EURÓPSKA
KOMISIA

V Bruseli 24. 9. 2020
COM(2020) 595 final

2020/0266 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014

(Text s významom pre EHP)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

- Dôvody a ciele návrhu

Tento návrh je súčasťou balíka týkajúceho sa digitálnych financií, balíka opatrení zameraných na ďalšie umožňovanie a podporu potenciálu digitálnych financií z hľadiska inovácie a hospodárskej súťaže pri zmierňovaní rizík, ktoré z toho vyplývajú. Je v súlade s prioritami Komisie pripraviť Európu na digitálny vek a vybudovať hospodárstvo pripravené na budúcnosť, ktoré pracuje pre ľudí. Súčasťou balíka týkajúceho sa digitálnych financií je nová stratégia v oblasti digitálnych financií pre finančný sektor EÚ[1], ktorej cieľom je zaistiť, aby EÚ využila digitálnu revolúciu a podnecovala ju na čele s európskymi inovačnými firmami pri sprístupňovaní výhod digitálnych financií spotrebiteľom a podnikom. Popri tomto návrhu balík obsahuje aj návrh nariadenia o trhoch s kryptoaktívami[2], návrh nariadenia o pilotnom režime pre trhové infraštruktúry založené na technológii distribuovanej databázy transakcií (DLT)[3] a návrh smernice na objasnenie alebo zmenu určitých súvisiacich pravidiel EÚ v oblasti finančných služieb[4]. Digitalizácia a prevádzková odolnosť vo finančnom sektore predstavujú dve strany jednej mince. Digitálne alebo informačné a komunikačné technológie (IKT) so sebou prinášajú príležitosti, ako aj riziká. Je potrebné dobre ich pochopiť a riadiť, a to najmä v čase stresu.

Tvorcovia politiky a orgány dohľadu sa preto čoraz viac zameriavali na riziká vyplývajúce zo spoliehania sa na IKT. Snažili sa najmä zvýšiť odolnosť spoločností prostredníctvom stanovovania noriem a koordináciou práce v oblasti regulácie alebo dohľadu. Táto činnosť sa vykonávala na medzinárodnej aj európskej úrovni a naprieč odvetviami, ako aj v niekoľkých osobitných sektoroch vrátane finančných služieb.

IKT riziká však naďalej predstavujú výzvu pre prevádzkovú odolnosť, výkonnosť a stabilitu finančného systému EÚ. Reformou, ktorá nasledovala po finančnej kríze v roku 2008, sa posilnila v prvom rade finančná odolnosť[5] finančného sektora EÚ, pričom IKT riziká sa riešili len nepriamo v niektorých oblastiach ako súčasť opatrení na všeobecnejšie riešenie prevádzkových rizík.

Aj keď zmeny právnych predpisov EÚ v oblasti finančných služieb po kríze priniesli jednotný súbor pravidiel, ktorým sa riadia veľké časti finančných rizík spojených s finančnými službami, digitálna prevádzková odolnosť sa ním úplne nevyriešila. Opatrenia prijaté v súvislosti touto odolnosťou charakterizovali viaceré vlastnosti, ktoré obmedzovali účinnosť týchto opatrení. Napríklad často mali podobu smerníc v oblasti minimálnej harmonizácie alebo nariadení na základe zásad, čím sa ponechával značný priestor na odlišné prístupy na

---

1 Oznámenie Komisie Európskemu Parlamentu, Európskej Rade, Rade, Európskej centrálnej banke, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom Stratégia v oblasti digitálnych financií pre EÚ, 23. septembra 2020, [COM(2020) 591].

2 Návrh nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami, ktorým sa mení smernica (EÚ) 2019/1937, [COM(2020) 593].

3 Návrh nariadenia Európskeho parlamentu a Rady o pilotnom režime pre trhové infraštruktúry založené na technológii distribuovanej databázy transakcií [COM(2020) 594].

4 Návrh smernice Európskeho parlamentu a Rady, ktorou sa menia smernice 2006/43/ES, 2009/65/ES, 2009/138/EÚ, 2011/61/EÚ, 2013/36/EÚ, 2014/65/EÚ, (EÚ) 2015/2366 a EÚ/2016/2341 [COM(2020) 596].

5 Rôzne prijaté opatrenia boli v zásade zamerané na zvýšenie kapitálových zdrojov a likvidity finančných subjektov, ako aj na zníženie trhového a kreditného rizika.

jednotnom trhu. Okrem toho zameranie sa na IKT riziká v kontexte pokrytia prevádzkových rizík bolo len obmedzené alebo neúplné. V konečnom dôsledku sa tieto opatrenia líšia v rámci odvetvových právnych predpisov v oblasti finančných služieb. Intervencia na úrovni Únie preto nebola v úplnom súlade s tým, čo európske finančné subjekty potrebovali na riadenie prevádzkových rizík spôsobom, ktorý odolá vplyvom incidentov v oblasti IKT, ktorý na ne zareaguje alebo od nich uľaví. Ani orgánom finančného dohľadu sa neposkytli najprimeranejšie nástroje na naplnenie ich mandátov na zabránenie finančnej nestabilite pochádzajúcej z prejavenia sa uvedených IKT rizík.

Neexistencia podrobných a komplexných pravidiel o digitálnej prevádzkovej odolnosti na úrovni EÚ viedla k prevládnutiu vnútroštátnych regulačných iniciatív (napr. o testovaní digitálnej prevádzkovej odolnosti) a prístupov orgánov dohľadu (napr. riešenie závislostí IKT od tretej strany). Činnosť na úrovni členských štátov má však len obmedzený účinok vzhľadom na cezhraničnú povahu IKT rizík. Okrem toho nekoordinované národné iniciatívy vyústili do prekrývania, nejednotností, duplicitných požiadaviek, vysokých administratívnych nákladov a nákladov na dodržanie súladu s predpismi, a to najmä v prípade cezhraničných finančných subjektov, alebo do toho, že IKT riziká ostali nezistené, a teda neriešené. V tejto situácii sa triešti jednotný trh, ohrozuje stabilita a integrita finančného sektora EÚ a ohrozuje ochrana spotrebiteľov a investorov.

Je preto nevyhnutné zaviesť podrobný a komplexný rámec pre digitálnu prevádzkovú odolnosť finančných subjektov EÚ. Týmto rámcom sa prehĺbi rozmer riadenia digitálneho rizika jednotného súboru pravidiel. Konkrétne sa zlepší a zjednotí vykonávanie riadenia IKT rizika finančnými subjektmi, stanoví sa dôkladné testovanie systémov IKT, zvýši sa informovanosť orgánov dohľadu o kybernetických rizikách a incidentoch súvisiacich s IKT, ktorým finančné subjekty čelia, ako aj sa zavedú právomoci pre orgány finančného dohľadu dozerať na riziká vyplývajúce zo závislosti finančných subjektov od externých poskytovateľov IKT služieb. Pomocou návrhu sa vytvorí jednotný mechanizmus hlásenia incidentov, ktorý prispeje k zníženiu administratívnej záťaže finančných subjektov a k posilneniu účinnosti dohľadu.

- Súlad s existujúcimi ustanoveniami v tejto oblasti politiky

Tento návrh je súčasťou všeobecnejšej práce, ktorá prebieha na európskej a medzinárodnej úrovni, s cieľom posilniť kybernetickú bezpečnosť vo finančných službách a riešiť všeobecnejšie prevádzkové riziká[6].

Reaguje aj na spoločné technické poradenstvo[7] európskych orgánov dohľadu z roku 2019, v ktorom vyzývali na jednotnejší prístup k riešeniu IKT rizika vo financiách a odporúčali Komisii primeraným spôsobom posilniť digitálnu prevádzkovú odolnosť odvetvia finančných služieb prostredníctvom iniciatívy EÚ zameranej na odvetvie. Poradenstvo európskych orgánov dohľadu bolo reakciou na Akčný plán Komisie pre finančné technológie na rok 2018[8].

- Súlad s ostatnými politikami Únie

[6] Bazilejský výbor pre bankový dohľad, *Kybernetická odolnosť: Škála postupov*, december 2018 a *Zásady správneho riadenia prevádzkového rizika (PSMOR)*, október 2014.

[7] Spoločné poradenstvo európskych orgánov dohľadu pre Európsku komisiu o potrebe legislatívnych zlepšení týkajúcich sa požiadaviek na riadenie IKT rizika vo finančnom sektore EÚ, JC 2019 26 (2019).

[8] Európska komisia, Akčný plán pre finančné technológie [COM(2018) 0109 final].

Ako uviedla predsedníčka von der Leyenová vo svojich politických usmerneniach[9] a ako je stanovené v oznámení s názvom Formovanie digitálnej budúcnosti Európy[10], pre Európu je veľmi dôležité využiť všetky výhody digitálnej doby a posilniť svoj priemysel a kapacitu inovácie v rámci bezpečných a etických hraníc. V Európskej dátovej stratégii[11] sú stanovené štyri piliere – ochrana údajov, základné práva, bezpečnosť a kybernetická bezpečnosť – ako nevyhnutné predpoklady pre spoločnosť posilnenú používaním údajov. Najnovšie Európsky parlament pracuje na správe o digitálnych financiách, v ktorej, okrem iného, vyzýva na spoločný prístup ku kybernetickej bezpečnosti finančného sektora[12]. Legislatívny rámec posilňujúci digitálnu prevádzkovú odolnosť finančných subjektov EÚ je v súlade s týmito politickými cieľmi. Návrhom by sa takisto podporili politiky zamerané na zotavenie sa z koronavírusu, keďže by sa zaistilo, aby zvýšené spoliehanie sa na digitálne financie šlo ruka v ruke s prevádzkovou odolnosťou.

V iniciatíve by sa zachovali výhody spojené s horizontálnym rámcom pre kybernetickú bezpečnosť (napríklad smernica o bezpečnosti sietí a informačných systémov, smernica NIS) udržiavaním finančného sektora v jeho rozsahu pôsobnosti. Finančný sektor by bol naďalej úzko spojený s orgánom pre spoluprácu v oblasti bezpečnosti sietí a informačných systémov a orgány finančného dohľadu by si mohli vymieňať relevantné informácie v rámci existujúceho ekosystému v oblasti bezpečnosti sietí a informačných systémov. Táto iniciatíva by bola v súlade so smernicou o európskej kritickej infraštruktúre, ktorá sa v súčasnosti preskúmava s cieľom zvýšiť ochranu a odolnosť kritických infraštruktúr proti nekybernetickým hrozbám. Na záver, tento návrh je úplne v súlade so stratégiou pre bezpečnostnú úniu[13], v ktorej sa vyzvalo na iniciatívu o digitálnej prevádzkovej odolnosti pre finančný sektor vzhľadom na jeho vysokú závislosť od IKT služieb a jeho vysokú zraniteľnosť voči kybernetickým útokom.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- Právny základ

Návrh nariadenia je založený na článku 114 ZFEÚ.

Odstraňuje prekážky a zlepšuje vytvorenie a fungovanie vnútorného trhu s finančnými službami harmonizovaním pravidiel uplatňujúcich sa na oblasť riadenia, vykazovania, testovania IKT rizika a IKT rizika tretej strany. Súčasné rozdiely v tejto oblasti na legislatívnej úrovni aj úrovni dohľadu, ako aj na vnútroštátnej úrovni a úrovni EÚ pôsobia ako prekážky jednotného trhu s finančnými službami, pretože finančné subjekty vykonávajúce cezhraničné činnosti čelia odlišným, ak niekedy nie prekrývajúcim sa regulačným

---

9 Predsedníčka Ursula Von Der Leyenová, Politické usmernenia pre budúcu Európsku komisiu, 2019 – 2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_sk.pdf.

10 Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom *Formovanie digitálnej budúcnosti Európy* [COM(2020) 67 final].

11 Oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov *Európska dátová stratégia* [COM(2020) 66 final].

12 Správa s odporúčaniami pre Komisiu o digitálnych financiách: vznikajúce riziká v kryptoaktívach – regulačné výzvy a výzvy v oblasti dohľadu v oblasti finančných služieb, inštitúcií a trhov [2020/2034(INL)], https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 Oznámenie Komisie Európskemu parlamentu, Európskej rade, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom „Stratégia EÚ pre bezpečnostnú úniu“ [COM(2020) 605 final].

požiadavkám alebo očakávaniam dohľadu s potenciálom obmedziť vykonávanie ich slobôd usadiť sa a poskytovať služby. Rozdielne pravidlá takisto narúšajú hospodársku súťaž medzi finančnými subjektmi rovnakého druhu v rôznych členských štátoch. Okrem toho v oblastiach, v ktorých harmonizácia chýba alebo je čiastočná či obmedzená, môže vývoj odlišných vnútroštátnych pravidiel či prístupov, buď už účinných alebo v procese prijímania a zavádzania na vnútroštátnej úrovni, pôsobiť ako bránenie v slobodách jednotného trhu s finančnými službami. Toto osobitne platí, pokiaľ ide o rámce pre digitálne prevádzkové testovanie a dozor nad externými poskytovateľmi kritických IKT služieb.

Keďže návrh má vplyv na viacero smerníc Európskeho parlamentu a Rady prijatých na základe článku 53 ods. 1 ZFEÚ, zároveň sa prijíma aj návrh smernice, aby sa zohľadnili nevyhnutné zmeny uvedených smerníc.

- Subsidiarita

Veľká miera vzájomnej prepojenosti medzi finančnými službami, významná cezhraničná činnosť finančných subjektov a rozsiahla závislosť finančného sektora ako celku od externých poskytovateľov IKT služieb si vyžadujú umožnenie silnej digitálnej prevádzkovej odolnosti ako verejného záujmu s cieľom zachovať dobrý stav finančných trhov EÚ. Nerovnosti vyplývajúce z nerovnakých či čiastkových režimov, prekrývania alebo viacerých požiadaviek uplatňujúcich sa na rovnaké finančné subjekty, ktoré pôsobia cezhranične alebo sú držiteľmi viacerých povolení[14] na jednotnom trhu možno účinne vyriešiť len na úrovni Únie.

Týmto návrhom sa harmonizuje digitálna prevádzková zložka hlboko integrovaného a vzájomne prepojeného sektora, ktorý už využíva jednotný súbor pravidiel a dohľadu vo väčšine ostatných kľúčových oblastí. V prípade záležitostí, ako je hlásenie incidentov súvisiacich s IKT, by len harmonizované pravidlá Únie mohli znížiť úroveň administratívnej záťaže a finančných nákladov spojených s hlásením rovnakého incidentu súvisiaceho s IKT rôznym orgánom Únie a vnútroštátnym orgánom. Opatrenie na úrovni EÚ je takisto potrebné na uľahčenie vzájomného uznávania výsledkov pokročilého testovania digitálnej prevádzkovej odolnosti subjektov pôsobiacich cezhranične, ktoré v prípade neexistencie pravidiel Únie podliehajú alebo by mohli podliehať odlišným rámcom v rôznych členských štátoch. Len opatrením na úrovni Únie sa dajú vyriešiť rozdiely v prístupoch k testovaniu, ktoré zaviedli členské štáty. Opatrenie na úrovni celej EÚ je takisto potrebné na riešenie chýbajúcich vhodných právomocí dozoru na monitorovanie rizík pochádzajúcich od externých poskytovateľov IKT služieb vrátane rizika koncentrácie a škodlivého vplyvu na finančný sektor EÚ.

- Proporcionalita

Navrhnuté pravidlá neprekračujú rámec toho, čo je potrebné na dosiahnutie cieľov tohto návrhu. Vzťahujú sa len na tie aspekty, ktoré členské štáty nedokážu dosiahnuť samy, a na prípady, v ktorých administratívne zaťaženie a náklady zodpovedajú konkrétnym a všeobecným cieľom, ktoré sa majú dosiahnuť.

Proporcionalita je navrhnutá z hľadiska rozsahu pôsobnosti a intenzity použitím kritérií kvalitatívneho a kvantitatívneho posúdenia. Ich cieľom je zabezpečiť, aby sa nové pravidlá vzťahovali na všetky finančné subjekty a aby zároveň boli prispôsobené rizikám a potrebám ich osobitných charakteristík z hľadiska ich veľkosti a podnikateľských profilov.

[14] Rovnaký finančný subjekt môže mať bankové povolenie, povolenie investičnej spoločnosti a platobnej inštitúcie, pričom každé z nich vydal iný orgán dohľadu v jednom alebo viacerých členských štátoch.

Proporcionalita je takisto zakotvená v pravidlách o riadení IKT rizika, testovaní digitálnej odolnosti, hlásení závažných incidentov súvisiacich s IKT a dozore nad externými poskytovateľmi kritických IKT služieb.

- Výber nástroja

Opatrenia potrebné na spravovanie riadenia IKT rizika, hlásenia incidentov súvisiacich s IKT, testovanie externých poskytovateľov kritických IKT služieb a dozor nad nimi musia byť obsiahnuté v nariadení, aby sa zaistilo, že budú podrobné požiadavky účinne a priamo uplatniteľné jednotne bez toho, aby bola ohrozená proporcionalita a osobitné pravidlá stanovené týmto nariadením. Jednotnosť v riešení digitálnych prevádzkových rizík prispieva k zlepšovaniu dôvery vo finančný systém a zachováva jeho stabilitu. Keďže použitím nariadenia sa pomáha znížiť regulačná zložitosť, podporuje sa konvergencia dohľadu a zvyšuje právna istotu, toto nariadenie takisto prispieva k obmedzeniu nákladov finančných subjektov na dodržiavanie predpisov, najmä v prípade subjektov pôsobiacich cezhranične, čo zase pomôže odstrániť narušenia hospodárskej súťaže.

Pomocou tohto nariadenia sa odstraňujú legislatívne rozdiely a nerovnaké vnútroštátne regulačné prístupy alebo prístupy dohľadu k IKT riziku a odstraňujú sa tak prekážky na jednotnom trhu s finančnými službami, najmä v bezproblémovom uplatňovaní slobody usadiť sa a poskytovať služby v prípade finančných subjektov s cezhraničnou prítomnosťou.

Na záver, jednotný súbor pravidiel bol prevažne vypracovaný prostredníctvom nariadení a jeho aktualizácia o zložku digitálnej prevádzkovej odolnosti by sa mala riadiť rovnakým výberom právneho nástroja.

3. VÝSLEDKY HODNOTENÍ *EX POST*, KONZULTÁCIÍ SO ZAINTERESOVANÝMI STRANAMI A POSÚDENÍ VPLYVU

- Hodnotenia *ex post*/kontroly vhodnosti existujúcich právnych predpisov

Žiadne právne predpisy Únie o finančných službách doteraz neboli zamerané na prevádzkovú odolnosť a žiadne komplexne neriešili riziká vyplývajúce z digitalizácie, a to ani tie, ktorých pravidlá sa všeobecnejšie zaoberajú rozmerom prevádzkového rizika, ktorého podriadenou zložkou je IKT riziko. Intervenciou Únie sa doteraz pomohlo riešiť potreby a problémy, ktoré sa vyskytli v dôsledku finančnej krízy v roku 2008: úverové inštitúcie neboli dostatočne kapitalizované, finančné trhy neboli dostatočne integrované a harmonizácia bola do toho času na minimálnej úrovni. IKT riziko sa vtedy nepovažovalo za prioritu, a preto sa právne rámce pre rôzne čiastkové finančné sektory vyvíjali nekoordinovaným spôsobom. Opatreniami na úrovni Únie sa však dosiahli ich ciele zabezpečenia finančnej stability a vytvorenia jedného súboru prudenciálnych pravidiel a pravidiel trhového správania uplatňujúcich sa na finančné subjekty v celej EÚ. Keďže faktory stimulujúce legislatívnu intervenciu Únie v minulosti neumožnili, aby osobitné alebo komplexné pravidlá riešili široké používanie digitálnych technológií a následných rizík vo financiách, vykonanie explicitného hodnotenia sa javí ako náročné. Vykonanie implicitného hodnotenia a následné legislatívne zmeny sú premietnuté v každom pilieri tohto nariadenia.

- Konzultácie so zainteresovanými stranami

Komisia počas celého procesu prípravy tohto návrhu viedla konzultácie so zainteresovanými stranami, najmä:

i) Komisia viedla špecializovanú otvorenú verejnú konzultáciu (19. decembra 2019 – 19. marca 2020)[15];

ii) Komisia viedla konzultáciu s verejnosťou prostredníctvom úvodného posúdenia vplyvu (19. decembra 2019 – 16. januára 2020)[16];

iii) útvary Komisie viedli konzultácie s odborníkmi členských štátov v expertnej skupine pre bankové, platobné a poisťovacie služby (EGBPI) pri dvoch príležitostiach (18. mája 2020 a 16. júla 2020)[17];

iv) útvary Komisie uskutočnili špecializovaný webinár o digitálnej prevádzkovej odolnosti v rámci série osvetových podujatí v oblasti digitálnych financií v roku 2020 (19. mája 2020).

Účelom verejných konzultácií bolo informovať Komisiu o vývoji a potenciálnom medziodvetvovom rámci EÚ pre digitálnu prevádzkovú odolnosť v oblasti finančných služieb. Z reakcií vyplynula všeobecná podpora pre zavedenie špecializovaného rámca s opatreniami zameranými na štyri oblasti, ktoré boli predmetom konzultácie, pričom sa zároveň zdôraznila potreba zaistiť proporcionalitu a dôsledne riešiť a vysvetliť vzájomné pôsobenie s horizontálnymi pravidlami smernice NIS. Komisii boli doručené dve reakcie na úvodné posúdenie vplyvu, v ktorých sa respondenti zaoberali osobitnými aspektmi súvisiacimi s ich oblasťou činnosti.

Členské štáty vyjadrili na zasadnutí skupiny EGBPI zorganizovanom 18. mája 2020 vysokú podporu posilneniu digitálnej prevádzkovej odolnosti finančného sektora prostredníctvom plánovaných opatrení týkajúcich sa štyroch prvkov stanovených Komisiou. Členské štáty takisto zdôraznili potrebu jasného stanovenia nových pravidiel s pravidlami týkajúcimi sa prevádzkového rizika (v rámci právnych predpisov EÚ v oblasti finančných služieb) a horizontálnymi pravidlami o kybernetickej bezpečnosti (smernica NIS). Počas druhého zasadnutia niektoré členské štáty zdôraznili potrebu zabezpečiť proporcionalitu a zvážiť osobitnú situáciu malých spoločností alebo dcérskych spoločností väčších skupín, ako aj potrebu mať silný mandát pre príslušné vnútroštátne orgány zapojené do dozoru.

Návrh takisto vychádza zo spätnej väzby čerpanej zo zasadnutí, ktoré sa konali so zainteresovanými stranami a orgánmi a inštitúciami EÚ, a je v ňom začlenená. Zainteresované strany vrátane externých poskytovateľov IKT služieb celkovo vyjadrovali podporu. Z analýzy získanej spätnej väzby vyplýva výzva na zachovanie proporcionality a sledovanie prístupu na základe zásad a rizika pri navrhovaní pravidiel. Zo strany inštitúcií prišiel hlavný príspevok od Európskeho výboru pre systémové riziká (ESRB), európskych orgánov dohľadu, Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) a Európskej centrálnej banky (ECB), ako aj od príslušných orgánov členských štátov.

- Získavanie a využívanie odborných znalostí

Komisia sa pri príprave tohto návrhu spoľahla na kvalitatívne a kvantitatívne dôkazy získané z uznávaných zdrojov vrátane dvoch spoločných technických poradenstiev európskych

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

orgánov dohľadu. Toto doplnili dôverné vstupné informácie a verejne dostupné správy od orgánov dohľadu, medzinárodných normotvorných orgánov a vedúcich výskumných inštitúcií, ako aj kvantitatívne a kvalitatívne vstupy od identifikovaných zainteresovaných strán v rámci globálneho finančného sektora.

- Posúdenie vplyvu

K tomuto návrhu je priložené posúdenie vplyvu[18], ktoré bolo predložené výboru pre kontrolu regulácie 29. apríla 2020 a schválené 29. mája 2020. Výbor pre kontrolu regulácie odporučil zlepšenia v niektorých oblastiach s cieľom: i) poskytnúť viac informácií o tom, ako by bola zaistená proporcionalita; ii) lepšie upozorniť na mieru, v ktorej sa uprednostňovaná možnosť líši od spoločného technického poradenstva európskych orgánov dohľadu a prečo je uvedená možnosť optimálna; a iii) podrobnejšie poukázať na to, ako návrh spolupôsobí s existujúcimi právnymi predpismi EÚ vrátane pravidiel, ktoré sa v súčasnosti revidujú. Posúdenie vplyvu bolo nastavené tak, aby sa riešili tieto body, pričom sa riešili aj podrobnejšie pripomienky výboru pre kontrolu regulácie.

Komisia zvážila niekoľko možností politiky pre vývoj rámca pre digitálnu prevádzkovú odolnosť:

- zachovanie súčasnej situácie: pravidlá o prevádzkovej odolnosti by boli naďalej stanovené súčasným rozmanitým súborom ustanovení právnych predpisov EÚ o finančných službách, čiastočne smernicou NIS a existujúcimi alebo budúcimi vnútroštátnymi režimami;
- možnosť 1: posilnenie kapitálových vankúšov: zaviedli by sa ďalšie kapitálové vankúše na zvýšenie schopnosti finančných subjektov absorbovať straty, ktoré by mohli vzniknúť z dôvodu nedostatočnej digitálnej prevádzkovej odolnosti;
- možnosť 2: zavedenie aktu o digitálnej prevádzkovej odolnosti finančných služieb: umožnenie komplexného rámca na úrovni EÚ s jednotnými pravidlami riešiacimi potreby digitálnej prevádzkovej odolnosti všetkých regulovaných finančných subjektov a stanovujúceho rámec dozoru pre externých poskytovateľov kritických IKT služieb;
- možnosť 3: akt o digitálnej prevádzkovej odolnosti finančných služieb v kombinácii s centralizovaným dohľadom nad externými poskytovateľmi kritických IKT služieb: okrem aktu o digitálnej prevádzkovej odolnosti (možnosť 2) by sa zriadil nový orgán pre dohľad nad poskytovaním služieb externých poskytovateľov IKT služieb.

Druhá možnosť sa ponechala, keďže sa ňou dosahuje najviac zamýšľaných cieľov spôsobom, ktorý je účinný, efektívny a je v súlade s inými politikami Únie. Väčšina zainteresovaných strán takisto uprednostňuje túto možnosť.

Ponechaná možnosť by spôsobila náklady jednorazového, ako aj pravidelného charakteru[19]. Jednorazové náklady predstavujú najmä investície do informačných systémov, a preto je zložité ich vyčísliť vzhľadom na rôzny stav komplexných IT prostredí spoločností, a najmä

[18] Pracovný dokument útvarov Komisie – správa o posúdení vplyvu, sprievodný dokument k nariadeniu Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora, ktorým sa menia nariadenia (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014, SWD(2020)198 z 24.09.2020.

[19] *Tamže, s. 89 – 94.*

ich pôvodných informačných systémov. Rovnako budú tieto náklady pravdepodobne nízke v prípade veľkých spoločností vzhľadom na významné investície do IKT, ktoré sa už uskutočnili. Očakáva sa, že náklady budú nízke aj v prípade menších spoločností, pretože by sa uplatňovali primerané opatrenia vzhľadom na ich nižšie riziko.

Zachovaná možnosť by mala kladné účinky na MSP pôsobiace v odvetví finančných služieb z hľadiska hospodárskych, sociálnych a environmentálnych vplyvov. Návrhom sa pre MSP objasní, ktoré pravidlá sa uplatňujú, vďaka čomu sa znížia náklady na dodržiavanie predpisov.

Zachovaná možnosť politiky by mala hlavné sociálne vplyvy na spotrebiteľov a investorov. Vďaka vyšším úrovniam digitálnej prevádzkovej odolnosti finančného systému EÚ by klesol počet incidentov a priemerné náklady na ne. Spoločnosť ako celok by profitovala zo zvýšenej dôvery v odvetvie finančných služieb.

Na záver, z hľadiska environmentálnych vplyvov by zvolená možnosť politiky podnietila lepšie využívanie najnovšej generácie IKT infraštruktúr a služieb, v prípade ktorých sa očakáva, že sa stanú environmentálne udržateľnejšími.

- Regulačná vhodnosť a zjednodušenie

Odstránením prekrývajúcich sa požiadaviek na hlásenie incidentov súvisiacich s IKT by sa znížila administratívna záťaž a klesli by súvisiace náklady. Okrem toho by sa harmonizovaním testovaním digitálnej prevádzkovej odolnosti so vzájomným uznávaním v rámci jednotného trhu znížili náklady, najmä pre cezhraničné spoločnosti, ktoré by inak mohli čeliť viacerým testom v rámci členských štátov[20].

- Základné práva

EÚ je odhodlaná zaistiť vysoké normy ochrany základných práv. Všetky dohody o dobrovoľnom vzájomnom poskytovaní údajov medzi finančnými subjektmi, ktoré sú podporované týmto nariadením, by sa realizovali v dôveryhodných prostrediach pri úplnom rešpektovaní pravidiel Únie v oblasti ochrany údajov, najmä nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679[21], osobitne ak je spracovanie osobných nevyhnutné na účely oprávneného záujmu, ktorý sleduje prevádzkovateľ.

4. VPLYV NA ROZPOČET

Keďže sa v tomto nariadení predpokladá posilnená úloha pre európske orgány dohľadu prostredníctvom im udelených právomocí, aby primerane dozerali nad externými poskytovateľmi kritických IKT služieb, z hľadiska vplyvu na rozpočet by návrh predstavoval využitie zvýšeného objemu zdrojov, najmä na plnenie úloh dozoru (napríklad kontroly na mieste a online, ako aj vykonávanie auditov), a využívanie zamestnancov, ktorí majú osobitné odborné znalosti v oblasti bezpečnosti IKT.

Rozsah a rozdelenie týchto nákladov bude závisieť od rozsahu nových právomocí dozoru a (presných) úloh, ktoré budú európske orgány dohľadu vykonávať. Z hľadiska zabezpečenia zdrojov, pokiaľ ide o nových zamestnancov, EBA, ESMA a EIOPA budú celkovo potrebovať 18 zamestnancov na plný pracovný čas (ekvivalent plného pracovného času) – 6 ekvivalentov

[20] *Tamže.*

[21] 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).

plného pracovného času pre každý orgán – keď sa začnú uplatňovať jednotlivé ustanovenia návrhu (s odhadom na úrovni 15,71 milióna EUR na obdobie rokov 2022 – 2027). Európskym orgánom dohľadu takisto vzniknú ďalšie náklady na IT, výdavky na misie na kontroly na mieste a náklady na preklad (odhad na úrovni 12 miliónov EUR na obdobie rokov 2022 – 2027), ako aj iné administratívne výdavky (odhad na úrovni 2,48 milióna EUR na obdobie rokov 2022 – 2027). Podľa odhadov preto dosiahne vplyv celkových nákladov za obdobie rokov 2022 – 2027 približne 30,19 milióna EUR.

Treba takisto poznamenať, že aj keď počet zamestnancov (napr. noví zamestnanci a iné výdavky súvisiace s novými úlohami) potrebný na priamy dozor bude v priebehu času závisieť od vývoja počtu a veľkosti externých poskytovateľov kritických IKT služieb, nad ktorými sa bude vykonávať dozor, príslušné výdavky budú v celom rozsahu financované z poplatkov vyberaných od uvedených účastníkov trhu. Nepredpokladá sa preto vplyv na rozpočtové prostriedky EÚ (okrem dodatočných zamestnancov), keďže tieto náklady budú plne financované z poplatkov.

Finančný a rozpočtový vplyv tohto návrhu je podrobne objasnený v legislatívnom finančnom výkaze, ktorý je prílohou k tomuto návrhu.

5. INÉ PRVKY

- Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ

Návrh obsahuje všeobecný plán monitorovania a hodnotenia vplyvu na konkrétne ciele, pričom od Komisie sa vyžaduje vykonanie preskúmania najmenej tri roky po nadobudnutí účinnosti a podanie správy Európskemu parlamentu a Rade o jej hlavných zisteniach.

Preskúmanie sa uskutoční v súlade s usmerneniami Komisie pre lepšiu právnu reguláciu.

- Podrobné vysvetlenie konkrétnych ustanovení návrhu

Súčasný návrh je členený do siedmich hlavných oblastí politiky, ktoré predstavujú kľúčové vzájomne súvisiace piliere konsenzuálne zahrnuté do európskych a medzinárodných usmernení a najlepších postupov zameraných na zlepšenie kybernetickej a prevádzkovej odolnosti finančného sektora.

Rozsah pôsobnosti nariadenia a uplatňovanie primeranosti požadovaných opatrení (článok 2)

V záujme zaistenia konzistentnosti týkajúcej sa požiadaviek na riadenie IKT rizika uplatňujúcich sa na finančný sektor sa toto nariadenie vzťahuje na škálu finančných subjektov regulovaných na úrovni Únie, konkrétne na úverové inštitúcie, platobné inštitúcie, inštitúcie elektronického peňažníctva, investičné spoločnosti, poskytovateľov služieb kryptoaktív, centrálnych depozitárov cenných papierov, centrálne protistrany, obchodné miesta, archívy obchodných údajov, správcov AIF a správcovské spoločnosti, poskytovateľov služieb vykazovania údajov, poisťovne a zaisťovne, sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia, inštitúcie zamestnaneckého dôchodkového zabezpečenia, ratingové agentúry, štatutárnych audítorov a audítorské spoločnosti, správcov kritických referenčných hodnôt a poskytovateľov služieb kolektívneho financovania.

Toto pokrytie umožňuje homogénne a jednotné uplatňovanie všetkých súčastí rizikového riadenia na oblasti súvisiace s IKT a zároveň chráni rovnaké podmienky medzi finančnými subjektmi, pokiaľ ide o ich regulačné povinnosti týkajúce sa IKT rizika. V nariadení sa

zároveň uznáva, že medzi finančnými subjektmi existujú významné rozdiely z hľadiska veľkosti, podnikateľských profilov alebo v súvislosti s ich vystavením digitálnemu riziku. Keďže väčšie finančné subjekty majú viac zdrojov, napríklad len od finančných subjektov, ktoré sa nekvalifikujú ako mikropodniky, sa vyžaduje stanoviť komplexný mechanizmus správy, vyhradené funkcie riadenia, vykonávať hĺbkové posúdenia po zásadných zmenách v sieťových infraštruktúrach a infraštruktúrach informačných systémov, pravidelne vykonávať analýzy rizík pôvodných systémov IKT, rozšíriť testovanie kontinuity podnikateľskej činnosti a plány reakcie a obnovy na zachytávanie scenárov prechodu medzi primárnou IKT infraštruktúrou a nadbytočnými zariadeniami. Okrem toho, len finančné subjekty identifikované ako významné na účely pokročilého testovania digitálnej odolnosti budú povinné vykonávať penetračné testy na základe konkrétnej hrozby.

Aj keď je toto pokrytie široké, nie je úplné. Toto nariadenie najmä nezachytáva systémových prevádzkovateľov, ktorí sú vymedzení v článku 2 písm. p) smernice 98/26/ES[22] o konečnom zúčtovaní v platobných systémoch a zúčtovacích systémoch cenných papierov („smernica o konečnom zúčtovaní“), ani žiadneho účastníka systému, pokiaľ samotný účastník nie je finančným subjektom regulovaným na úrovni Únie a ako na takého by sa na neho vzťahovalo toto nariadenie z jeho vlastnej podstaty (t. j. úverová inštitúcia, investičná spoločnosť, CCP). Okrem toho je mimo rozsahu pôsobnosti aj register Únie pre emisné kvóty, ktorý je prevádzkovaný, v súlade so smernicou 2003/87/ES,[23] pod záštitou Európskej komisie.

V týchto vylúčeniach zo smernice o konečnom zúčtovaní sa zohľadňuje potreba podrobnejšieho preskúmania legislatívnych a politických otázok týkajúcich sa systémových prevádzkovateľov a účastníkov podľa smernice o konečnom zúčtovaní s náležitým zvážením vplyvu rámcov, ktoré sa v súčasnosti uplatňujú na platobné systémy[24] prevádzkované centrálnymi bankami. Keďže tieto otázky môžu zahŕňať aspekty, ktoré zostávajú odlišné od problémov, na ktoré sa vzťahuje toto nariadenie, Komisia bude naďalej posudzovať nevyhnutnosť a vplyv ďalšieho rozšírenia rozsahu pôsobnosti tohto nariadenia na subjekty a infraštruktúry IKT, ktoré sú v súčasnosti mimo jeho rozsahu pôsobnosti.

Požiadavky súvisiace so správou (článok 4)

Toto nariadenie je určené na lepšie zosúladenie obchodných stratégií finančných subjektov a vykonávania riadenia IKT rizika. Na tento účel bude riadiaci orgán povinný udržiavať si rozhodujúcu, aktívnu úlohu v riadení rámca pre riadenie IKT rizika a presadzovať rešpektovanie dôslednej kybernetickej hygieny. Úplná zodpovednosť riadiaceho orgánu za riadenie IKT rizika finančného subjektu bude predstavovať všeobecnú zásadu, ktorá sa ďalej pretaví do súboru osobitných požiadaviek, ako je pridelenie jasných úloh a zodpovedností za všetky funkcie súvisiace s IKT, priebežné zapojenie sa do kontroly monitorovania riadenia IKT rizika, ako aj do celej škály schvaľovacích a kontrolných procesov a vhodného prideľovania investícií na IKT a odbornú prípravu.

Požiadavky na riadenie IKT rizika (články 5 až 14)

---

[22] Smernica Európskeho parlamentu a Rady 98/26/ES z 19. mája 1998 o konečnom zúčtovaní v platobných systémoch a zúčtovacích systémoch cenných papierov (Ú. v. ES L 166, 11.6.1998, s. 45).

[23] Smernica 2003/87/ES Európskeho parlamentu a Rady z 13. októbra 2003 o vytvorení systému obchodovania s emisnými kvótami skleníkových plynov v Spoločenstve, a ktorou sa mení a dopĺňa smernica Rady 96/61/ES (Ú. v. EÚ L 275, 25.10.2003, s. 32).

[24] Najmä nariadenie Európskej centrálnej banky (EÚ) č. 795/2014 z 3. júla 2014 o požiadavkách v oblasti dohľadu nad systémovo dôležitými platobnými systémami.

Digitálna prevádzková odolnosť je zakotvená v súbore kľúčových zásad a požiadaviek týkajúcich sa rámca pre riadenie IKT rizika v súlade so spoločným technickým poradenstvom európskych orgánov dohľadu. Tieto požiadavky inšpirované príslušnými medzinárodnými, vnútroštátnymi a odvetvovými normami, usmerneniami a odporúčaniami, sú sústredené okolo osobitných funkcií v riadení IKT rizika (identifikácia, ochrana a prevencia, zistenie, reakcia a obnova, učenie sa a vývoj a komunikácia). Na udržanie tempa s rýchlo sa vyvíjajúcim prostredím kybernetických hrozieb sú finančné subjekty povinné zriadiť a udržiavať odolné IKT systémy a nástroje, ktoré minimalizujú vplyv IKT rizika, identifikovať na priebežnom základe všetky zdroje IKT rizika, nastaviť ochranné a preventívne opatrenia, rýchle zistiť nezvyčajné činnosti, zaviesť špecializované a komplexné politiky v oblasti kontinuity podnikateľskej činnosti a plány obnovy po havárii ako neoddeliteľnej súčasti politiky prevádzkovej kontinuity podnikateľskej činnosti. Tieto posledné uvedené zložky sú nevyhnutné na rýchlu obnovu po incidentoch súvisiacich s IKT, najmä kybernetických útokoch, prostredníctvom obmedzenia škôd a stanovenia priorít v rámci bezpečnej obnovy činností. Samotným nariadením sa neukladá osobitná normalizácia, ale buduje sa na európskych a medzinárodne uznaných technických normách alebo odvetvových najlepších postupoch, pokiaľ sú v plnom rozsahu v súlade s pokynmi orgánov dohľadu týkajúcimi sa používania a začlenenia týchto medzinárodných noriem. Toto nariadenie sa takisto vzťahuje na integritu, bezpečnosť a odolnosť fyzických infraštruktúr a zariadení, ktoré podporujú používanie technológie a príslušných procesov a ľudí súvisiacich s IKT ako súčasti digitálnej stopy operácií finančného subjektu.

Podávanie správ o incidentoch súvisiacich s IKT (články 15 až 20)

Zosúladenie a zjednotenie hlásenia incidentov súvisiacich s IKT sa dosahuje, po prvé, všeobecnou požiadavkou, aby finančné subjekty vytvorili a zaviedli proces riadenia na monitorovanie a zaznamenávanie incidentov súvisiacich s IKT, nasledovaný povinnosťou ich klasifikácie na základe kritérií podrobne stanovených v nariadení a podrobnejšie vyvinutých európskymi orgánmi dohľadu s cieľom stanoviť prahové hodnoty významnosti. Po druhé, príslušným orgánom sa musia nahlasovať len incidenty súvisiace s IKT, ktoré sa považujú za závažné. Toto nahlasovanie by sa malo spracúvať pomocou spoločného vzoru a na základe harmonizovaného postupu, ktorý vypracujú európske orgány dohľadu. Finančné subjekty by mali predkladať úvodné, predbežné a záverečné správy a informovať svojich používateľov a klientov v prípadoch, ak incident má alebo by mohol mať vplyv na ich finančné záujmy. Príslušné orgány by mali poskytnúť podrobnosti týkajúce sa incidentov iným inštitúciám alebo orgánom: európskym orgánom dohľadu, ECB a jednotným kontaktným miestam určeným v súlade so smernicou (EÚ) 2016/1148.

Na začatie dialógu medzi finančnými subjektmi a príslušnými orgánmi, ktorý by prispel k minimalizovaniu vplyvu a určeniu vhodných nápravných opatrení, by hlásenie závažných incidentov súvisiacich s IKT mala sprevádzať spätná väzba a usmernenia dohľadu.

Na záver, možnosť centralizovania hlásenia incidentov súvisiacich s IKT na úrovni Únie by sa mala podrobnejšie preskúmať v spoločnej správe európskych orgánov dohľadu, ECB a ENISA, v ktorej sa posúdi realizovateľnosť vytvorenia jednotného centra EÚ pre hlásenie závažných incidentov súvisiacich s IKT finančnými subjektmi.

Testovanie digitálnej prevádzkovej odolnosti (články 21 až 24)

Je potrebné pravidelne testovať pripravenosť a identifikovať slabé stránky, nedostatky alebo medzery v schopnostiach a funkciách zahrnutých do rámca pre riadenie IKT rizika, ako aj rýchlom vykonaní nápravných opatrení. Toto nariadenie umožňuje primerané uplatňovanie požiadaviek na testovanie digitálnej prevádzkovej odolnosti podľa veľkosti, podnikateľskej činnosti a rizikových profilov finančných subjektov: aj keď všetky subjekty by mali

vykonávať testovanie IKT nástrojov a systémov, len subjekty identifikované príslušnými orgánmi (na základe kritérií uvedených v tomto nariadení a podrobnejšie vypracovaných európskymi orgánmi dohľadu) ako významné a kyberneticky vyspelé by mali byť povinné vykonávať pokročilé testovanie založené na penetračnom testovaní na základe konkrétnej hrozby. V tomto nariadení sa takisto stanovujú požiadavky na testovacie subjekty a uznávanie výsledkov penetračného testovania na základe konkrétnej hrozby v celej Únii pre finančné subjekty pôsobiace vo viacerých členských štátoch.

IKT riziko tretej strany (články 25 až 39)

Nariadenie je určené na zabezpečenie riadneho monitorovania IKT rizika tretej strany. Tento cieľ sa dosiahne, po prvé, dodržiavaním pravidiel na základe zásad uplatňujúcich sa na monitorovanie rizika finančných subjektov pochádzajúcich od externých poskytovateľov IKT. Po druhé, týmto nariadením sa harmonizujú kľúčové prvky služieb a vzťahu s externými poskytovateľmi IKT. Tieto prvky pokrývajú minimálne aspekty považované za veľmi dôležité na umožnenie úplného monitorovania IKT rizika tretej strany finančným subjektom počas celého uzavretia, plnenia, ukončenia a pozmluvných fáz ich vzťahu.

Najdôležitejšie je, že sa bude vyžadovať, aby zmluvy, ktorými sa uvedený vzťah riadi, obsahovali úplný opis služieb, uvedenie miest, na ktorých sa budú spracúvať údaje, úplné opisy úrovne poskytovaných služieb sprevádzané kvantitatívnymi a kvalitatívnymi výkonnostnými cieľmi, príslušné ustanovenia o prístupnosti, dostupnosti, integrite, bezpečnosti a ochrane osobných údajov a záruky týkajúce sa prístupu, obnovy a vrátenia v prípade zlyhaní externých poskytovateľov IKT služieb, výpovedné lehoty a povinnosti podávania správ externými poskytovateľmi IKT služieb, práva na prístup, kontrolu a audit finančným subjektom alebo určenou treťou stranou, jasné práva na ukončenie a špecializované stratégie ukončenia angažovanosti. Okrem toho, keďže niektoré z týchto zmluvných prvkov môžu byť normalizované, nariadením sa podnecuje dobrovoľné používanie zmluvných doložiek, ktoré má vypracovať Komisia na používanie služby cloud computing.

Na záver, snahou nariadenia je podporiť konvergenciu prístupov dohľadu k IKT riziku tretej strany vo finančnom sektore podriadením externých poskytovateľov kritických IKT služieb rámcu dozoru Únie. Prostredníctvom nového harmonizovaného legislatívneho rámca získa európsky orgán dohľadu poverený ako hlavný orgán dozoru pre každého takéhoto externého poskytovateľa kritických IKT služieb právomoci zabezpečiť, aby poskytovatelia technologických služieb plniaci kritickú úlohu pre fungovanie finančného sektora boli primerane monitorovaní v celoeurópskom meradle. Rámec dozoru plánovaný v tomto nariadení vychádza z existujúcej inštitucionálnej architektúry v oblasti finančných služieb, pričom spoločný výbor európskych orgánov dohľadu zabezpečuje medziodvetvovú koordináciu vo vzťahu ku všetkým záležitostiam týkajúcim sa IKT rizika v súlade s jeho úlohami v oblasti kybernetickej bezpečnosti s podporou príslušného podvýboru (fórum pre dozor), ktorý vykonáva prípravnú prácu pre jednotlivé rozhodnutia a kolektívne odporúčania určené externým poskytovateľom kritických IKT služieb.

Výmena informácií (článok 40)

Na zvýšenie informovanosti o IKT riziku, minimalizovanie jeho šírenia, podporu ochranných schopností finančných subjektov a techník zisťovania hrozieb sa v nariadení finančným subjektom umožňuje vytvoriť si dohody o vzájomnej výmene informácií a spravodajských informácií o kybernetických hrozbách.

2020/0266 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskej centrálnej banky[25],

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[26],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) V digitálnom veku informačné a komunikačné technológie (IKT) podporujú zložité systémy používané pri každodenných spoločenských činnostiach. Udržiavajú chod našich hospodárstiev v kľúčových odvetviach vrátane financií a zlepšujú fungovanie jednotného trhu. Zvýšená digitalizácia a vzájomná prepojenosť zároveň zvyšujú riziko, že spoločnosť ako celok – a najmä finančný systém – bude zraniteľnejšia voči kybernetickým hrozbám alebo narušeniam v oblasti IKT. Zatiaľ čo všadeprítomné využívanie IKT systémov a vysoká miera digitalizácie a pripojiteľnosti sú v súčasnosti základnými prvkami všetkých činností finančných subjektov Únie, digitálna odolnosť ešte nie je dostatočne začlenená do ich operačných rámcov.

(2) Využívanie IKT začalo v posledných desaťročiach plniť v oblasti financovania kľúčovú úlohu, pričom v súčasnosti nadobúda zásadný význam pre fungovanie typických každodenných funkcií všetkých finančných subjektov. Digitalizáciu možno pozorovať napríklad pri platbách, ktoré čoraz viac prechádzajú od hotovostných a papierových metód k používaniu digitálnych riešení, ako aj pri zúčtovávaní a vyrovnávaní cenných papierov, elektronickom a algoritmickom obchodovaní, operáciách požičiavania a financovania, partnerskom financovaní, úverových ratingoch, upisovaní poistenia, správe poistných nárokov a operáciách back-office. Nielenže sa financie stali v celom sektore vo veľkej miere digitálnymi, ale digitalizácia zároveň prehĺbila aj prepojenia a vzájomnú závislosť v rámci finančného sektora a s externou infraštruktúrou a externými poskytovateľmi služieb.

---

25 [*doplniť odkaz*] Ú. v. EÚ C , , s. .

26 [*doplniť odkaz*] Ú. v. EÚ C , , s. .

(3) Európsky výbor pre systémové riziká (ESRB) v správe z roku 2020, ktorá sa zaoberá systémovým kybernetickým rizikom[27], opätovne potvrdil, že súčasná vysoká úroveň prepojenosti medzi finančnými subjektmi, finančnými trhmi a infraštruktúrami finančného trhu, a najmä vzájomná závislosť ich IKT systémov, môže potenciálne predstavovať systémovú zraniteľnosť, keďže lokalizované kybernetické incidenty by sa mohli rýchlo rozšíriť z ktoréhokoľvek z približne 22 000 finančných subjektov Únie[28] do celého finančného systému, a to bez ohľadu na geografické hranice. Závažné narušenia IKT, ku ktorým dochádza vo finančnej sfére, nemajú vplyv len na finančné subjekty vnímané izolovane. Zároveň uľahčujú aj cestu pre šírenie lokalizovaných zraniteľných miest naprieč finančnými prenosovými kanálmi a potenciálne vedú k nepriaznivým dôsledkom pre stabilitu celého finančného systému Únie, keďže generujú toky likvidity a celkovú stratu dôvery vo finančné trhy.

(4) V posledných rokoch sa na IKT riziká sústredila pozornosť vnútroštátnych, európskych a medzinárodných tvorcov politík, regulačných orgánov a orgánov stanovujúcich normy, ktorých snahou bolo zvýšiť odolnosť, stanoviť normy a koordinovať regulačnú činnosť alebo prácu v oblasti dohľadu. Na medzinárodnej úrovni si Bazilejský výbor pre bankový dohľad, Výbor pre platobnú a trhovú infraštruktúru, Rada pre finančnú stabilitu, Inštitút pre finančnú stabilitu, ako aj skupiny krajín G7 a G20 stanovili za cieľ poskytnúť príslušným orgánom a účastníkom trhu v rôznych jurisdikciách nástroje na posilnenie odolnosti ich finančných systémov.

(5) Napriek cieleným vnútroštátnym a európskym politickým a legislatívnym iniciatívam IKT riziká naďalej predstavujú výzvu pre prevádzkovú odolnosť, výkonnosť a stabilitu finančného systému Únie. Reforma, ktorá nasledovala po finančnej kríze z roku 2008, predovšetkým posilnila finančnú odolnosť finančného sektora Únie a bola zameraná na ochranu konkurencieschopnosti a stability Únie z hospodárskeho a prudenciálneho hľadiska a z hľadiska trhového správania. Hoci sú bezpečnosť IKT a digitálna odolnosť súčasťou operačného rizika, v pokrízovom regulačnom programe neboli práve stredobodom pozornosti, pričom sa vyvinuli len v niektorých oblastiach politiky a regulácie Únie vo sfére finančných služieb, resp. len v niekoľkých členských štátoch.

(6) V akčnom pláne Komisie pre finančné technológie[29] z roku 2018 sa zdôraznilo, že je mimoriadne dôležité zvýšiť odolnosť finančného sektora Únie aj z prevádzkového hľadiska s cieľom zaistiť jeho technologickú bezpečnosť a dobré fungovanie, rýchle zotavenie z narušení a incidentov v oblasti IKT, čo v konečnom dôsledku umožní

---

27 Správa ESRB o systémovom kybernetickom riziku z februára 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Podľa posúdenia vplyvu priloženého k preskúmaniu európskych orgánov dohľadu [SWD(2017) 308] existuje približne 5 665 úverových inštitúcií, 5 934 investičných spoločností, 2 666 poisťovní, 1 573 inštitúcií zamestnaneckého dôchodkového zabezpečenia, 2 500 investičných správcovských spoločností, 350 trhových infraštruktúr (ako napríklad centrálne protistrany, burzy cenných papierov, systémoví internalizátori, archívy obchodných údajov a multilaterálne obchodné systémy), 45 ratingových agentúr a 2 500 platobných inštitúcií a inštitúcií elektronického peňažníctva, ktorým bolo udelené povolenie. Celkovo tak ide približne o 21 233 subjektov, pričom v tomto počte nie sú zahrnuté subjekty kolektívneho financovania, štatutárni audítori a audítorské spoločnosti, poskytovatelia služieb kryptoaktív a správcovia referenčných hodnôt.

29 Oznámenie Komisie Európskemu parlamentu, Rade, Európskej centrálnej banke, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov nazvané *„Akčný plán pre finančné technológie: Za konkurencieschopnejší a inovatívnejší európsky finančný sektor*, COM(2018) 0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

účinne a bez problémov poskytovať finančné služby v celej Únii, a to aj v stresových situáciách, a zároveň sa tým pomôže zachovať dôvera spotrebiteľov a trhu.

(7) V apríli 2019 Európsky orgán pre bankovníctvo (EBA), Európsky orgán pre cenné papiere a trhy (ESMA) a Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (EIOPA) (spoločne označované ako „európske orgány dohľadu“ alebo „ESA“) spolu vydali dve technické odporúčania, v ktorých vyzvali na jednotný prístup k IKT riziku vo financovaní a odporučili primeraným spôsobom posilniť digitálnu prevádzkovú odolnosť odvetvia finančných služieb prostredníctvom iniciatívy Únie špecifickej pre toto odvetvie.

(8) Finančný sektor Únie je regulovaný harmonizovaným jednotným súborom pravidiel a riadi sa európskym systémom finančného dohľadu. Ustanovenia zamerané na digitálnu prevádzkovú odolnosť a bezpečnosť IKT však ešte nie sú úplne alebo dôsledne harmonizované, a to napriek tomu, že digitálna prevádzková odolnosť je v digitálnom veku nevyhnutná na zabezpečenie finančnej stability a integrity trhu a v žiadnom prípade nie je menej dôležitá než napríklad spoločné prudenciálne normy alebo normy správania na trhu. Jednotný súbor pravidiel a systém dohľadu by sa preto mali vypracovať tak, aby zahŕňali aj túto zložku, a to rozšírením mandátov orgánov finančného dohľadu poverených monitorovaním a ochranou finančnej stability a integrity trhu.

(9) Legislatívne rozdiely a nerovnaké vnútroštátne regulačné prístupy alebo prístupy dohľadu nad IKT rizikom vytvárajú prekážky na jednotnom trhu s finančnými službami, čo finančným subjektom s cezhraničnou prítomnosťou bráni v bezproblémovom uplatňovaní slobody usadiť sa a poskytovať služby. Rovnako narušená môže byť aj hospodárska súťaž medzi rovnakým typom finančných subjektov pôsobiacich v rôznych členských štátoch. Najmä v oblastiach, v ktorých bola harmonizácia na úrovni Únie veľmi obmedzená – ako napríklad testovanie digitálnej prevádzkovej odolnosti – alebo v ktorých úplne chýba – ako napríklad monitorovanie IKT rizika tretej strany – by rozdiely vyplývajúce z predpokladaného vývoja na vnútroštátnej úrovni mohli vytvoriť ďalšie prekážky, ktoré by bránili fungovaniu jednotného trhu na úkor účastníkov trhu a finančnej stability.

(10) Čiastočný spôsob, akým sa doteraz na úrovni Únie riešili ustanovenia týkajúce sa IKT rizika, vykazuje nedostatky alebo sa navzájom prekrýva v dôležitých oblastiach, ako je nahlasovanie incidentov súvisiacich s IKT a testovanie digitálnej prevádzkovej odolnosti, a vytvára nezrovnalosti v dôsledku nových rozdielnych vnútroštátnych pravidiel alebo nákladovo neúčinného uplatňovania prekrývajúcich sa pravidiel. Je to obzvlášť škodlivé pre používateľa intenzívne využívajúceho IKT, ako je napríklad oblasť financovania, keďže technologické riziká nepoznajú hranice a finančný sektor využíva svoje služby na širokom cezhraničnom základe v rámci Únie aj mimo nej.

Jednotlivé finančné subjekty pôsobiace na cezhraničnom základe alebo s viacerými povoleniami (napr. jeden finančný subjekt môže mať licenciu na prevádzkovanie bankových služieb, služieb investičnej spoločnosti a služieb platobnej inštitúcie, pričom každé povolenie mohol vydať iný príslušný orgán v jednom alebo viacerých členských štátoch) čelia pri riešení IKT rizík a zmierňovaní nepriaznivých vplyvov IKT incidentov prevádzkovým výzvam samostatne a koherentným, nákladovo efektívnym spôsobom.

(11) Keďže jednotný súbor pravidiel nesprevádza komplexný rámec pre IKT riziká alebo operačné riziká, je potrebná ďalšia harmonizácia kľúčových požiadaviek na digitálnu prevádzkovú odolnosť všetkých finančných subjektov. Spôsobilosti a celková

odolnosť, ktoré by finančné subjekty rozvíjali na základe takýchto kľúčových požiadaviek s cieľom odolávať prevádzkovým výpadkom, by pomohli zachovať stabilitu a integritu finančných trhov Únie, a tým by prispeli k zabezpečeniu vysokej úrovne ochrany investorov a spotrebiteľov v Únii. Keďže cieľom tohto nariadenia je prispieť k bezproblémovému fungovaniu jednotného trhu, malo by vychádzať z ustanovení článku 114 ZFEÚ, ako sa vykladá v súlade s príslušnou judikatúrou Súdneho dvora Európskej únie.

(12) Cieľom tohto nariadenia je v prvom rade konsolidovať a modernizovať požiadavky na IKT riziko, ktoré sa doteraz riešili samostatne v rôznych nariadeniach a smerniciach. Uvedenými právnymi aktmi Únie boli síce pokryté hlavné kategórie finančného rizika (napr. kreditné riziko, trhové riziko, kreditné riziko protistrany, riziko likvidity a riziko trhového správania), no v čase ich prijatia nemohli komplexne riešiť všetky zložky prevádzkovej odolnosti. Požiadavky na operačné riziko, ak sú ďalej rozpracované v týchto právnych aktoch Únie, často uprednostňovali skôr tradičný kvantitatívny prístup k riešeniu rizika (konkrétne stanovenie kapitálovej požiadavky na pokrytie IKT rizík) než uzákonenie cielených kvalitatívnych požiadaviek na posilnenie spôsobilostí prostredníctvom požiadaviek zameraných na ochranu, odhaľovanie, obmedzovanie, obnovu a nápravu incidentov súvisiacich s IKT, alebo stanovovali kapacity v oblasti nahlasovania a digitálneho testovania. Uvedené smernice a nariadenia mali v prvom rade upravovať základné pravidlá prudenciálneho dohľadu, integrity trhu alebo trhového správania.

Prostredníctvom tohto procesu, ktorým sa konsolidujú a aktualizujú pravidlá týkajúce sa IKT rizika, by sa všetky ustanovenia týkajúce sa digitálneho rizika vo financovaní po prvýkrát jednotným spôsobom spojili do jedného legislatívneho aktu. Táto iniciatíva by tak mala vyplniť medzery alebo odstrániť nezrovnalosti v niektorých z uvedených právnych aktov, a to aj v súvislosti s terminológiou, ktorá sa v nich používa, a mala by výslovne odkazovať na IKT riziko prostredníctvom cielených pravidiel týkajúcich sa spôsobilostí v oblasti riadenia IKT rizika, podávania správ a testovania a monitorovania rizík tretích strán.

(13) Finančné subjekty by sa pri riešení IKT rizika mali riadiť rovnakým prístupom a rovnakými pravidlami, ktoré by boli založené na stanovených zásadách. Konzistentnosť prispieva k posilneniu dôvery vo finančný systém a k zachovaniu jeho stability, a to najmä v časoch nadmerného využívania IKT systémov, platforiem a infraštruktúr, čo so sebou prináša zvýšené digitálne riziká.

Pomôcť pri predchádzaní vzniku vysokých nákladov pre hospodárstvo by malo aj dodržiavanie základnej kybernetickej hygieny, a to tak, že sa minimalizuje vplyv a náklady narušení v oblasti IKT.

(14) Použitím nariadenia sa pomáha znížiť regulačná zložitosť, podporuje sa konvergencia dohľadu, zvyšuje sa právna istota a zároveň sa prispieva k obmedzeniu nákladov na dodržiavanie predpisov, najmä v prípade finančných subjektov pôsobiacich cezhranične, a k zníženiu miery narušenia hospodárskej súťaže. Voľba nariadenia na vytvorenie spoločného rámca pre digitálnu prevádzkovú odolnosť finančných subjektov sa preto javí ako najvhodnejší spôsob, ako zaručiť homogénne a ucelené uplatňovanie všetkých zložiek riadenia IKT rizika finančnými sektormi Únie.

(15) Okrem právnych predpisov o finančných službách je súčasným všeobecným rámcom pre kybernetickú bezpečnosť na úrovni Únie smernica Európskeho parlamentu a Rady

(EÚ) 2016/1148[30]. Spomedzi siedmich kritických sektorov sa uvedená smernica vzťahuje aj na tri typy finančných subjektov, a to úverové inštitúcie, obchodné miesta a centrálne protistrany. Keďže sa však v smernici (EÚ) 2016/1148 stanovuje mechanizmus identifikácie prevádzkovateľov základných služieb na vnútroštátnej úrovni, v praxi sa do rozsahu pôsobnosti smernice zavádzajú len určité úverové inštitúcie, obchodné miesta a centrálne protistrany určené členskými štátmi, a preto sa od nich vyžaduje, aby spĺňali požiadavky na bezpečnosť IKT a oznamovanie incidentov, ktoré sú v nej stanovené.

(16) Keďže týmto nariadením sa zvyšuje úroveň harmonizácie zložiek digitálnej odolnosti zavedením požiadaviek na riadenie IKT rizika a nahlasovanie incidentov súvisiacich s IKT, ktoré sú prísnejšie v porovnaní s požiadavkami stanovenými v súčasných právnych predpisoch Únie o finančných službách, predstavuje to zvýšenú harmonizáciu aj v porovnaní s požiadavkami stanovenými v smernici (EÚ) 2016/1148. Toto nariadenie preto predstavuje *lex specialis* k smernici (EÚ) 2016/1148.

Je nevyhnutné zachovať silný vzťah s finančným sektorom, pričom horizontálnym rámcom Únie v oblasti kybernetickej bezpečnosti by sa zabezpečil súlad so stratégiami kybernetickej bezpečnosti, ktoré už členské štáty prijali, a orgánom finančného dohľadu by sa umožnilo, aby boli informované o kybernetických incidentoch týkajúcich sa iných sektorov, na ktoré sa vzťahuje smernica (EÚ) 2016/1148.

(17) S cieľom umožniť vzájomné medzisektorové učenie a účinne sa poučiť zo skúseností iných sektorov pri riešení kybernetických hrozieb by finančné subjekty uvedené v smernici (EÚ) 2016/1148 mali zostať súčasťou „ekosystému“ uvedenej smernice (napr. skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti a jednotky CSIRT).

Európske orgány dohľadu a príslušné vnútroštátne orgány by mali mať možnosť zúčastňovať sa na diskusiách o strategickej politike a na technických činnostiach skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, vymieňať si informácie a ďalej spolupracovať s jednotnými kontaktnými miestami určenými podľa smernice (EÚ) 2016/1148. Príslušné orgány podľa tohto nariadenia by mali zároveň konzultovať a spolupracovať s vnútroštátnymi jednotkami CSIRT určenými v súlade s článkom 9 smernice (EÚ) 2016/1148.

(18) Takisto je dôležité zabezpečiť súlad so smernicou o európskej kritickej infraštruktúre (ECI), ktorá sa v súčasnosti preskúmava s cieľom posilniť ochranu a odolnosť kritických infraštruktúr proti nekybernetickým hrozbám, pričom to môže mať dôsledky pre finančný sektor[31].

(19) Poskytovatelia služieb cloud computingu sú jednou z kategórií poskytovateľov digitálnych služieb, na ktorých sa vzťahuje smernica (EÚ) 2016/1148. Ako takí podliehajú dohľadu *ex post* vykonávanému vnútroštátnymi orgánmi určenými podľa uvedenej smernice, ktorý sa obmedzuje na požiadavky na bezpečnosť IKT a oznamovanie incidentov stanovené v uvedenom akte. Keďže rámec dozoru stanovený týmto nariadením sa vzťahuje na všetkých externých poskytovateľov kritických IKT služieb vrátane poskytovateľov služieb cloud computingu, keď

[30] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

[31] Smernica Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu (Ú. v. EÚ L 345, 23.12.2008, s. 75).

poskytujú IKT služby finančným subjektom, mal by sa považovať za doplnkový k dohľadu, ktorý sa vykonáva na základe smernice (EÚ) 2016/1148. Rámec dozoru zriadený týmto nariadením by sa navyše mal vzťahovať na poskytovateľov služieb cloud computingu, keďže neexistuje horizontálny sektorovo neutrálny rámec Únie, ktorým by sa zriaďoval orgán pre digitálny dozor.

(20) Na to, aby si finančné subjekty zachovali plnú kontrolu nad IKT rizikami, musia mať zavedené komplexné spôsobilosti umožňujúce silné a účinné riadenie IKT rizika, ako aj osobitné mechanizmy a politiky na nahlasovanie incidentov súvisiacich s IKT, testovanie systémov, kontrol a procesov IKT, ako aj riadenie IKT rizika tretej strany. Mala by sa zvýšiť úroveň digitálnej prevádzkovej odolnosti finančného systému, pričom by sa malo umožniť primerané uplatňovanie požiadaviek na finančné subjekty, ktoré sú mikropodnikmi v zmysle vymedzenia v odporúčaní Komisie 2003/361/ES[32].

(21) Prahové hodnoty nahlasovania incidentov súvisiacich s IKT a príslušné taxonómie sa v jednotlivých členských štátoch výrazne líšia. Hoci je možné dosiahnuť spoločný základ prostredníctvom relevantnej práce Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA)[33] a skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti pre finančné subjekty podľa smernice (EÚ) 2016/1148, stále existujú alebo sa môžu objaviť rozdielne prístupy k prahovým hodnotám a taxonómii pre ostatné finančné subjekty. To sa týka viacerých požiadaviek, ktoré musia finančné subjekty dodržiavať, najmä ak pôsobia v niekoľkých jurisdikciách Únie a sú súčasťou finančnej skupiny. Tieto rozdiely môžu navyše brániť vytvoreniu ďalších jednotných alebo centralizovaných mechanizmov Únie, ktoré by urýchlili proces podávania správ a podporili rýchlu a plynulú výmenu informácií medzi príslušnými orgánmi, ktorá je kľúčová pre riešenie IKT rizík v prípade rozsiahlych útokov s potenciálne systémovými následkami.

(22) V snahe umožniť príslušným orgánom, aby si plnili úlohy dohľadu získaním úplného prehľadu o povahe, frekvencii, význame a vplyve incidentov súvisiacich s IKT, a zlepšiť výmenu informácií medzi príslušnými verejnými orgánmi vrátane orgánov presadzovania práva a orgánov pre riešenie krízových situácií je potrebné stanoviť pravidlá, ktorých cieľom bude doplniť režim nahlasovania incidentov súvisiacich s IKT o požiadavky, ktoré v súčasnosti v právnych predpisoch finančného subsektora chýbajú, a odstrániť akékoľvek existujúce prekrývanie a duplicitu s cieľom zmierniť náklady. Preto je nevyhnutné harmonizovať režim nahlasovania incidentov súvisiacich s IKT tak, že sa od všetkých finančných subjektov bude vyžadovať, aby incidenty nahlasovali len svojim príslušným orgánom. Európske orgány dohľadu by okrem toho mali byť splnomocnené bližšie spresniť prvky nahlasovania incidentov súvisiacich s IKT, ako je taxonómia, časové rámce, dátové súbory, vzory a príslušné prahové hodnoty.

(23) Požiadavky na testovanie digitálnej prevádzkovej odolnosti sa v niektorých finančných subsektoroch vyvinuli vo viacerých a nekoordinovaných vnútroštátnych rámcoch, ktoré riešia rovnaké otázky nesúrodým spôsobom. To vedie k duplicite

---

[32] Odporúčanie Komisie zo 6. mája 2003 o definícii mikropodnikov, malých a stredných podnikov (Ú. v. EÚ L 124, 20.5.2003, s. 36).

[33] Taxonómia referenčnej klasifikácie incidentov ENISA, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

nákladov pre cezhraničné finančné subjekty a sťažuje vzájomné uznávanie výsledkov. Nekoordinované testovanie preto môže jednotný trh segmentovať.

(24) Okrem toho, ak sa testovanie nevyžaduje, zraniteľné miesta zostávajú neodhalené, čo v konečnom dôsledku ohrozuje tak samotný finančný subjekt, ako aj stabilitu a integritu celého finančného sektora. Bez zásahu Únie by testovanie digitálnej prevádzkovej odolnosti bolo naďalej nesúrodé a v rôznych jurisdikciách by nedošlo k vzájomnému uznaniu výsledkov testovania. Keďže je tiež nepravdepodobné, že by iné finančné subsektory prijali takéto schémy v zmysluplnom rozsahu, ušli by im potenciálne prínosy, ako je odhalenie zraniteľných miest a rizík, testovanie obranných spôsobilostí a kontinuity činností a zvýšená dôvera zákazníkov, dodávateľov a obchodných partnerov. S cieľom napraviť takéto prekrývanie, rozdiely a nedostatky treba stanoviť pravidlá zamerané na koordinované testovanie finančnými subjektmi a príslušnými orgánmi, čím sa uľahčí vzájomné uznávanie pokročilého testovania významných finančných subjektov.

(25) Závislosť finančných subjektov od IKT služieb je čiastočne podmienená ich potrebou prispôsobiť sa vznikajúcemu konkurenčnému globálnemu digitálnemu hospodárstvu, zvýšiť ich podnikateľskú efektívnosť a uspokojiť dopyt spotrebiteľov. Povaha a rozsah takejto závislosti sa v posledných rokoch neustále vyvíjali, čo viedlo k znižovaniu nákladov za finančné sprostredkovanie, umožnilo obchodné rozširovanie a škálovateľnosť pri zavádzaní finančných činností a zároveň ponúklo širokú škálu nástrojov IKT na riadenie zložitých interných procesov.

(26) Toto rozsiahle využívanie IKT služieb je doložené zložitými zmluvnými dojednaniami, v rámci ktorých sa finančné subjekty často stretávajú s ťažkosťami pri rokovaniach o zmluvných podmienkach, ktoré sú prispôsobené prudenciálnym normám alebo iným regulatórnym požiadavkám, ktorým podliehajú, alebo inak pri presadzovaní osobitných práv, ako sú práva na prístup alebo audit, ak sú tieto práva zakotvené v dohodách. Mnohé takéto zmluvy okrem toho neposkytujú dostatočné záruky umožňujúce plnohodnotne monitorovať subdodávateľské procesy, čím finančný subjekt stráca schopnosť posúdiť tieto súvisiace riziká. Keďže okrem toho externí poskytovatelia IKT služieb často poskytujú štandardizované služby rôznym typom klientov, v takýchto zmluvách sa nemusia vždy primerane zohľadňovať individuálne alebo osobitné potreby subjektov finančného sektora.

(27) Napriek tomu, že v niektorých právnych predpisoch Únie týkajúcich sa finančných služieb existujú určité všeobecné pravidlá externého zabezpečovania funkcií, monitorovanie zmluvného rozmeru nie je plne zakotvené v právnych predpisoch Únie. Keďže neexistujú jasné a cielené normy Únie, ktoré by sa vzťahovali na zmluvné dojednania uzatvorené s externými poskytovateľmi IKT služieb, nie je komplexne vyriešený externý zdroj IKT rizika. V dôsledku toho treba stanoviť určité kľúčové zásady, na základe ktorých by sa usmerňovalo, ako majú finančné subjekty riadiť IKT riziká tretej strany, pričom toto usmernenie by sprevádzal súbor základných zmluvných práv týkajúcich sa viacerých prvkov plnenia a vypovedania zmlúv s cieľom zakotviť určité minimálne záruky podporujúce schopnosť finančných subjektov účinne monitorovať všetky IKT riziká vznikajúce na úrovni tretej strany.

(28) Vo všeobecnosti existuje nedostatočná miera homogénnosti a konvergencie, pokiaľ ide o IKT riziko tretej strany a závislosť od tretej strany v oblasti IKT. Napriek určitému úsiliu o riešenie konkrétnej oblasti externého zabezpečovania funkcií, ako sú napríklad

odporúčania z roku 2017 o externom zabezpečovaní funkcií v prípade poskytovateľov cloudových služieb[34], sa problematika systémového rizika, ktoré môže byť vyvolané vystavením finančného sektora obmedzenému počtu externých poskytovateľov kritických IKT služieb, v právnych predpisoch Únie takmer nerieši. Tento nedostatok na úrovni Únie ešte zhoršuje neexistencia osobitných mandátov a nástrojov, ktoré by vnútroštátnym orgánom dohľadu umožňovali náležite pochopiť závislosť IKT od tretej strany a primerane monitorovať riziká vyplývajúce z koncentrácie takýchto závislostí IKT od tretej strany.

(29) Vzhľadom na potenciálne systémové riziká súvisiace so zvýšenou mierou externého zabezpečovania funkcií a koncentráciou externých poskytovateľov IKT a so zreteľom na nedostatočnosť vnútroštátnych mechanizmov umožňujúcich orgánom finančného dohľadu kvantifikovať, kvalifikovať a riešiť dôsledky IKT rizík, ku ktorým dochádza u externých poskytovateľov kritických IKT služieb, je potrebné vytvoriť vhodný rámec dozoru Únie, ktorý umožní nepretržité monitorovanie činností externých poskytovateľov IKT služieb, ktorí sú pre finančné subjekty kritickými poskytovateľmi.

(30) Keďže hrozby IKT sú čoraz zložitejšie a sofistikovanejšie, dobré opatrenia na odhaľovanie a prevenciu do veľkej miery závisia od pravidelnej výmeny spravodajských informácií o hrozbách a zraniteľnosti medzi finančnými subjektmi. Výmena informácií prispieva k zvýšenej informovanosti o kybernetických hrozbách, čo zase zvyšuje schopnosť finančných subjektov predchádzať tomu, aby sa hrozby stali skutočnými incidentmi, a finančným subjektom umožňuje lepšie obmedziť účinky incidentov súvisiacich s IKT a účinnejšie sa z nich zotavovať. Keďže na úrovni Únie neexistujú príslušné usmernenia, zdá sa, že takejto výmene spravodajských informácií bránia viaceré faktory, najmä neistota týkajúca sa zlučiteľnosti s pravidlami ochrany údajov, protimonopolnými pravidlami a pravidlami zodpovednosti.

(31) Váhanie, pokiaľ ide o druh informácií, ktoré sa môžu vymieňať s inými účastníkmi trhu alebo s orgánmi, ktoré nie sú orgánmi dohľadu (ako je agentúra ENISA na analytické vstupy alebo Europol na účely presadzovania práva), vedie k tom, že sa neposkytnú užitočné informácie. Rozsah a kvalita výmeny informácií sú stále obmedzené a roztrieštené, pričom k príslušným výmenám dochádza väčšinou na miestnej úrovni (prostredníctvom vnútroštátnych iniciatív) a bez ucelených celoúniových mechanizmov výmeny informácií, ktoré by boli prispôsobené potrebám integrovaného finančného sektora.

(32) Finančné subjekty by sa preto mali nabádať, aby kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operačnej úrovni s cieľom zlepšiť svoje spôsobilosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne. Na úrovni Únie preto treba umožniť vznik mechanizmov pre dobrovoľné dojednania o výmene informácií, ktoré by v prípade, že sa vykonávajú v dôveryhodnom prostredí, pomohli finančnej komunite predchádzať hrozbám a kolektívne na ne reagovať tak, aby sa rýchlo obmedzilo šírenie IKT rizík a aby sa zabránilo potenciálnej nákaze cez finančné kanály. Uvedené mechanizmy by sa mali vykonávať v plnom súlade s príslušnými pravidlami práva Únie v oblasti hospodárskej súťaže[35], a zároveň aj spôsobom, ktorým

[34] Odporúčania týkajúce sa externého zabezpečovania funkcií v prípade poskytovateľov cloudových služieb (EBA/REC/2017/03), aktuálne zrušené usmerneniami EBA o externom zabezpečovaní funkcií (EBA/GL/2019/02).

[35] Oznámenie Komisie – Usmernenia o uplatňovaní článku 101 Zmluvy o fungovaní Európskej únie na dohody o horizontálnej spolupráci (2011/C 11/01).

sa zaručí úplné dodržiavanie pravidiel Únie v oblasti ochrany údajov, hlavne nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679[36], a to najmä v súvislosti so spracúvaním osobných údajov, ktoré je potrebné na účely oprávneného záujmu, ktorý sleduje prevádzkovateľ alebo tretia strana, ako sa uvádza v článku 6 ods. 1 písm. f) uvedeného nariadenia.

(33) Bez ohľadu na široké pokrytie, s ktorým sa počíta v tomto nariadení, by sa pri uplatňovaní pravidiel digitálnej prevádzkovej odolnosti mali zohľadňovať významné rozdiely medzi finančnými subjektmi, pokiaľ ide o veľkosť, obchodný profil alebo vystavenie digitálnemu riziku. Vo všeobecnosti platí, že pri nasmerúvaní zdrojov a spôsobilostí na vykonávanie rámca riadenia IKT rizika by finančné subjekty mali dosiahnuť náležitú rovnováhu medzi svojimi potrebami súvisiacimi s IKT a svojou veľkosťou a obchodným profilom, pričom príslušné orgány by mali naďalej posudzovať a preskúmavať prístup týkajúci sa takéhoto rozdelenia.

(34) Keďže väčšie finančné subjekty môžu mať väčšie zdroje a mohli by rýchlo vynaložiť finančné prostriedky na rozvoj riadiacich štruktúr a stanovenie rôznych podnikových stratégií, vytvorenie komplexnejších mechanizmov správy a riadenia by sa malo vyžadovať len od finančných subjektov, ktoré nie sú mikropodnikmi v zmysle tohto nariadenia. Takéto subjekty sú lepšie vybavené najmä na zriadenie špecializovaných riadiacich funkcií na dohľad nad dohodami s externými poskytovateľmi IKT služieb alebo na zvládanie krízového riadenia, na organizáciu riadenia IKT rizika na základe modelu „troch línií obrany“ alebo na prijatie dokumentu o ľudských zdrojoch, v ktorom sa komplexne vysvetľujú politiky v oblasti prístupových práv.

Z rovnakého dôvodu by sa len takéto finančné subjekty mali vyzvať, aby vykonávali hĺbkové posúdenia po rozsiahlych zmenách infraštruktúr a procesov sietí a informačných systémov, pravidelne vykonávali analýzy rizík v súvislosti s pôvodnými IKT systémami alebo aby rozšírili testovanie kontinuity činností a plánov reakcie a obnovy tak, aby sa v nich zachytili scenáre prechodu medzi primárnou infraštruktúrou IKT a redundantnými zariadeniami.

(35) Okrem toho, keďže len uvedené finančné subjekty identifikované ako významné na účely pokročilého testovania digitálnej odolnosti by mali byť povinné vykonávať penetračné testy na základe konkrétnej hrozby, administratívne postupy a finančné náklady spojené s vykonávaním takýchto testov by sa mali preniesť na malý percentuálny podiel finančných subjektov. S cieľom zmierniť regulačné zaťaženie by sa len iné finančné subjekty než mikropodniky mali napokon požiadať, aby pravidelne nahlasovali príslušným orgánom všetky náklady a straty spôsobené narušeniami v oblasti IKT a výsledky preskúmaní po incidente po závažných narušeniach v oblasti IKT.

(36) S cieľom zabezpečiť úplné zosúladenie a celkovú konzistentnosť medzi obchodnými stratégiami finančných subjektov na jednej strane a riadením IKT rizika na strane druhej by sa od riadiaceho orgánu malo vyžadovať, aby si zachoval kľúčovú a aktívnu úlohu pri riadení a prispôsobovaní rámca riadenia IKT rizika a celkovej stratégie digitálnej odolnosti. Prístup, ktorý má riadiaci orgán zaujať, by sa nemal zameriavať len na prostriedky na zabezpečenie odolnosti IKT systémov, ale mal by sa vzťahovať aj na osoby a procesy prostredníctvom súboru politík, ktoré na každej podnikovej

[36] 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).

úrovni a v prípade všetkých zamestnancov podporujú silný zmysel pre informovanosť o kybernetických rizikách a záväzok dodržiavať prísnu kybernetickú hygienu na všetkých úrovniach.

Hlavnou zásadou tohto komplexného prístupu by mala byť konečná zodpovednosť riadiaceho orgánu za riadenie IKT rizika finančného subjektu, ktorá by sa mala ďalej premietnuť do nepretržitého zapojenia riadiaceho orgánu do kontroly monitorovania riadenia IKT rizika.

(37) Úplná zodpovednosť riadiaceho orgánu navyše ide ruka v ruke so zabezpečením takej úrovne investícií do IKT a celkového rozpočtu pre daný finančný subjekt, aby tento subjekt mohol dosiahnuť základnú úroveň digitálnej prevádzkovej odolnosti.

(38) Toto nariadenie, inšpirované príslušnými medzinárodnými, vnútroštátnymi a odvetvovými normami, usmerneniami, odporúčaniami alebo prístupmi v oblasti riadenia kybernetického rizika[37], presadzuje súbor funkcií, ktoré uľahčujú celkové štruktúrovanie riadenia IKT rizika. Pokiaľ hlavné spôsobilosti, ktoré finančné subjekty zavedú, budú zodpovedať potrebám cieľov, ktoré boli v tomto nariadení stanovené pre jednotlivé funkcie (identifikácia, ochrana a prevencia, odhaľovanie, reakcia a obnova, učenie a vývoj a komunikácia), finančné subjekty môžu naďalej voľne používať modely riadenia IKT rizika, ktoré sú rôzne vymedzené alebo kategorizované.

(39) V snahe držať krok s vývojom v oblasti kybernetických hrozieb by finančné subjekty mali udržiavať svoje IKT systémy v aktualizovanom stave, aby boli spoľahlivé a vybavené dostatočnou kapacitou nielen na zaručenie spracúvania údajov, keďže je to potrebné na výkon ich služieb, ale aj na zabezpečenie technologickej odolnosti, ktorá finančným subjektom umožní primerane riešiť dodatočné potreby v oblasti spracovania, ktoré môžu vzniknúť v dôsledku stresových trhových podmienok alebo iných nepriaznivých situácií. Hoci toto nariadenie nezahŕňa štandardizáciu špecifických IKT systémov, nástrojov alebo technológií, spolieha sa na to, že finančné subjekty budú vhodne využívať európske a medzinárodne uznávané technické normy (napr. ISO) alebo najlepšie priemyselné postupy, pokiaľ je takéto používanie plne v súlade s osobitnými pokynmi v oblasti dohľadu týkajúcimi sa používania a začlenenia medzinárodných noriem.

(40) Na to, aby finančné subjekty mohli promptne a rýchlo riešiť incidenty súvisiace s IKT, a najmä kybernetické útoky, sú potrebné efektívne plány na zabezpečenie kontinuity činnosti a obnovy, aby sa obmedzili škody a uprednostnilo obnovenie činností a opatrenia zamerané na obnovu. Zatiaľ čo záložné systémy by mali začať fungovať bez zbytočného odkladu, takéto spustenie by v žiadnom prípade nemalo ohroziť integritu a bezpečnosť sietí a informačných systémov alebo dôvernosť údajov.

(41) Hoci toto nariadenie umožňuje finančným subjektom pružne určovať ciele v súvislosti s lehotou na obnovu, a teda stanoviť takéto ciele tak, aby sa v plnej miere zohľadnila

---

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures* (Usmernenie o kybernetickej bezpečnosti pre infraštruktúry finančných trhov), https://www.bis.org/cpmi/publ/d146.pdf, G7 *Fundamental Elements of Cybersecurity for the Financial Sector* (Základne prvky kybernetickej bezpečnosti pre finančný sektor), https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; *NIST Cybersecurity Framework* (Rámec kybernetickej bezpečnosti NIST), https://www.nist.gov/cyberframework; FSB *CIRR toolkit* (Súbor nástrojov CIRR), https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

povaha a kritickosť príslušnej funkcie a akékoľvek osobitné obchodné potreby, pri určovaní takýchto cieľov by sa malo vyžadovať aj posúdenie potenciálneho celkového vplyvu na efektívnosť trhu.

