Úradný vestník
Európskej únie

SK
Séria L

2025/295

13.2.2025

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2025/295

z 24. októbra 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy týkajúce sa harmonizácie podmienok umožňujúcich vykonávanie činností dozoru

(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 41 ods. 2 druhý pododsek,

keďže:

(1) Rámcom pre digitálnu prevádzkovú odolnosť finančného sektora stanoveným nariadením (EÚ) 2022/2554 sa zavádza rámec dozoru Únie nad externými poskytovateľmi služieb informačných a komunikačných technológií (IKT) pre finančný sektor, ktorí sú určení ako kritickí v súlade s článkom 31 uvedeného nariadenia.

(2) Externý poskytovateľ IKT služieb, ktorý sa rozhodne predložiť dobrovoľnú požiadavku, aby bol určený ako kritický, by mal európskemu orgánu dohľadu, ktorý prijíma žiadosť, predložiť všetky informácie potrebné na preukázanie svojej kritickosti v súlade so zásadami a kritériami stanovenými v nariadení (EÚ) 2022/2554. Z tohto dôvodu by informácie, ktoré sa majú uviesť v dobrovoľnej žiadosti, mali byť dostatočne podrobné a úplné, aby umožnili jasné a úplné posúdenie kritickosti podľa článku 31 ods. 11 uvedeného nariadenia. Príslušný európsky orgán dohľadu by mal zamietnuť každú neúplnú žiadosť a požiadať o poskytnutie chýbajúcich informácií.

(3) Právna identifikácia externých poskytovateľov IKT služieb v rozsahu pôsobnosti tohto regulačného technického predpisu by mala byť zosúladená s identifikačným kódom stanoveným vo vykonávacom nariadení Komisie prijatom v súlade s článkom 28 ods. 9 nariadenia (EÚ) 2022/2554.

(4) V nadväznosti na odporúčania, ktoré hlavný orgán dozoru vydal kritickým externým poskytovateľom IKT služieb, by hlavný orgán dozoru mal monitorovať, či kritickí externí poskytovatelia IKT služieb dodržiavajú odporúčania. S cieľom zabezpečiť efektívne a účinné monitorovanie opatrení, ktoré prijali kritickí externí poskytovatelia IKT služieb v súvislosti s týmito odporúčaniami, alebo nápravných opatrení, ktoré vykonali kritickí externí poskytovatelia IKT služieb v súvislosti s týmito odporúčaniami, by hlavný orgán dozoru mal mať možnosť žiadať o správy uvedené v článku 35 ods. 1 písm. c) nariadenia (EÚ) 2022/2554, ktoré by sa mali považovať za priebežné správy o pokroku a záverečné správy.

(5) Na účely posúdenia uvedeného v článku 42 ods. 1 nariadenia (EÚ) 2022/2554, podľa ktorého je hlavný orgán dozoru povinný vyhodnotiť, či je vysvetlenie poskytnuté kritickým externým poskytovateľom IKT služieb dostatočné, by sa oznámenie kritického externého poskytovateľa IKT služieb hlavnému orgánu dozoru o jeho zámere dodržiavať prijaté odporúčania malo doplniť opisom krokov a opatrení, ktoré boli prijaté na zmiernenie rizík uvedených v odporúčaniach, spolu s príslušnými lehotami. Takéto vysvetlenie by malo mať podobu plánu nápravy.

(6) Keďže sa očakáva, že hlavný orgán dozoru posudzuje subdodávateľské dojednania kritického externého poskytovateľa IKT služieb, treba vypracovať vzor na predkladanie informácií o uvedených dojednaniach. Vo vzore by sa mala zohľadniť skutočnosť, že kritickí externí poskytovatelia IKT služieb majú odlišné štruktúry ako finančné subjekty.

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

(7) Keď hlavný orgán dozoru vydá odporúčania kritickému externému poskytovateľovi IKT služieb a po tom, ako príslušné orgány informujú príslušné finančné subjekty o rizikách identifikovaných v týchto odporúčaniach, hlavný orgán dozoru by mal monitorovať a posudzovať, ako kritický externý poskytovateľ IKT služieb vykonáva opatrenia a nápravné opatrenia na dodržiavanie odporúčaní. Príslušné orgány by mali monitorovať a posudzovať rozsah, v akom sú finančné subjekty vystavené rizikám identifikovaným v týchto odporúčaniach. S cieľom zachovať rovnaké podmienky pri vykonávaní svojich príslušných úloh, najmä ak sú riziká identifikované v odporúčaniach závažné a rozdelené medzi veľký počet finančných subjektov vo viacerých členských štátoch, by si príslušné orgány aj hlavný orgán dozoru by si mali navzájom vymieňať všetky relevantné zistenia, ktoré sú potrebné na vykonávanie ich príslušných úloh. Cieľom výmeny informácií je zabezpečiť, aby spätná väzba hlavného orgánu dozoru voči kritickému externému poskytovateľovi IKT služieb vo vzťahu k opatreniam a nápravným opatreniam, ktoré kritický externý poskytovateľ IKT služieb vykonáva, zohľadňovala vplyv na riziká finančných subjektov a aby činnosti dohľadu vykonávané príslušnými orgánmi boli založené na posúdení vykonanom hlavným orgánom dozoru.

(8) Na umožnenie efektívnej a účinnej výmeny informácií by príslušné orgány mali v rámci svojich činností dohľadu posudzovať rozsah, v akom sú finančné subjekty, nad ktorými vykonávajú dozor, vystavené rizikám identifikovaným v odporúčaniach. Toto posúdenie by sa malo vykonávať primerane a spôsobom založeným na riziku. Hlavný orgán dozoru by mal požiadať príslušné orgány o poskytnutie výsledkov tohto posúdenia v konkrétnych prípadoch, keď sú riziká spojené s odporúčaniami závažné a rozdelené medzi veľký počet finančných subjektov vo viacerých členských štátoch. V záujme čo najlepšieho využitia zdrojov príslušných orgánov by mal hlavný orgán dozoru pri žiadaní o poskytnutie výsledkov tohto posúdenia vždy zohľadňovať, že cieľom týchto žiadostí je vyhodnotiť vykonávanie opatrení a nápravných opatrení kritickými externými poskytovateľmi IKT služieb.

(9) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([2]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal 22. júla 2024 svoje stanovisko.

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

(11) Spoločný výbor európskych orgánov dohľadu uskutočnil otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzoval možné súvisiace náklady a prínosy a požiadal o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([3]), Skupinu zainteresovaných strán v poisťovníctve a zaisťovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([4]) a Skupinu zainteresovaných strán v oblasti cenných papierov a trhov zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([5]),

([2]) 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).

([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).

PRIJALA TOTO NARIADENIE:

Článok 1

Informácie, ktoré má poskytnúť externý poskytovateľ IKT služieb v žiadosti, aby bol určený ako kritický

1. Externý poskytovateľ služieb informačných a komunikačných technológií (IKT) predkladá podľa článku 31 ods. 11 nariadenia (EÚ) 2022/2554 v odôvodnenej žiadosti o dobrovoľnú požiadavku, aby bol podľa článku 31 ods. 1 písm. a) nariadenia (EÚ) 2022/2554 určený ako kritický, tieto informácie:

a) názov právnickej osoby;

b) identifikačný kód právneho subjektu;

c) meno kontaktnej osoby a kontaktné údaje kritického externého poskytovateľa IKT služieb;

d) krajina, v ktorej má právnická osoba sídlo;

e) opis podnikovej štruktúry vrátane minimálne informácií o svojej materskej spoločnosti a iných prepojených podnikoch poskytujúcich IKT služby finančným subjektom Únie. Tieto informácie v prípade potreby zahŕňajú:

   i) názov právnických osôb;

   ii) identifikačný kód právneho subjektu;

   iii) krajinu, v ktorej má právnická osoba sídlo;

f) odhad trhového podielu externého poskytovateľa IKT služieb vo finančnom sektore Únie a odhad trhového podielu podľa typu finančného subjektu, ako sa uvádza v článku 2 ods. 1 nariadenia (EÚ) 2022/2554, v roku predloženia žiadosti, aby bol určený ako kritický, a v roku pred podaním žiadosti;

g) opis každej IKT služby poskytovanej finančným subjektom Únie vrátane:

   i) opisu povahy obchodnej činnosti a druhu IKT služieb poskytovaných finančným subjektom;

   ii) zoznamu funkcií finančných subjektov, ktoré sú podporované poskytovanými IKT službami, ak sú k dispozícii;

   iii) informácií o tom, či IKT služby poskytované finančným subjektom podporujú kritické alebo dôležité funkcie, ak sú k dispozícii;

h) zoznam finančných subjektov, ktoré využívajú IKT služby poskytované externým poskytovateľom IKT služieb, vrátane nasledujúcich informácií pre každý z finančných subjektov, ktorým sa poskytuje služba, ak sú k dispozícii:

   i) názov právnickej osoby;

   ii) identifikačný kód právneho subjektu, ak je známy externému poskytovateľovi IKT služieb;

   iii) typ finančného subjektu v zmysle vymedzenia v článku 2 ods. 1 nariadenia (EÚ) 2022/2554;

   iv) geografická poloha, z ktorej sa IKT služby poskytujú uvedenému konkrétnemu právnemu subjektu;

i) zoznam kritických externých poskytovateľov IKT služieb uvedených v najnovšom dostupnom zozname takýchto poskytovateľov uverejnenom európskymi orgánmi dohľadu podľa článku 31 ods. 9 nariadenia (EÚ) 2022/2554, ktorí závisia od služieb poskytovaných žiadateľom, ak sú k dispozícii;

j) sebahodnotenie, pokiaľ ide o tieto aspekty:

   i) stupeň nahraditeľnosti každej IKT služby poskytovanej žiadateľom vzhľadom na tieto aspekty:

      — trhový podiel externého poskytovateľa IKT služieb v rámci finančného sektora Únie;

— počet známych relevantných konkurentov podľa druhu IKT služieb alebo skupiny IKT služieb;

— opis osobitostí vo vzťahu k ponúkaným IKT službám, a to aj vo vzťahu k akejkoľvek proprietárnej technológii, alebo špecifických vlastností organizácie alebo činnosti daného externého poskytovateľa IKT služieb;

ii) poznatky o dostupnosti alternatívnych externých poskytovateľov IKT služieb na poskytovanie rovnakých IKT služieb, aké poskytuje externý poskytovateľ IKT služieb predkladajúci žiadosť;

k) informácie o budúcej obchodnej stratégii v súvislosti s poskytovaním IKT služieb a infraštruktúry finančným subjektom v Únii vrátane všetkých plánovaných zmien v skupine alebo riadiacej štruktúre, vstupu na nové trhy alebo činností;

l) identifikácia subdodávateľov externého poskytovateľa IKT služieb, ktorí boli určení ako kritickí externí poskytovatelia IKT služieb;

m) všetky iné dôvody relevantné pre žiadosť externého poskytovateľa IKT služieb, aby bol určený ako kritický.

2. Ak externý poskytovateľ IKT služieb patrí do skupiny, informácie uvedené v odseku 1 sa predkladajú vo vzťahu k IKT službám, ktoré poskytuje skupina ako celok.

Článok 2

Obsah, štruktúra a formát informácií, ktoré majú predložiť, zverejniť alebo oznámiť kritickí externí poskytovatelia IKT služieb

1. Kritickí externí poskytovatelia IKT služieb predkladajú hlavnému orgánu dozoru na jeho žiadosť všetky informácie, ktoré hlavný orgán dozoru potrebuje na vykonávanie svojich povinností v oblasti dozoru v súlade s požiadavkami nariadenia (EÚ) 2022/2554.

2. Informácie uvedené v odseku 1 obsahujú okrem iného tieto faktory:

a) informácie o dojednaniach a kópie zmluvných dokumentov medzi:

i) kritickým externým poskytovateľom IKT služieb a finančnými subjektmi uvedenými v článku 2 ods. 1 nariadenia (EÚ) 2022/2554;

ii) kritickým externým poskytovateľom IKT služieb a jeho subdodávateľmi s cieľom zachytiť technologický hodnotový reťazec IKT služieb poskytovaných finančným subjektom v Únii;

b) informácie o organizačnej a skupinovej štruktúre kritického externého poskytovateľa IKT služieb vrátane identifikácie všetkých subjektov patriacich do tej istej skupiny, ktoré priamo alebo nepriamo poskytujú IKT služby finančným subjektom v Únii;

c) informácie o hlavných akcionároch vrátane ich štruktúry a geografického rozloženia, ak ide o niektorý z týchto subjektov:

i) subjekty, ktoré majú v držbe samostatne alebo spoločne so subjektmi, ktoré sú s nimi prepojené, 25 % alebo viac kapitálu alebo hlasovacích práv kritického externého poskytovateľa IKT služieb;

ii) subjekty, ktoré majú právo vymenúvať alebo odvolávať väčšinu členov správneho, riadiaceho alebo dozorného orgánu kritického externého poskytovateľa IKT služieb;

iii) subjekty, ktoré podľa dohody kontrolujú väčšinu hlasovacích práv akcionárov alebo členov v kritickom externom poskytovateľovi IKT služieb;

d) informácie o trhovom podiele kritického externého poskytovateľa IKT služieb podľa druhu služieb na relevantných trhoch, na ktorých pôsobí;

e) informácie o vnútorných mechanizmoch správy a riadenia kritického externého poskytovateľa IKT služieb vrátane štruktúry s líniami zodpovednosti za riadenie a pravidlami zodpovednosti;

f) zápisnice zo zasadnutí riadiaceho orgánu kritického externého poskytovateľa IKT služieb a všetkých iných príslušných vnútorných výborov, ktoré sa akýmkoľvek spôsobom týkajú činností a rizík týkajúcich sa externých IKT služieb, ktoré podporujú funkcie finančných subjektov v Únii;

g) informácie o bezpečnosti IKT kritického externého poskytovateľa IKT služieb vrátane príslušných stratégií, cieľov, politík, postupov, protokolov, procesov, kontrolných opatrení na ochranu citlivých údajov, kontrol prístupu, postupov šifrovania, plánov reakcie na incidenty a informácií o dodržiavaní všetkých príslušných predpisov a prípadne vnútroštátnych a medzinárodných noriem;

h) informácie o technických a organizačných opatreniach na zabezpečenie ochrany údajov a dôvernosti údajov vrátane osobných a iných ako osobných údajov, zavedených kontrolných opatrení na ochranu citlivých údajov, prístupu, kontrol postupov šifrovania, plánu reakcie na porušenie ochrany údajov. Ak v súvislosti so spracúvaním osobných údajov externý poskytovateľ IKT služieb podlieha právnym predpisom tretích krajín vrátane žiadosti vlády tretej krajiny o prístup, zoznam krajín a uplatniteľných právnych predpisov:

i) informácie o mechanizmoch prenosnosti údajov, prenosnosti aplikácií a interoperability, ktoré kritický externý poskytovateľ IKT služieb ponúka finančným subjektom Únie;

j) informácie o umiestnení dátových centier a centier poskytovania IKT používaných na účely poskytovania služieb finančným subjektom vrátane zoznamu všetkých relevantných priestorov a zariadení kritického externého poskytovateľa IKT služieb, a to aj mimo Únie;

