d) informace o tom, jak byla splněna kritéria stanovená v článcích 1 až 8 nařízení v přenesené pravomoci (EU) 2024/1772, na jejichž základě finanční subjekt klasifikoval incident související s IKT jako závažný;

e) druh incidentu souvisejícího s IKT;

f) případné hrozby a techniky použité aktérem hrozby;

g) dotčené funkční oblasti a obchodní procesy;

h) dotčené součásti infrastruktury podporující podnikové procesy;

i) dopad na finanční zájmy klientů;

j) informace o hlášení incidentu souvisejícího s IKT jiným orgánům;

k) dočasná opatření, která finanční subjekt přijal nebo hodlá přijmout k překonání účinků incidentu souvisejícího s IKT;

l) případné informace o ukazatelích narušení.

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

Článek 4

Konkrétní informace, které mají být uvedeny v závěrečných zprávách

Závěrečné zprávy podle čl. 19 odst. 4 písm. c) nařízení (EU) 2022/2554 musí obsahovat všechny tyto konkrétní informace:

a) informace o hlavních příčinách incidentu souvisejícího s IKT;

b) data a časy, kdy byl incident související s IKT vyřešen a kdy byla odstraněna jeho hlavní příčina nebo příčiny;

c) informace o řešení incidentu souvisejícího s IKT;

d) případné informace významné pro orgány příslušné k řešení krize;

e) informace o přímých a nepřímých nákladech a ztrátách, jež z incidentu souvisejícího s IKT vyplývají, a informace o zpětně získaných finančních prostředcích;

f) případné informace o opakujících se incidentech souvisejících s IKT.

Článek 5

Lhůty pro prvotní oznámení a pro průběžnou a závěrečnou zprávu

1. Finanční subjekty předloží prvotní oznámení a průběžnou a závěrečnou zprávu podle čl. 19 odst. 4 písm. a), b) a c) nařízení (EU) 2022/2554 v těchto lhůtách:

a) v případě prvotní zprávy: co nejdříve, v každém případě však do čtyř hodin od klasifikace incidentu souvisejícího s IKT jako závažného incidentu souvisejícího s IKT a nejpozději do 24 hodin od okamžiku, kdy se finanční subjekt o incidentu souvisejícím s IKT dozvěděl;

b) v případě průběžné zprávy: nejpozději do 72 hodin od předložení prvotního oznámení, a to i v případech, kdy se stav nebo způsob řešení incidentu nezměnily, jak je uvedeno v čl. 19 odst. 4 písm. b) nařízení (EU) 2022/2554. Aktualizovanou průběžnou zprávu předloží finanční subjekty bez zbytečného odkladu a v každém případě po obnovení běžných činností;

c) v případě závěrečné zprávy: nejpozději jeden měsíc buď po předložení průběžné zprávy, nebo po předložení případné poslední aktualizované průběžné zprávy.

2. Pokud finanční subjekt neklasifikoval incident související s IKT jako závažný do 24 hodin od okamžiku, kdy se o něm dozvěděl, ale klasifikuje ho jako závažný později, předloží prvotní oznámení do čtyř hodin od klasifikace tohoto incidentu souvisejícího s IKT jako závažného.

3. Finanční subjekty, které nejsou schopny předložit prvotní oznámení, průběžnou zprávu nebo závěrečnou zprávu ve lhůtách stanovených v odstavci 1, uvědomí o této skutečnosti příslušný orgán bez zbytečného odkladu, nejpozději však v příslušných lhůtách pro předložení oznámení nebo zprávy, a vysvětlí důvody tohoto prodlení.

4. Pokud lhůta pro předložení prvotního oznámení, průběžné zprávy nebo závěrečné zprávy připadne na víkendový den nebo státní svátek v členském státě finančního subjektu, který hlášení podává, může finanční subjekt předložit prvotní oznámení, průběžnou zprávu nebo závěrečnou zprávu nejpozději v poledne následujícího pracovního dne.

5. Odstavec 4 se nepoužije pro předložení prvotního oznámení nebo průběžné zprávy úvěrovými institucemi, ústředními protistranami, provozovateli obchodních systémů a dalšími finančními subjekty, které se podle článku 3 směrnice (EU) 2022/2555 považují za základní nebo důležité subjekty.

6. Příslušné orgány mohou rozhodnout, že se odstavec 4 nepoužije pro předložení prvotního oznámení nebo průběžné zprávy jinými finančními subjekty než těmi uvedenými v odstavci 5, které jsou významné nebo mají systemický charakter pro finanční sektor na vnitrostátní nebo unijní úrovni. Příslušné orgány oznámí své rozhodnutí určeným finančním subjektům. Rozhodnutí příslušného orgánu se použije pouze v případě incidentů nahlášených po dni, kdy příslušný orgán oznámil své rozhodnutí určeným finančním subjektům.

Článek 6

Obsah dobrovolného oznámení o významných kybernetických hrozbách

Obsah dobrovolného oznámení týkajícího se kybernetických hrozeb podle čl. 19 odst. 2 nařízení (EU) 2022/2554 zahrnuje všechny tyto údaje:

a) obecné informace o oznamujícím finančním subjektu podle článku 1;

b) datum a čas zjištění významné kybernetické hrozby a další relevantní časová razítka související s významnou kybernetickou hrozbou;

c) popis významné kybernetické hrozby;

d) informace o potenciálním dopadu významné kybernetické hrozby na finanční subjekt, jeho klienty nebo finanční protistrany;

e) klasifikační kritéria, která by v případě naplnění kybernetické hrozby vedla k hlášení závažného incidentu, podle článků 1 až 8 nařízení v přenesené pravomoci (EU) 2024/1772;

f) informace o stavu významné kybernetické hrozby a o případných změnách v její aktivitě;

g) popis případných opatření, která finanční subjekt přijal, aby zabránil naplnění významných kybernetických hrozeb;

h) informace o jakémkoli oznámení významné kybernetické hrozby jiným finančním subjektům nebo orgánům;

i) případné informace o ukazatelích narušení;

j) případné další relevantní informace.

Článek 7

Vstup v platnost

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

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

V Bruselu dne 23. října 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN