Úradný vestník
Európskej únie

SK
Séria L

2025/301

20.2.2025

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

(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 tretí pododsek,

keďže:

(1) S cieľom zabezpečiť harmonizáciu a zjednodušenie požiadaviek na oznamovanie a nahlasovanie závažných incidentov súvisiacich s IKT uvedených v článku 19 ods. 4 nariadenia (EÚ) 2022/2554 by sa lehoty na nahlasovanie závažných incidentov súvisiacich s IKT mali riadiť jednotným prístupom pre všetky typy finančných subjektov. Z týchto dôvodov by sa aj lehoty mali v čo najväčšej možnej miere riadiť konzistentným prístupom k požiadavkám stanoveným v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 ([2]) a mali by im byť aspoň rovnocenné.

(2) Aby sa predišlo neprimeranej nahlasovacej záťaži finančných subjektov v čase, keď riešia incident súvisiaci s IKT, obsah počiatočného oznámenia by sa mal obmedziť na najdôležitejšie informácie. Aby mohli príslušné orgány prijať náležité opatrenia dohľadu, musia dostať informácie o závažných incidentoch súvisiacich s IKT čo najskôr po tom, ako finančný subjekt klasifikoval incident súvisiaci s IKT ako závažný. V dôsledku toho by lehota na predloženie počiatočného oznámenia uvedená v článku 19 ods. 4 písm. a) nariadenia (EÚ) 2022/2554 mala byť čo najkratšia po tom, ako bol incident súvisiaci s IKT klasifikovaný ako závažný, a zároveň by mala umožňovať flexibilitu, najmä v prípade obchodných modelov služieb, ktoré nie sú mimoriadne časovo kritické, ak finančné subjekty potrebujú viac času na riešenie incidentu súvisiaceho s IKT po tom, ako sa o ňom dozvedeli.

(3) Po prijatí počiatočného oznámenia by príslušné orgány mali dostať podrobnejšie informácie o incidente súvisiacom s IKT v priebežnej správe a všetky relevantné informácie v záverečnej správe. Informácie v týchto správach by mali príslušným orgánom umožniť ďalšie posúdenie incidentu súvisiaceho s IKT a vyhodnotenie opatrení dohľadu, ktoré by mohli chcieť prijať.

(4) Lehoty na nahlasovanie uvedené v článku 20 ods. 1 písm. a) bode ii) nariadenia (EÚ) 2022/2554 by preto mali vyvážiť potrebu príslušných orgánov rýchlo získať informácie s potrebou poskytnúť finančným subjektom dostatok času na získanie úplných a presných informácií.

(5) Vzhľadom na kritériá stanovené v článku 20 ods. 1 písm. a) nariadenia (EÚ) 2022/2554 by lehoty na nahlasovanie nemali predstavovať neprimeranú záťaž pre mikropodniky a iné finančné subjekty, ktoré nie sú významné. Okrem toho, aby sa predišlo neprimeranej záťaži finančných subjektov, lehoty na nahlasovanie by mali zohľadňovať víkendy a sviatky.

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

([2]) 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).

(6) Keďže významné kybernetické hrozby sa majú oznamovať dobrovoľne, obsah takýchto oznámení by nemal predstavovať záťaž pre finančné subjekty a mal by byť obmedzenejší ako informácie požadované v prípade závažných incidentov súvisiacich s IKT.

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

(8) Európske orgány dohľadu uskutočnili otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorého toto nariadenie vychádza, analyzovali možné súvisiace náklady a prínosy a požiadali o poradenstvo skupiny zainteresovaných strán zriadené 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]).

(9) 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 z nariadenia (EÚ) 2018/1725,

PRIJALA TOTO NARIADENIE:

Článok 1

Všeobecné informácie, ktoré sa majú poskytnúť v počiatočných oznámeniach a priebežných a záverečných správach o závažných incidentoch súvisiacich s IKT

Finančné subjekty uvedú v počiatočnom oznámení, priebežnej správe a záverečnej správe, ako sa uvádza v článku 19 ods. 4 nariadenia (EÚ) 2022/2554, tieto všeobecné informácie:

a) typ predloženia (počiatočné oznámenie, priebežná správa alebo záverečná správa);

b) názov finančného subjektu, jeho identifikátor právneho subjektu a typ finančného subjektu, ako sa uvádza v článku 2 ods. 1 nariadenia (EÚ) 2022/2554;

c) názov a identifikačný kód subjektu, ktorý predkladá počiatočné oznámenie alebo priebežnú či záverečnú správu za finančný subjekt;

d) v náležitých prípadoch názvy a identifikátory právneho subjektu všetkých finančných subjektov, na ktoré sa vzťahuje súhrnné počiatočné oznámenie alebo priebežná či záverečná správa;

e) kontaktné údaje osôb zodpovedných za komunikáciu s príslušným orgánom o závažnom incidente súvisiacom s IKT;

f) v náležitých prípadoch identifikáciu materského podniku skupiny, do ktorej finančný subjekt patrí;

g) v prípade peňažného vplyvu menu, v ktorej sú sumy vyčíslené.

([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).

Článok 2

Špecifické informácie, ktoré sa majú poskytnúť v počiatočných oznámeniach

Počiatočné oznámenia uvedené v článku 19 ods. 4 písm. a) nariadenia (EÚ) 2022/2554 obsahujú aspoň všetky tieto špecifické informácie:

a) referenčný kód incidentu pridelený finančným subjektom;

b) dátum zistenia, čas zistenia a klasifikáciu incidentu podľa článku 8 delegovaného nariadenia Komisie (EÚ) 2024/1772 ([7]);

c) opis incidentu súvisiaceho s IKT;

d) kritériá stanovené v článkoch 1 až 8 delegovaného nariadenia (EÚ) 2024/1772, na základe ktorých finančný subjekt klasifikoval incident súvisiaci s IKT ako závažný;

e) členské štáty, ktoré sú ovplyvnené incidentom súvisiacim s IKT;

f) informácie o tom, ako bol incident súvisiaci s IKT zistený;

g) ak sú k dispozícii, informácie o pôvode incidentu súvisiaceho s IKT;

h) informácie o tom, či finančný subjekt aktivoval plán kontinuity činností;

i) v náležitých prípadoch informácie o preklasifikovaní incidentu súvisiaceho s IKT zo závažného na menej závažný;

j) ak sú k dispozícii, akékoľvek ďalšie relevantné informácie.

Článok 3

Špecifické informácie, ktoré sa majú poskytnúť v priebežných správach

Priebežné správy uvedené v článku 19 ods. 4 písm. b) nariadenia (EÚ) 2022/2554 obsahujú aspoň všetky tieto špecifické informácie:

a) v náležitých prípadoch referenčný kód incidentu poskytnutý príslušným orgánom;

b) dátum a čas výskytu incidentu súvisiaceho s IKT;

c) v náležitých prípadoch dátum a čas, kedy finančný subjekt obnovil svoje pravidelné činnosti;

d) informácie o tom, ako boli splnené kritériá stanovené v článkoch 1 až 8 delegovaného nariadenia (EÚ) 2024/1772, na základe ktorých finančný subjekt klasifikoval incident súvisiaci s IKT ako závažný;

e) typ incidentu súvisiaceho s IKT;

f) v náležitých prípadoch hrozby a techniky používané aktérom hrozby;

g) dotknuté funkčné oblasti a obchodné procesy;

h) dotknuté komponenty infraštruktúry podporujúce obchodné procesy;

i) vplyv na finančné záujmy klientov;

j) informácie o nahlasovaní incidentov súvisiacich s IKT iným orgánom;

k) dočasné kroky alebo opatrenia, ktoré finančný subjekt prijal alebo plánuje prijať na obnovu po incidente súvisiacom s IKT;

l) v náležitých prípadoch informácie o ukazovateľoch ohrozenia.

([7]) 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).

Článok 4

Špecifické informácie, ktoré sa majú poskytnúť v konečných správach

Konečné správy uvedené v článku 19 ods. 4 písm. c) nariadenia (EÚ) 2022/2554 obsahujú všetky tieto špecifické informácie:

a) informácie o hlavných príčinách incidentu súvisiaceho s IKT;

b) dátumy a časy, kedy bol incident súvisiaci s IKT vyriešený a kedy bola odstránená jeho hlavná príčina (príčiny);

c) informácie o riešení incidentu súvisiaceho s IKT;

d) v náležitých prípadoch informácie relevantné pre orgány na riešenie krízových situácií;

e) informácie o priamych a nepriamych nákladoch a stratách vyplývajúcich z incidentu súvisiaceho s IKT a informácie o finančných náhradách;

f) v náležitých prípadoch informácie o opakujúcich sa incidentoch súvisiacich s IKT.

Článok 5

Lehoty na počiatočné oznámenie a na priebežné a záverečné správy

1. Finančné subjekty predložia počiatočné oznámenie a priebežné a záverečné správy uvedené v článku 19 ods. 4 písm. a), b) a c) nariadenia (EÚ) 2022/2554 v týchto lehotách:

a) v prípade počiatočnej správy: čo najskôr, v každom prípade však do štyroch hodín od klasifikácie incidentu súvisiaceho s IKT ako závažného incidentu súvisiaceho s IKT a najneskôr do 24 hodín od momentu, keď sa finančný subjekt o incidente súvisiacom s IKT dozvedel;

b) v prípade priebežnej správy: najneskôr do 72 hodín od predloženia počiatočného oznámenia, a to aj v prípade, že sa stav alebo spôsob riešenia incidentu nezmenil, ako sa uvádza v článku 19 ods. 4 písm. b) nariadenia (EÚ) 2022/2554. Finančné subjekty predkladajú aktualizovanú priebežnú správu, a to v každom prípade po obnovení pravidelných činností;

c) v prípade záverečnej správy: najneskôr jeden mesiac po predložení priebežnej správy alebo v náležitých prípadoch po poslednej aktualizovanej priebežnej správe.

2. Ak finančný subjekt neklasifikoval incident súvisiaci s IKT ako závažný do 24 hodín od momentu, keď sa finančný subjekt dozvedel o incidente súvisiacom s IKT, ale klasifikuje tento incident súvisiaci s IKT ako závažný neskôr, finančný subjekt predloží počiatočné oznámenie do štyroch hodín od klasifikácie incidentu súvisiaceho s IKT ako závažného incidentu.

3. Finančné subjekty, ktoré nie sú schopné predložiť počiatočné oznámenie, priebežnú správu alebo záverečnú správu v lehotách stanovených v odseku 1, o tom informujú príslušný orgán bez zbytočného odkladu, najneskôr však do uplynutia príslušných lehôt na predloženie oznámenia alebo správy, a vysvetlia dôvody omeškania.

4. Ak lehota na predloženie počiatočného oznámenia, priebežnej správy alebo záverečnej správy pripadne na víkendový deň alebo sviatok v členskom štáte nahlasujúceho finančného subjektu, finančný subjekt môže predložiť počiatočné oznámenie, priebežnú správu alebo záverečnú správu do poludnia nasledujúceho pracovného dňa.

5. Odsek 4 sa neuplatňuje na predloženie počiatočného oznámenia alebo priebežnej správy úverovými inštitúciami, centrálnymi protistranami, prevádzkovateľmi obchodných miest a inými finančnými subjektmi, ktoré sú podľa článku 3 smernice (EÚ) 2022/2555 identifikované ako kľúčové alebo dôležité subjekty.

6. Príslušné orgány môžu rozhodnúť, že odsek 4 sa neuplatňuje na predloženie prvotného oznámenia alebo priebežnej správy finančnými subjektmi inými ako tie, ktoré sú uvedené v odseku 5, ktoré sú významné alebo majú systémový charakter pre finančný sektor na vnútroštátnej úrovni alebo na úrovni Únie. Príslušné orgány oznámia svoje rozhodnutie identifikovaným finančným subjektom. Rozhodnutie príslušného orgánu sa uplatňuje len v súvislosti s incidentmi nahlásenými po dátume oznámenia rozhodnutia príslušným orgánom identifikovaným finančným subjektom.

Článok 6

Obsah dobrovoľného oznamovania o významných kybernetických hrozbách

Obsah dobrovoľného oznamovania v súvislosti s významnými kybernetickými hrozbami, ako sa uvádza v článku 19 ods. 2 nariadenia (EÚ) 2022/2554, zahŕňa všetky tieto informácie:

a) všeobecné informácie o oznamujúcom finančnom subjekte, ako sa uvádza v článku 1;

b) dátum a čas zistenia významnej kybernetickej hrozby a akékoľvek iné relevantné časové pečiatky súvisiace s významnou kybernetickou hrozbou;

c) opis významnej kybernetickej hrozby;

d) informácie o potenciálnom vplyve významnej kybernetickej hrozby na finančný subjekt, jeho klientov alebo finančné protistrany;

e) klasifikačné kritériá, na základe ktorých by bolo možné podať správu o závažnom incidente stanovené v článkoch 1 až 8 delegovaného nariadenia (EÚ) 2024/1772, ak by sa kybernetická hrozba naplnila;

f) informácie o stave významnej kybernetickej hrozby a o akýchkoľvek zmenách v aktivite hrozby;

g) v náležitých prípadoch opis opatrení, ktoré finančný subjekt prijal s cieľom zabrániť naplneniu významných kybernetických hrozieb;

h) informácie o akomkoľvek oznámení významnej kybernetickej hrozby iným finančným subjektom alebo orgánom;

i) v náležitých prípadoch informácie o ukazovateľoch ohrozenia;

j) ak sú k dispozícii, akékoľvek ďalšie relevantné informácie.

Článok 7

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