k) informácie o poskytovaní služieb kritickým externým poskytovateľom IKT služieb z tretích krajín vrátane informácií o príslušných právnych ustanoveniach uplatniteľných na osobné a iné ako osobné údaje spracúvané externým poskytovateľom IKT služieb;

l) informácie o opatreniach prijatých na riešenie rizík vyplývajúcich z poskytovania IKT služieb kritickým externým poskytovateľom IKT služieb a jeho subdodávateľmi z tretích krajín;

m) informácie o rámci riadenia rizík a rámci riadenia incidentov vrátane politík, postupov, nástrojov, mechanizmov a mechanizmov správy a riadenia kritického externého poskytovateľa IKT služieb a jeho subdodávateľov vrátane zoznamu a opisu závažných incidentov s priamym alebo nepriamym vplyvom na finančné subjekty v Únii vrátane relevantných údajov na určenie závažnosti incidentu na finančné subjekty a posúdenie možných cezhraničných vplyvov;

n) informácie o rámci riadenia zmien vrátane politík, postupov a kontrol kritického externého poskytovateľa IKT služieb a jeho subdodávateľov;

o) informácie o celkovom rámci reakcie a obnovy kritického externého poskytovateľa IKT služieb vrátane plánov kontinuity činností a súvisiacich opatrení a postupov, politiky životného cyklu vývoja softvéru, plánov reakcie a obnovy a súvisiacich opatrení a postupov, politík týkajúcich sa opatrení a postupov zálohovania;

p) informácie o monitorovaní výkonnosti, monitorovaní bezpečnosti a sledovaní incidentov, ako aj informácie o mechanizmoch nahlasovania týkajúcich sa výkonnosti služieb, incidentov a súladu s dohodnutými dohodami o úrovni poskytovaných služieb a cieľmi týkajúcimi sa úrovne služieb alebo podobnými dojednaniami medzi kritickými externými poskytovateľmi IKT služieb a finančnými subjektmi v Únii;

q) informácie o externom rámci riadenia IKT kritického externého poskytovateľa IKT služieb, vrátane stratégií, politík, postupov, procesov a kontrol vrátane údajov o náležitej starostlivosti a posúdení rizika, ktoré vykonal kritický externý poskytovateľ IKT služieb u svojich subdodávateľov pred uzavretím dohody s nimi a s cieľom monitorovať vzťah zahŕňajúci všetky príslušné IKT riziká a riziká protistrany;

r) extrakcie z monitorovacích a skenovacích systémov kritického externého poskytovateľa IKT služieb a jeho subdodávateľov, ktoré zahŕňajú okrem iného monitorovanie siete, monitorovanie serverov, monitorovanie aplikácií, monitorovanie bezpečnosti, skenovanie zraniteľnosti, riadenie záznamov (logov), monitorovanie výkonnosti, riadenie incidentov a merania vzhľadom na ciele spoľahlivosti, ako sú ciele týkajúce sa úrovne služieb;

s) extrakcie z každého výrobného, predvýrobného a testovacieho systému alebo aplikácie, ktoré používa kritický externý poskytovateľ IKT služieb a jeho subdodávatelia na priame alebo nepriame poskytovanie služieb finančným subjektom v Únii;

t) správy o dodržiavaní súladu a dostupné audítorské správy, ako aj všetky relevantné zistenia auditu vrátane auditov vykonaných vnútroštátnymi orgánmi v Únii a mimo Únie, ak sa v dohodách o spolupráci s príslušnými orgánmi stanovuje takáto výmena informácií, alebo certifikácie, ktoré získal kritický externý poskytovateľ IKT služieb alebo jeho subdodávatelia, vrátane správ od interných a externých audítorov, certifikácií alebo posúdení súladu s normami platnými v jednotlivých odvetviach. Zahŕňa to informácie o každom type dostupného nezávislého testovania odolnosti IKT systémov kritického externého poskytovateľa IKT služieb vrátane každého typu penetračného testovania na základe konkrétnej hrozby vykonávaného externým poskytovateľom IKT služieb;

