Úradný vestník
Európskej únie

SK
Séria L

2024/1773

25.6.2024

DELEGOVANÉ NARIADENIE KOMISIE (EÚ) 2024/1773

z 13.marca 2024,

ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, ktorými sa bližšie spresňuje podrobný obsah politiky v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb

(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 28 ods. 10 tretí pododsek,

keďže:

(1) V rámci pre digitálnu prevádzkovú odolnosť finančného sektora zriadenom nariadením (EÚ) 2022/2554 sa vyžaduje, aby finančné subjekty stanovili určité kľúčové zásady riadenia IKT rizika tretej strany, ktoré majú osobitný význam vtedy, keď finančné subjekty v snahe podporiť svoje kritické alebo dôležité funkcie spolupracujú s externými poskytovateľmi IKT služieb.

(2) Finančné subjekty majú ako súčasť svojho rámca riadenia IKT rizika prijať a pravidelne preskúmavať stratégiu týkajúcu sa IKT rizika tretej strany. V súlade s článkom 28 ods. 2 nariadenia (EÚ) 2022/2554 má uvedená stratégia zahŕňať politiku využívania IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb. Uplatňuje sa na individuálnom a prípadne na subkonsolidovanom a konsolidovanom základe.

(3) Finančné subjekty sa značne líšia veľkosťou, štruktúrou a vnútornou organizáciou, ako aj povahou a zložitosťou svojich činností a operácií. Túto rozmanitosť treba zohľadniť pri ukladaní určitých základných regulačných požiadaviek, ktoré sú vhodné pre všetky finančné subjekty pri vypracúvaní politiky týkajúcej sa zmluvných dojednaní o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie, ktoré poskytujú externí poskytovatelia IKT služieb (ďalej len „politika“), a zabezpečiť, aby sa tieto požiadavky uplatňovali primerane.

(4) Ak finančné subjekty patria do skupiny, materský podnik, ktorý je zodpovedný za zostavovanie konsolidovanej alebo subkonsolidovanej účtovnej závierky skupiny, by mal preto zabezpečiť, aby sa politika uplatňovala v rámci skupiny konzistentne a koherentne.

(5) Pri uplatňovaní tejto politiky by sa vnútroskupinoví poskytovatelia IKT služieb skupiny vrátane tých, ktorí sú v úplnom alebo kolektívnom vlastníctve finančných subjektov v rámci toho istého systému inštitucionálneho zabezpečenia, mali považovať za externých poskytovateľov IKT služieb. Riziká, ktoré predstavujú vnútroskupinoví poskytovatelia IKT služieb, môžu byť odlišné, ale požiadavky, ktoré sa na nich vzťahujú, sú podľa nariadenia (EÚ) 2022/2554 rovnaké. Podobne by sa táto politika mala uplatňovať na subdodávateľov, ktorí poskytujú IKT služby podporujúce kritické alebo dôležité funkcie alebo ich závažné časti externým poskytovateľom IKT služieb, ak existuje reťazec externých poskytovateľov IKT služieb.

(6) Konečná zodpovednosť riadiaceho orgánu za riadenie IKT rizika finančného subjektu je zastrešujúcou zásadou, ktorá je uplatniteľná aj na využívanie externých poskytovateľov IKT služieb. Táto zodpovednosť by sa mala ďalej premietnuť do nepretržitého zapojenia riadiaceho orgánu do kontroly a monitorovania riadenia IKT rizika, a to aj pri prijímaní a preskúmavaní politiky aspoň raz ročne.

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

(7) S cieľom zabezpečiť primerané podávanie správ riadiacemu orgánu by sa v politike mali jasne stanoviť a určiť interné zodpovednosti za schvaľovanie, riadenie, kontrolu a dokumentáciu zmluvných dojednaní o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb (ďalej len „zmluvné dojednania“) vrátane IKT služieb poskytovaných na základe zmluvných dojednaní uvedených v článku 28 ods. 1 písm. a) nariadenia (EÚ) 2022/2554.

(8) V snahe zohľadniť všetky možné riziká, ktoré môžu vzniknúť pri uzatváraní zmlúv o IKT službách podporujúcich kritickú alebo dôležitú funkciu, by sa štruktúra politiky mala riadiť všetkými krokmi každej hlavnej fázy životného cyklu zmluvných dojednaní s externými poskytovateľmi.

(9) Na zmiernenie identifikovaných rizík by sa v politike malo špecifikovať plánovanie zmluvných dojednaní vrátane posúdenia rizík, náležitej starostlivosti a procesu schvaľovania nových alebo závažných zmien týchto zmluvných dojednaní. S cieľom riadiť riziká, ktoré môžu vzniknúť pred uzavretím zmluvného dojednania s externým poskytovateľom IKT služieb, by sa v politike mal stanoviť vhodný a primeraný postup výberu a posudzovania vhodnosti potenciálnych externých poskytovateľov IKT služieb a vyžadovať, aby finančný subjekt zohľadňoval demonštratívny zoznam prvkov, ktoré by mali mať externí poskytovatelia IKT služieb zavedené. Zoznam by mal obsahovať prvky týkajúce sa dobrého mena poskytovateľov služieb, ich finančných, ľudských a technických zdrojov, ich informačnej bezpečnosti, ich organizačnej štruktúry vrátane riadenia rizík a ich vnútorných kontrol.

(10) Na zabezpečenie spoľahlivého riadenia rizík pri poskytovaní IKT služieb podporujúcich kritické alebo dôležité funkcie externými poskytovateľmi IKT služieb by táto politika mala obsahovať informácie o vykonávaní, monitorovaní a riadení zmluvných dojednaní, a to prípadne aj na konsolidovanej a subkonsolidovanej úrovni. Patria sem požiadavky na zmluvné doložky týkajúce sa vzájomných záväzkov finančných subjektov a externých poskytovateľov IKT služieb, ktoré by sa mali stanoviť písomne. S cieľom zabezpečiť účinný dohľad a posilniť odolnosť v prípade zmien obchodného modelu alebo podnikateľského prostredia by sa politikou mali zabezpečiť práva finančných subjektov alebo vymenovaných tretích strán a príslušných orgánov na inšpekcie a prístup k informáciám a mali by sa v nej takisto bližšie určiť stratégie ukončenia angažovanosti a postupy ukončenia.

(11) Pokiaľ u externých poskytovateľov IKT služieb dochádza k spracúvaniu osobných údajov, touto politikou a akýmikoľvek zmluvnými dojednaniami nie sú dotknuté povinnosti vyplývajúce z nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([2]), pričom by ich mali dopĺňať; ide napríklad o povinnosť mať uzavretú písomnú zmluvu, v ktorej sa opisuje spracúvanie osobných údajov, požiadavku na zaistenie bezpečnosti spracúvania osobných údajov a stanovenie všetkých ostatných prvkov požadovaných podľa uvedeného nariadenia.

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Spoločný výbor európskych orgánov uvedený v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([3]), v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([4]) a v článku 54 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([5]) uskutočnil otvorené verejné konzultácie k návrhu regulačných technických predpisov, z ktorých toto nariadenie vychádza, analyzoval potenciálne náklady a prínosy navrhovaných predpisov a požiadal o poradenstvo Skupinu zainteresovaných strán v bankovníctve zriadenú v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010, Skupinu zainteresovaných strán v poisťovníctve a zaisťovníctve a skupinu zainteresovaných strán v dôchodkovom poistení zamestnancov zriadené v súlade s článkom 37 nariadenia Európskeho parlamentu a Rady (EÚ) č. 1094/2010 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.

(13) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([6]) prebehli konzultácie s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal svoje stanovisko 24. januára 2024,

PRIJALA TOTO NARIADENIE:

Článok 1

Celkový rizikový profil a zložitosť

V politike týkajúcej sa využívania IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb (ďalej len „politika“) sa zohľadňuje veľkosť a celkový rizikový profil finančného subjektu, ako aj povaha, rozsah a prvky zvýšenej alebo zníženej zložitosti jeho služieb, činností a operácií vrátane prvkov týkajúcich sa:

a) typu IKT služieb zahrnutých do zmluvného dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb (ďalej len „zmluvné dojednanie“) medzi finančným subjektom a externým poskytovateľom IKT služieb;

b) sídla externého poskytovateľa IKT služieb alebo sídla jeho materského podniku;

c) toho, či IKT služby podporujúce kritické alebo dôležité funkcie poskytuje externý poskytovateľ IKT služieb so sídlom v členskom štáte alebo v tretej krajine, a to aj vzhľadom na miesto, odkiaľ sa IKT služby poskytujú, a na miesto, kde sa údaje spracúvajú a uchovávajú;

d) povahy údajov poskytovaných externému poskytovateľovi IKT služieb;

e) toho, či je externý poskytovateľ IKT služieb súčasťou tej istej skupiny ako finančný subjekt, ktorému sa služby poskytujú;

([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).

f) využívania externých poskytovateľov IKT služieb, ktorí majú povolenie, sú registrovaní alebo podliehajú dohľadu alebo dozoru zo strany príslušného orgánu v členskom štáte alebo ktorí podliehajú rámcu dozoru podľa kapitoly V oddielu II nariadenia (EÚ) 2022/2554, ako aj využívania externých poskytovateľov IKT služieb, ktorí nemajú povolenie, nie sú registrovaní alebo nepodliehajú dohľadu alebo dozoru zo strany príslušného orgánu v členskom štáte alebo ktorí nepodliehajú rámcu dozoru podľa kapitoly V oddielu II nariadenia (EÚ) 2022/2554;

g) využívania externých poskytovateľov IKT služieb, ktorí majú povolenie, sú registrovaní alebo podliehajú dohľadu alebo dozoru zo strany orgánu dohľadu v tretej krajine, ako aj využívania externých poskytovateľov IKT služieb, ktorí nemajú povolenie, nie sú registrovaní alebo nepodliehajú dohľadu alebo dozoru zo strany orgánu dohľadu v tretej krajine;

h) toho, či je poskytovanie IKT služieb podporujúcich kritické alebo dôležité funkcie sústredené na jediného externého poskytovateľa IKT služieb alebo na malý počet takýchto poskytovateľov služieb;

i) prenosnosti IKT služieb podporujúcich kritické alebo dôležité funkcie na iného externého poskytovateľa IKT služieb, a to aj v dôsledku technologických špecifík;

j) potenciálneho vplyvu narušení poskytovania IKT služieb podporujúcich kritické alebo dôležité funkcie na kontinuitu činností finančného subjektu a na dostupnosť jeho služieb.

Článok 2

Uplatňovanie na úrovni skupiny

Ak sa toto nariadenie uplatňuje na subkonsolidovanom alebo konsolidovanom základe, materský podnik, ktorý je zodpovedný za zostavovanie konsolidovanej alebo subkonsolidovanej účtovnej závierky za skupinu, zabezpečí, aby sa politika vykonávala konzistentne vo všetkých finančných subjektoch, ktoré sú súčasťou skupiny, a aby bola primeraná účinnému uplatňovaniu tohto nariadenia na všetkých príslušných úrovniach skupiny.

Článok 3

Mechanizmy správy a riadenia

1. Riadiaci orgán preskúmava politiku aspoň raz ročne a v prípade potreby ju aktualizuje. Zmeny politiky sa vykonajú včas a čo najskôr, ako to je možné v rámci príslušných zmluvných dojednaní. Finančný subjekt zdokumentuje plánovaný harmonogram vykonávania.

2. V snahe určiť, ktoré IKT služby podporujú kritické alebo dôležité funkcie, sa v politike musí stanoviť príslušná metodika alebo uviesť odkaz na ňu. V politike sa takisto uvedie, kedy sa má toto posúdenie vykonať a preskúmať.

3. V politike sa jasne určia interné zodpovednosti za schvaľovanie, riadenie, kontrolu a dokumentáciu príslušných zmluvných dojednaní a zabezpečí sa, aby sa vo finančnom subjekte zachovali primerané zručnosti, skúsenosti a znalosti na účely účinného dozoru nad príslušnými zmluvnými dojednaniami vrátane IKT služieb poskytovaných na základe týchto dojednaní.

4. Bez toho, aby bola dotknutá konečná zodpovednosť finančného subjektu za vykonávanie účinného dozoru nad príslušnými zmluvnými dojednaniami, sa v politike vyžaduje, aby bolo pri externom poskytovateľovi IKT služieb možné konštatovať, že disponuje dostatočnými zdrojmi na zabezpečenie toho, že finančný subjekt spĺňa všetky svoje právne a regulačné požiadavky týkajúce sa poskytovaných IKT služieb podporujúcich kritické alebo dôležité funkcie.

5. V politike sa jasne určí funkcia alebo člen vrcholového manažmentu, ktorí zodpovedajú za monitorovanie príslušných zmluvných dojednaní. V politike sa stanoví, ako uvedená funkcia alebo člen vrcholového manažmentu spolupracuje s kontrolnými funkciami, pokiaľ nie je ich súčasťou, ako aj hierarchické vzťahy voči riadiacemu orgánu vrátane povahy informácií, ktoré sa majú podávať, a dokumentov, ktoré sa majú predkladať. Stanoví sa v nej aj frekvencia takéhoto podávania správ.

6. Touto politikou sa zabezpečí, aby zmluvné dojednania boli v súlade s:

a) rámcom riadenia IKT rizika uvedeným v článku 6 nariadenia (EÚ) 2022/2554;

b) politikou v oblasti informačnej bezpečnosti uvedenou v článku 9 ods. 4 nariadenia (EÚ) 2022/2554;

c) politikou kontinuity činností v oblasti IKT uvedenou v článku 11 nariadenia (EÚ) 2022/2554;

d) požiadavkami na nahlasovanie incidentov uvedenými v článku 19 nariadenia (EÚ) 2022/2554.

7. V politike sa vyžaduje, aby IKT služby podporujúce kritické alebo dôležité funkcie poskytované externými poskytovateľmi IKT služieb podliehali nezávislému preskúmaniu a boli zahrnuté do plánu auditu.

8. V politike sa výslovne stanoví, že zmluvné dojednania:

a) nezbavujú finančný subjekt a jeho riadiaci orgán ich regulačných povinností a zodpovedností voči ich klientom;

b) nebránia účinnému dohľadu nad finančným subjektom a nie sú v rozpore so žiadnymi obmedzeniami zo strany dohľadu nad službami a činnosťami;

c) majú vyžadovať, aby externí poskytovatelia IKT služieb spolupracovali s príslušnými orgánmi;

d) majú vyžadovať, aby finančný subjekt, jeho audítori a príslušné orgány mali účinný prístup k údajom a do objektov, ktoré súvisia s využívaním IKT služieb podporujúcich kritické alebo dôležité funkcie.

Článok 4

Hlavné fázy životného cyklu prijímania a používania zmluvných dojednaní

V politike sa bližšie určia požiadavky vrátane pravidiel, zodpovedností a procesov pre každú hlavnú fázu životného cyklu zmluvného dojednania, pričom obsiahnuté musia byť aspoň tieto prvky:

a) zodpovednosti riadiaceho orgánu vrátane jeho prípadného zapojenia do rozhodovacieho procesu o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb;

b) plánovanie zmluvných dojednaní vrátane posúdenia rizík a náležitej starostlivosti, ako sa uvádza v článkoch 5 a 6, a schvaľovacieho procesu týkajúceho sa nových alebo závažných zmien zmluvných dojednaní podľa článku 8 ods. 4;

c) zapojenie organizačných útvarov, vnútorných kontrol a iných príslušných útvarov v súvislosti so zmluvnými dojednaniami;

d) vykonávanie, monitorovanie a riadenie zmluvných dojednaní uvedených v článkoch 7, 8 a 9, a to prípadne aj na konsolidovanej a subkonsolidovanej úrovni;

e) dokumentácia a vedenie záznamov s prihliadnutím na požiadavky týkajúce sa registra informácií stanoveného v článku 28 ods. 3 nariadenia (EÚ) 2022/2554;

f) stratégia ukončenia angažovanosti a postupy ukončenia, ako sa stanovuje v článku 10.

Článok 5

Posúdenie rizika *ex ante*

1. V politike sa vyžaduje, aby k vymedzeniu obchodných potrieb finančného subjektu došlo pred uzavretím príslušného zmluvného dojednania.

2. V politike sa vyžaduje, aby k posudzovaniu rizík na úrovni finančného subjektu a prípadne na konsolidovanej a subkonsolidovanej úrovni dochádzalo pred uzavretím zmluvného dojednania.

V posúdení rizika sa zohľadňujú všetky príslušné požiadavky stanovené v nariadení (EÚ) 2022/2554 a uplatniteľné odvetvové právne predpisy Únie. Zohľadní sa v ňom najmä vplyv poskytovania IKT služieb podporujúcich kritické alebo dôležité funkcie externými poskytovateľmi IKT služieb na finančný subjekt a všetky riziká, ktoré predstavuje poskytovanie týchto IKT služieb podporujúcich kritické alebo dôležité funkcie externými poskytovateľmi IKT služieb vrátane:

a) operačných rizík;

b) právnych rizík;

c) IKT rizík;

d) rizík poškodenia dobrej povesti;

e) rizík spojených s ochranou dôverných alebo osobných údajov;

f) rizík spojených s dostupnosťou údajov;

g) rizík spojených s miestom, kde sa údaje spracúvajú a uchovávajú;

h) rizík spojených so sídlom externého poskytovateľa IKT služieb;

i) rizík koncentrácie IKT na úrovni subjektu.

Článok 6

Náležitá starostlivosť

1. V politike sa stanoví vhodný a primeraný postup výberu a posudzovania potenciálnych externých poskytovateľov IKT služieb s prihliadnutím na to, či je externý poskytovateľ IKT služieb vnútroskupinovým poskytovateľom IKT služieb alebo nie, pričom sa v nej vyžaduje, aby finančný subjekt pred uzavretím zmluvného dojednania posúdil, či externý poskytovateľ IKT služieb:

a) má dobré meno, dostatočné schopnosti, odborné znalosti a primerané finančné, ľudské a technické zdroje, normy informačnej bezpečnosti, primeranú organizačnú štruktúru, riadenie rizík a vnútorné kontroly, ako aj prípadne požadované povolenia alebo registrácie na spoľahlivé a profesionálne poskytovanie IKT služieb podporujúcich kritickú alebo dôležitú funkciu;

b) dokáže monitorovať relevantný technologický vývoj a identifikovať najlepšie postupy v oblasti bezpečnosti IKT a prípadne ich vykonávať s cieľom mať účinný a spoľahlivý rámec digitálnej prevádzkovej odolnosti;

c) využíva alebo má v úmysle využívať subdodávateľov IKT na vykonávanie IKT služieb podporujúcich kritické alebo dôležité funkcie alebo ich závažné časti;

d) má sídlo alebo spracúva či uchováva údaje v tretej krajine, a ak je to tak, či má tento postup vplyv na úroveň operačného rizika alebo rizika ohrozenia dobrej povesti, alebo na riziko, že bude ovplyvnený reštriktívnymi opatreniami vrátane embarga a sankcií, ktoré môžu ovplyvniť schopnosť externého poskytovateľa IKT služieb poskytovať IKT služby alebo finančného subjektu prijímať tieto IKT služby;

e) súhlasí so zmluvnými dojednaniami, ktorými sa zabezpečuje, že samotný finančný subjekt, vymenované tretie strany a príslušné orgány budú mať reálnu možnosť vykonávať audity externého poskytovateľa IKT služieb, a to aj v jeho priestoroch;

f) koná eticky a sociálne zodpovedne, rešpektuje ľudské práva a práva detí vrátane zákazu detskej práce, dodržiava platné zásady ochrany životného prostredia a zabezpečuje primerané pracovné podmienky.

2. V politike sa bližšie určí požadovaná úroveň zabezpečenia, pokiaľ ide o účinnosť rámca riadenia rizika externých poskytovateľov IKT služieb pre IKT služby podporujúce kritické alebo dôležité funkcie, ktoré má poskytovať externý poskytovateľ IKT služieb. V politike sa vyžaduje, aby postup náležitej starostlivosti zahŕňal posúdenie existencie opatrení na zmiernenie rizika a opatrení na zabezpečenie kontinuity činností, ako aj toho, ako je u externého poskytovateľa IKT služieb zabezpečené ich fungovanie.

3. V politike sa určí postup náležitej starostlivosti pri výbere a posudzovaní potenciálnych externých poskytovateľov IKT služieb a uvádza sa v ňom, ktoré z nasledujúcich prvkov sa majú použiť v súvislosti s požadovanou úrovňou zabezpečenia, pokiaľ ide o výkonnosť externého poskytovateľa IKT služieb:

a) audity alebo nezávislé posúdenia vykonané samotným finančným subjektom alebo v jeho mene;

b) využívanie nezávislých audítorských správ vypracovaných na žiadosť externého poskytovateľa IKT služieb;

c) využívanie audítorských správ vypracovaných funkciou vnútorného auditu externého poskytovateľa IKT služieb;

d) využívanie vhodných certifikácií tretej strany;

e) využívanie iných relevantných informácií, ktoré má finančný subjekt k dispozícii, alebo iných informácií, ktoré poskytol externý poskytovateľ IKT služieb.

4. Finančné subjekty zabezpečia primeranú úroveň zabezpečenia, pokiaľ ide o výkonnosť externého poskytovateľa IKT služieb, pričom zohľadňujú prvky uvedené v odseku 3 písm. a) až e). V prípade potreby sa použije viac ako jeden prvok uvedený v spomínaných písmenách.

Článok 7

Konflikty záujmov

1. V politike sa bližšie určia vhodné opatrenia na identifikáciu, predchádzanie a riadenie skutočných alebo potenciálnych konfliktov záujmov vyplývajúcich z využívania externých poskytovateľov IKT služieb, ktoré sa majú prijať pred uzavretím príslušných zmluvných dojednaní, a zabezpečí sa priebežné monitorovanie takýchto konfliktov záujmov.

2. Ak IKT služby podporujúce kritické alebo dôležité funkcie poskytujú vnútroskupinoví poskytovatelia IKT služieb, v politike sa bližšie určí, že rozhodnutia o podmienkach vrátane finančných podmienok sa v prípade IKT služby majú prijímať objektívne.

Článok 8

Zmluvné doložky

1. V politike sa stanoví, že príslušné zmluvné dojednanie má mať písomnú formu a má zahŕňať všetky prvky uvedené v článku 30 ods. 2 a 3 nariadenia (EÚ) 2022/2554. Politika musí zahŕňať aj prvky týkajúce sa požiadaviek uvedených v článku 1 ods. 1 písm. a) nariadenia (EÚ) 2022/2554 a prípadne aj požiadavky vyplývajúce z iného príslušného práva Únie a vnútroštátneho práva.

2. V politike sa stanoví, že príslušné zmluvné dojednania majú zahŕňať právo finančného subjektu na prístup k informáciám, na vykonávanie inšpekcií a auditov, ako aj na vykonávanie testov IKT. Na tento účel sa v politike vyžaduje, aby finančný subjekt používal nasledujúce metódy bez toho, aby bola dotknutá konečná zodpovednosť finančného subjektu:

a) svoj vlastný vnútorný audit alebo audit vykonaný vymenovanou treťou stranou;

b) v prípade potreby spoločné audity a spoločné testovanie IKT vrátane penetračného testovania na základe konkrétnej hrozby, ktoré sú organizované spoločne s inými obstarávateľskými finančnými subjektmi alebo spoločnosťami, ktoré využívajú IKT služby toho istého externého poskytovateľa IKT služieb, a ktoré vykonávajú uvedené obstarávateľské finančné subjekty alebo spoločnosti alebo nimi určená tretia strana;

c) v prípade potreby certifikácie tretej strany;

d) v prípade potreby interné alebo externé audítorské správy, ktoré dal k dispozícii externý poskytovateľ IKT služieb.

3. Finančný subjekt sa v priebehu času nesmie spoliehať výlučne na certifikácie uvedené v odseku 2 písm. c) alebo na audítorské správy uvedené v písmene d) uvedeného odseku. Touto politikou sa povoľuje používanie metód uvedených v odseku 2 písm. c) a d) len vtedy, ak finančný subjekt spĺňa nasledovné:

a) k svojej spokojnosti sa oboznámil s plánom auditu externého poskytovateľa IKT služieb, pokiaľ ide o príslušné zmluvné dojednania;

b) zabezpečuje, aby sa rozsah certifikácie alebo audítorských správ vzťahoval na identifikované systémy a kľúčové kontroly, a zaisťuje súlad s príslušnými regulačnými požiadavkami;

c) dôkladne priebežne posudzuje obsah certifikácií alebo audítorských správ a overuje, či správy alebo certifikácie nie sú zastarané;

d) zabezpečuje, aby kľúčové systémy a kontroly boli zahrnuté v budúcich verziách certifikácie alebo audítorskej správy;

e) presvedčil sa o schopnostiach strany, ktorá poskytuje certifikáciu alebo vykonáva audit;

f) presvedčil sa o tom, že sa vydávajú certifikácie a že audity sa vykonávajú na základe všeobecne uznávaných príslušných odborných noriem a zahŕňajú skúšku prevádzkovej účinnosti zavedených kľúčových kontrol;

g) má zmluvné právo požadovať s primeranou a legitímnou frekvenciou z hľadiska riadenia rizík, aby sa rozsah certifikácie alebo audítorských správ upravil o iné relevantné systémy a kontroly;

h) má zmluvné právo vykonávať individuálne a spoločné audity podľa vlastného uváženia, pokiaľ ide o zmluvné dojednania, ako aj vykonávať tieto práva v súlade s dohodnutou frekvenciou.

4. Touto politikou sa musí zabezpečiť, aby sa závažné zmeny zmluvného dojednania formalizovali v písomnom dokumente, ktorý obsahuje dátum a podpis všetkých strán a v ktorom sa bližšie určuje postup obnovovania zmluvných dojednaní.

Článok 9

Monitorovanie zmluvných dojednaní

1. V politike sa vyžaduje, aby sa v zmluvných dojednaniach stanovili opatrenia a kľúčové ukazovatele týkajúce sa priebežného monitorovania výkonnosti externých poskytovateľov IKT služieb vrátane opatrení na monitorovanie dodržiavania požiadaviek týkajúcich sa dôvernosti, dostupnosti, integrity a pravosti údajov a informácií a súladu externých poskytovateľov IKT služieb s príslušnými politikami a postupmi finančného subjektu. V politike sa bližšie určia aj opatrenia, ktoré sa uplatňujú v prípade nesplnenia dohôd o úrovni poskytovaných služieb, vrátane prípadných zmluvných pokút.

2. V politike sa bližšie určí, ako má finančný subjekt posudzovať, či externí poskytovatelia IKT služieb využívaní na IKT služby podporujúce kritické alebo dôležité funkcie spĺňajú primerané normy výkonnosti a kvality v súlade so zmluvným dojednaním a vlastnými politikami finančného subjektu. Touto politikou sa zabezpečí najmä, aby:

a) externí poskytovatelia IKT služieb poskytovali finančnému subjektu primerané správy o svojich činnostiach a službách vrátane pravidelných správ, správ o incidentoch, správ o poskytnutí služieb, správ o bezpečnosti IKT a správ o opatreniach na zabezpečenie kontinuity činností a o testovaní;

b) sa výkonnosť externých poskytovateľov IKT služieb posudzovala na základe kľúčových ukazovateľov výkonnosti, kľúčových kontrolných ukazovateľov, auditov, vlastných certifikácií a nezávislých preskúmaní v súlade s rámcom riadenia IKT rizika finančného subjektu;

c) finančný subjekt dostával od externých poskytovateľov IKT služieb ďalšie relevantné informácie;

d) finančný subjekt bol v prípade potreby informovaný o incidentoch súvisiacich s IKT a prevádzkových alebo bezpečnostných incidentoch súvisiacich s platbami;

e) dochádzalo k nezávislým preskúmaniam a auditom, ktorými sa overuje súlad s právnymi a regulačnými požiadavkami a politikami.

3. V politike sa stanoví, že posúdenie uvedené v odseku 2 sa má zdokumentovať a jeho výsledky sa majú použiť na aktualizáciu posúdenia rizika finančného subjektu uvedeného v článku 6.

4. V politike sa stanovia vhodné opatrenia, ktoré má finančný subjekt prijať, ak u externých poskytovateľov IKT služieb zistí nedostatky – vrátane incidentov súvisiacich s IKT a prevádzkových alebo bezpečnostných incidentov súvisiacich s platbami – súvisiace s poskytovaním IKT služieb podporujúcich kritické alebo dôležité funkcie alebo nedostatky týkajúce sa súladu so zmluvnými dojednaniami alebo právnymi požiadavkami. Takisto sa v nej stanoví, ako sa má vykonávanie takýchto opatrení monitorovať, aby sa zabezpečilo ich účinné dodržiavanie vo vymedzenom časovom rámci, pričom sa zohľadňuje závažnosť nedostatkov.

Článok 10

Ukončenie angažovanosti a ukončenie zmluvných dojednaní

Politika musí obsahovať požiadavky na zdokumentovaný plán ukončenia angažovanosti pre každé zmluvné dojednanie a na pravidelné preskúmanie a testovanie zdokumentovaného plánu ukončenia angažovanosti. Pri vypracúvaní plánu ukončenia angažovanosti sa zohľadňujú tieto aspekty:

a) neočakávané a pretrvávajúce výpadky v poskytovaní služieb;

b) neprimerané alebo neúspešné poskytovanie služieb;

c) neočakávané ukončenie zmluvného dojednania.

Plán ukončenia angažovanosti musí byť realistický, uskutočniteľný, založený na vierohodných scenároch a primeraných predpokladoch a musí obsahovať plánovaný harmonogram realizácie zlučiteľný s podmienkami ukončenia angažovanosti a ukončenia zmluvných dojednaní stanovených v zmluvných dojednaniach.

Článok 11

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 13. marca 2024

Za Komisiu
predsedníčka
Ursula VON DER LEYEN