u) informácie o všetkých posúdeniach vykonaných kritickým externým poskytovateľom IKT služieb na jeho žiadosť alebo v jeho mene, ktorými sa vyhodnocuje vhodnosť a integrita osôb zastávajúcich kľúčové pozície v rámci kritického externého poskytovateľa IKT služieb;

v) informácie o každom pláne nápravy na riešenie odporúčaní podľa článku 3 a príslušné súvisiace informácie na potvrdenie vykonania nápravných opatrení;

w) informácie o dostupných systémoch odbornej prípravy zamestnancov a programoch zvyšovania informovanosti o bezpečnosti vrátane, ak je to relevantné, informácií o investíciách, zdrojoch a metódach kritického externého poskytovateľa IKT služieb, pokiaľ ide o odbornú prípravu zamestnancov v oblasti zaobchádzania s citlivými finančnými údajmi a zachovávania vysokej úrovne bezpečnosti;

x) informácie o činnostiach kritického externého poskytovateľa IKT služieb a finančné výkazy vrátane informácií o rozpočte a zdrojoch súvisiacich s IKT a bezpečnosťou.

Článok 3

Informácie od kritických externých poskytovateľov IKT služieb po vydaní odporúčaní

1. Kritický externý poskytovateľ IKT služieb poskytuje hlavnému orgánu dozoru správu obsahujúcu plán nápravy v súvislosti s odporúčaniami a nápravnými opatreniami, ktoré kritický externý poskytovateľ IKT služieb plánuje vykonať s cieľom zmierniť riziká identifikované v odporúčaniach uvedených v článku 35 ods. 1 písm. d) nariadenia (EÚ) 2022/2254. Správa musí byť v súlade s harmonogramom stanoveným hlavným orgánom dozoru pre každé odporúčanie.

2. Aby sa umožnilo monitorovanie vykonávania opatrení, ktoré prijal uskutočnil kritický externý poskytovateľ IKT služieb v súvislosti s prijatými odporúčaniami, alebo nápravných opatrení, ktoré uskutočnil kritický externý poskytovateľ IKT služieb v súvislosti s prijatými odporúčaniami, kritický externý poskytovateľ IKT služieb na požiadanie predkladá hlavnému orgánu dozoru tieto správy:

a) priebežné správy o pokroku a súvisiace podporné dokumenty, v ktorých sa upresňuje pokrok pri vykonávaní krokov a opatrení stanovených v správe, ktorú hlavnému orgánu dozoru poskytuje kritický externý poskytovateľ IKT služieb v lehote stanovenej hlavným orgánom dozoru;

b) záverečné správy a súvisiace podporné dokumenty, v ktorých sa upresňujú opatrenia, ktoré prijal kritický externý poskytovateľ IKT služieb, alebo nápravné opatrenia, ktoré uskutočnil kritický externý poskytovateľ IKT služieb v záujme zmiernenia rizík identifikovaných v prijatých odporúčaniach.

Článok 4

Štruktúra a formát informácií, ktoré predkladajú kritickí externí poskytovatelia IKT služieb

1. Kritický externý poskytovateľ IKT služieb predkladá požadované informácie hlavnému orgánu dozoru prostredníctvom špecializovaných zabezpečených elektronických kanálov, ktoré hlavný orgán dozoru uviedol vo svojej žiadosti, a to v podobe stanovenej hlavným orgánom dozoru.

2. Pri predkladaní informácií hlavnému orgánu dozoru externí poskytovatelia kritických IKT služieb:

a) dodržiavajú štruktúru, ktorú hlavný orgán dozoru uviedol vo svojej žiadosti o informácie;

b) jasne umiestňujú príslušné informácie v predloženej dokumentácii.

3. Informácie, ktoré hlavnému orgánu dozoru predkladá, zverejňuje alebo oznamuje kritický externý poskytovateľ IKT služieb, musia byť v jazyku bežne používanom v oblasti medzinárodných financií.

Článok 5

Vzor na predkladanie informácií o subdodávateľských dojednaniach

Kritický externý poskytovateľ IKT služieb, od ktorého sa vyžaduje výmena informácií o subdodávateľských dojednaniach, poskytuje informácie hlavnému orgánu dozoru podľa vzoru uvedeného v prílohe.

Článok 6

Posúdenie rizík, ktoré sú identifikované v odporúčaniach hlavného orgánu dozoru príslušnými orgánmi

1. Príslušný orgán v rámci dohľadu nad finančnými subjektmi posudzuje vplyv opatrení, ktoré prijal kritický externý poskytovateľ IKT služieb, na finančné subjekty na základe odporúčaní hlavného orgánu dozoru v súlade so zásadou proporcionality.

2. Pri vykonávaní posúdenia uvedeného v odseku 1 príslušný orgán zohľadňuje všetky tieto aspekty:

a) primeranosť a koherentnosť opravných a nápravných opatrení prijatých finančnými subjektmi na zmiernenie rizík identifikovaných v odporúčaniach;

b) posúdenie hlavným orgánom dozoru týkajúce sa dodržiavania súladu kritického externého poskytovateľa IKT služieb s opatreniami a krokmi zahrnutými v správe, ak to má vplyv na vystavenie finančných subjektov, ktoré sa nachádzajú v rozsahu jeho pôsobnosti, rizikám identifikovaným v odporúčaniach;

c) stanovisko akýchkoľvek iných príslušných orgánov, s ktorými sa konzultovalo v súlade s článkom 42 ods. 5 nariadenia (EÚ) 2022/2554;

d) či hlavný orgán dozoru považoval opatrenia a nápravné opatrenia vykonané kritickým externým poskytovateľom IKT služieb za primerané na zmiernenie vystavenia finančných subjektov, ktoré sa nachádzajú v rozsahu jeho pôsobnosti, rizikám identifikovaným v odporúčaniach.

3. Na žiadosť hlavného orgánu dozoru príslušný orgán poskytuje výsledky posúdenia uvedeného v odseku 1 v primeranom čase. Pri žiadaní o výsledky tohto posúdenia hlavný orgán dozoru zvažuje zásadu proporcionality a rozsah rizík spojených s odporúčaniami vrátane cezhraničných vplyvov týchto rizík, ak majú vplyv na finančné subjekty pôsobiace vo viac ako jednom členskom štáte.

4. Príslušný orgán v prípade potreby požiada finančné subjekty, aby predložili všetky informácie potrebné na vykonanie posúdenia uvedeného v odseku 1.

Článok 7

Nadobudnutie účinnosti

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

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

V Bruseli 24. októbra 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

PRÍLOHA

VZOR NA VÝMENU INFORMÁCIÍ O SUBDODÁVATEĽSKÝCH DOJEDNANIACH

Kategória informácií	Kľúčové informačné prvky
Všeobecné informácie	— Názov kritického externého poskytovateľa IKT služieb. — Identifikačný kód kritického externého poskytovateľa IKT služieb. — Meno kontaktnej osoby a kontaktné údaje kritického externého poskytovateľa IKT služieb. — Dátum predloženia vzoru.
Prehľad subdodávateľských dojednaní	— Mapovanie subdodávateľských dojednaní vrátane krátkeho opisu účelu a rozsahu subdodávateľských vzťahov (vrátane uvedenia úrovne kritickosti alebo významu subdodávateľských dojednaní pre kritického externého poskytovateľa IKT služieb). — Špecifikácia a opis druhov IKT služieb zadaných subdodávateľom, ako aj ich význam pre IKT služby poskytované finančným subjektom v súlade s vykonávacími technickými predpismi prijatými podľa článku 28 ods. 9 nariadenia (EÚ) 2022/2554. — Pri špecifikovaní druhov IKT služieb pozri zoznam v prílohe IV k vykonávacím technickým predpisom prijatým podľa článku 28 ods. 9 nariadenia (EÚ) 2022/2554.
Informácie o subdodávateľoch	— Názov a údaje o právnom subjekte (vrátane identifikačného kódu) za každého subdodávateľa. — Kontaktné údaje zamestnancov zodpovedných za každý zo subdodávateľských vzťahov v riadiacej štruktúre kritického externého poskytovateľa IKT služieb. — Prehľad odborných znalostí, skúseností a kvalifikácií vo vzťahu k zmluvným IKT službám za každého subdodávateľa.
Opis služieb poskytovaných subdodávateľmi	— Podrobný opis konkrétnych IKT služieb poskytovaných každým subdodávateľom. — Rozčlenenie zodpovedností a úloh pridelených subdodávateľom prostredníctvom podrobného opisu rôznych úloh v rôznych fázach procesov IKT. — Informácie o úrovni prístupu, ktorý majú subdodávatelia k osobným alebo inak citlivým údajom alebo systémom, pokiaľ ide o IKT služby poskytované finančným subjektom. — Informácie o lokalitách, z ktorých sa poskytujú služby subdodávateľov, a o opatreniach prijatých na riešenie rizík vyplývajúcich zo služieb poskytovaných mimo Únie.
Správa a riadenie subdodávateľov a dohľad nad nimi	— Opis zmluvného rámca, ako aj rámca správy a riadenia zavedeného na riadenie subdodávateľských vzťahov vrátane doložiek obmedzujúcich používanie citlivých údajov. — Vysvetlenie postupov výberu, zapojenia a monitorovania subdodávateľov. — Prehľad ukazovateľov výkonnosti, cieľov týkajúcich sa úrovne služieb a dohôd o úrovni poskytovaných služieb, ako aj kľúčových ukazovateľov výkonnosti používaných na posúdenie monitorovania výkonnosti a spoľahlivosti subdodávateľa.
Riadenie rizík a dodržiavanie súladu s predpismi	— Posúdenie rizikových profilov subdodávateľa a potenciálneho vplyvu na IKT služby poskytované finančným subjektom. — Vysvetlenie opatrení na zmiernenie rizika zavedených na riešenie rizík súvisiacich so subdodávateľskými vzťahmi. — Údaje o dodržiavaní súladu s príslušnými predpismi zo strany subdodávateľa vrátane noriem v oblasti ochrany údajov a odvetvových noriem.

Kategória informácií	Kľúčové informačné prvky
Plánovanie kontinuity činností a pohotovostné plánovanie	— Prehľad plánov kontinuity činností subdodávateľa a plánov reakcie a obnovy. — Opis zavedených opatrení na zabezpečenie kontinuity služieb v prípade narušenia alebo ukončenia zo strany subdodávateľa. — Frekvencia testov plánov kontinuity činností a plánov reakcie a obnovy zo strany subdodávateľov, dátumy posledných testov za posledné tri roky a špecifikácia, či bol do týchto testov zapojený kritický externý poskytovateľ IKT služieb.
Nahlasovanie	— Opis mechanizmov nahlasovania a frekvencie nahlasovania medzi kritickým externým poskytovateľom IKT služieb a jeho subdodávateľmi.
Náprava a riadenie incidentov	— Náčrt postupov riešenia incidentov, porušení alebo nedodržiavania opatrení súvisiacich so subdodávateľom.
Certifikácie a audity	— Informácie o všetkých certifikátoch, nezávislých auditoch alebo posúdeniach vykonaných u subdodávateľov s cieľom overiť ich bezpečnostné kontroly, normy kvality alebo dodržiavanie súladu s právnymi predpismi. — Dátum a frekvencia auditov subdodávateľov, ktoré vykonal kritický externý poskytovateľ IKT služieb.