(42) Významné následky kybernetických útokov sa znásobujú, ak k nim dôjde vo finančnom sektore, čo je oblasť, ktorej hrozí oveľa väčšie riziko, že bude cieľom šírenia škodlivých kódov, ktorých zámerom sú finančné zisky priamo pri zdroji. V snahe zmierniť takéto riziká a zabrániť tomu, aby IKT systémy stratili integritu alebo sa stali nedostupnými a došlo k porušeniu dôvernosti údajov alebo poškodeniu fyzickej infraštruktúry IKT, by sa malo výrazne zlepšiť nahlasovanie závažných incidentov súvisiacich s IKT finančnými subjektmi.

Nahlasovanie incidentov súvisiacich s IKT by sa malo harmonizovať pre všetky finančné subjekty tak, že sa od nich bude vyžadovať, aby incidenty nahlasovali len svojim príslušným orgánom. Hoci toto nahlasovanie by platilo pre všetky finančné subjekty, nie všetky z nich by mali byť ovplyvnené rovnakým spôsobom, keďže príslušné prahové hodnoty významnosti a časové rámce by mali byť kalibrované tak, aby zachytávali len závažné incidenty súvisiace s IKT. Priame nahlasovanie by orgánom finančného dohľadu umožnilo prístup k informáciám o incidentoch súvisiacich s IKT. Orgány finančného dohľadu by však mali tieto informácie postúpiť nefinančným verejným orgánom (príslušným orgánom NIS, vnútroštátnym orgánom na ochranu údajov a orgánom presadzovania práva v prípade incidentov trestnej povahy). Informácie o incidentoch súvisiacich s IKT by si mali jednotliví aktéri poskytovať navzájom: orgány finančného dohľadu by mali finančnému subjektu poskytnúť všetku potrebnú spätnú väzbu alebo usmernenia, zatiaľ čo európske orgány dohľadu by mali zdieľať anonymizované údaje o hrozbách a zraniteľných miestach súvisiacich s konkrétnou udalosťou s cieľom napomôcť širšej kolektívnej obrane.

(43) Mala by sa zvážiť aj ďalšia reflexia o možnej centralizácii správ o incidentoch súvisiacich s IKT, a to prostredníctvom jediného ústredného centra EÚ, ktoré by buď priamo prijímalo príslušné správy a automaticky informovalo príslušné orgány, alebo len centrálne zhromažďovalo správy zasielané príslušnými vnútroštátnymi orgánmi a plnilo koordinačnú úlohu. Od európskych orgánov dohľadu by sa malo vyžadovať, aby po konzultácii s ECB a agentúrou ENISA do určitého dátumu vypracovali spoločnú správu, v ktorej preskúmajú uskutočniteľnosť zriadenia takéhoto ústredného centra EÚ.

(44) V snahe dosiahnuť silnú digitálnu prevádzkovú odolnosť a v súlade s medzinárodnými normami (napr. základnými prvkami G7 pre penetračné testovanie na základe konkrétnej hrozby) by finančné subjekty mali pravidelne testovať svoje IKT systémy a personál, pokiaľ ide o účinnosť ich spôsobilostí v oblasti predchádzania, odhaľovania, reakcie a obnovy, v záujme odhalenia a riešenia potenciálnych zraniteľných miest v oblasti IKT. S cieľom reagovať na rozdiely medzi jednotlivými finančnými subsektormi a v rámci nich, pokiaľ ide o pripravenosť finančných subjektov v oblasti kybernetickej bezpečnosti, by testovanie malo zahŕňať širokú škálu nástrojov a opatrení, od posúdenia základných požiadaviek (napr. posúdenia a prehľady zraniteľnosti, analýzy otvorených zdrojov, posúdenia bezpečnosti sietí, analýzy nedostatkov, preskúmania fyzickej bezpečnosti, dotazníky a skenovacie softvérové riešenia, preskúmania zdrojových kódov, ak je to možné, testy založené na konkrétnych scenároch, testovanie kompatibility, testovanie výkonnosti alebo testovanie medzi koncovými bodmi) až po pokročilejšie testovanie (napr. penetračné testovanie na základe konkrétnej hrozby –TLPT – pre tie finančné subjekty, ktoré sú z hľadiska IKT dostatočne vyspelé na to, aby takéto testovanie dokázali realizovať).

Testovanie digitálnej prevádzkovej odolnosti by preto malo byť náročnejšie pre významné finančné subjekty (ako sú veľké úverové inštitúcie, burzy cenných papierov, centrálne depozitáre cenných papierov, centrálne protistrany atď.). Testovanie digitálnej prevádzkovej odolnosti by zároveň malo byť relevantnejšie aj pre niektoré subsektory, ktoré zohrávajú kľúčovú systémovú úlohu (napr. platby, bankovníctvo, zúčtovanie a vyrovnanie), a menej relevantné pre iné subsektory (napr. správcovia aktív, ratingové agentúry atď.). Cezhraničné finančné subjekty, ktoré si uplatňujú slobodu usadiť sa alebo poskytovať služby v rámci Únie, by mali spĺňať jednotný súbor pokročilých požiadaviek na testovanie (napr. TLPT) vo svojom domovskom členskom štáte a uvedený test by mal zahŕňať infraštruktúry IKT vo všetkých jurisdikciách, v ktorých cezhraničná skupina pôsobí v rámci Únie, čím by cezhraničným skupinám umožnil, aby im náklady na testovanie vznikli len v jednej jurisdikcii.

(45) Na zabezpečenie riadneho monitorovania IKT rizika tretej strany treba stanoviť súbor pravidiel založených na zásadách s cieľom usmerňovať finančné subjekty pri monitorovaní rizík, ktoré vznikajú v súvislosti s externe zabezpečovanými funkciami externých poskytovateľov IKT služieb a všeobecnejšie v súvislosti so závislosťou IKT od tretej strany.

(46) Za dodržiavanie povinností podľa tohto nariadenia by mal neustále niesť plnú zodpovednosť finančný subjekt. Primerané monitorovanie rizík, ktoré vznikajú na úrovni externých poskytovateľov IKT služieb, by sa malo organizovať tak, že sa náležite zohľadní rozsah, zložitosť a význam závislostí súvisiacich s IKT, kritickosť alebo význam služieb, procesov alebo funkcií, na ktoré sa vzťahujú zmluvné dojednania, a v konečnom dôsledku na základe dôkladného posúdenia akéhokoľvek potenciálneho vplyvu na kontinuitu a kvalitu finančných služieb na individuálnej, resp. skupinovej úrovni.

(47) Vykonávanie takéhoto monitorovania by sa malo riadiť strategickým prístupom k IKT riziku tretej strany, ktoré by bolo formalizované tak, že riadiaci orgán finančného subjektu prijme špecializovanú stratégiu, ktorá bude vychádzať z nepretržitého preverovania všetkých takýchto závislostí IKT od tretej strany. S cieľom zvýšiť informovanosť orgánov dohľadu o závislostiach IKT od tretej strany a s cieľom ďalej podporovať rámec dozoru ustanovený týmto nariadením by mali orgány finančného dohľadu od príslušných registrov pravidelne dostávať základné informácie a mali by mať možnosť požadovať výpisy z nich na *ad hoc* báze.

(48) Formálne uzavretie zmluvných dojednaní by mala podporiť a mala by mu predchádzať dôkladná analýza pred uzavretím zmluvy, pričom ukončenie zmlúv by malo byť motivované aspoň súborom okolností, ktoré vykazujú nedostatky u externého poskytovateľa IKT služieb.

(49) S cieľom riešiť systémový vplyv rizika koncentrácie externých poskytovateľov IKT by sa malo podporovať vyvážené riešenie prostredníctvom flexibilného a postupného prístupu, keďže pevné horné hranice alebo prísne obmedzenia môžu brániť obchodnému správaniu a zmluvnej slobode. Finančné subjekty by mali dôkladne posúdiť zmluvné dojednania s cieľom identifikovať pravdepodobnosť vzniku takéhoto rizika, a to aj prostredníctvom hĺbkových analýz dohôd o subdodávkach, najmä ak sa uzatvárajú s externými poskytovateľmi IKT služieb usadenými v tretej krajine. V tejto fáze a s cieľom dosiahnuť spravodlivú rovnováhu medzi nevyhnutnosťou zachovať zmluvnú slobodu a povinnosťou zaručiť finančnú stabilitu sa nepovažuje za vhodné stanoviť prísne horné hranice a obmedzenia expozícií voči tretím stranám v oblasti

IKT. Európsky orgán dohľadu určený na vykonávanie dozoru nad každým externým poskytovateľom kritických IKT služieb (ďalej len „hlavný orgán dozoru“) by mal pri vykonávaní úloh dozoru venovať osobitnú pozornosť plnému využitiu celého rozsahu vzájomných závislostí a odhaľovať konkrétne prípady, keď vysoký stupeň koncentrácie externých poskytovateľov kritických IKT služieb v Únii pravdepodobne zaťaží stabilitu a integritu finančného systému Únie a namiesto toho by mal zabezpečiť dialóg s externými poskytovateľmi kritických IKT služieb, ak dôjde k identifikácii takéhoto rizika[38].

(50) Aby bolo možné pravidelne vyhodnocovať a monitorovať schopnosť externého poskytovateľa IKT služieb bezpečne poskytovať služby finančnému subjektu bez nepriaznivých účinkov na jeho odolnosť, malo by dôjsť k harmonizácii kľúčových zmluvných prvkov počas plnenia zmlúv s externými poskytovateľmi IKT služieb. Uvedené prvky zahŕňajú len minimálne zmluvné aspekty považované za kľúčové pre to, aby finančné subjekty dokázali úplne monitorovať to, či zabezpečujú svoju digitálnu odolnosť, ktorá závisí od stability a bezpečnosti IKT služby.

(51) Zmluvné dojednania by mali obsahovať najmä uvedenie úplných opisov funkcií a služieb, miest, kde sa takéto funkcie poskytujú a kde sa údaje spracúvajú, ako aj uvedenie úplných opisov úrovne služieb spolu s kvantitatívnymi a kvalitatívnymi výkonnostnými cieľmi v rámci dohodnutých úrovní služieb, aby ich finančný subjekt mohol účinne monitorovať. Rovnako by sa za základné prvky schopnosti finančného subjektu zabezpečiť monitorovanie rizík tretej strany mali považovať aj ustanovenia o prístupnosti, dostupnosti, integrite, bezpečnosti a ochrane osobných údajov, ako aj záruky týkajúce sa prístupu, obnovy a návratu v prípade platobnej neschopnosti, riešenia krízových situácií alebo ukončenia obchodných činností externého poskytovateľa IKT služieb.

(52) S cieľom zabezpečiť, aby si finančné subjekty zachovali plnú kontrolu nad všetkými možnosťami vývoja, ktorý môže narušiť ich bezpečnosť IKT, by sa mali stanoviť výpovedné lehoty a ohlasovacie povinnosti externých poskytovateľov IKT služieb v prípade vývoja, ktorý môže mať potenciálne významný vplyv na schopnosť externého poskytovateľa IKT služieb účinne vykonávať kritické alebo dôležité funkcie vrátane poskytovania pomoci zo strany externého poskytovateľa IKT služieb v prípade incidentu súvisiaceho s IKT bez toho, aby sa vyskytli dodatočné náklady, alebo aby sa vyskytli len náklady, ktoré boli stanovené *ex ante*.

(53) Kľúčovými nástrojmi pri priebežnom monitorovaní výkonnosti externého poskytovateľa IKT služieb sú prístupové práva, kontrola a audit zo strany finančného subjektu alebo určenej tretej strany, ako aj úplná spolupráca uvedenej tretej strany počas kontrol. V rovnakom duchu by sa príslušnému orgánu finančného subjektu mali na základe oznámení udeliť uvedené práva na kontrolu a audit externého poskytovateľa IKT služieb, a to pod podmienkou zachovania dôvernosti.

(54) V zmluvných dojednaniach by sa mali stanoviť jasné práva na ukončenie zmluvy a súvisiace minimálne výpovedné lehoty, ako aj osobitné stratégie ukončenia angažovanosti umožňujúce najmä povinné prechodné obdobia, počas ktorých by externí poskytovatelia IKT služieb mali naďalej poskytovať príslušné funkcie s cieľom znížiť riziko narušení na úrovni finančného subjektu alebo umožniť tomuto subjektu

[38] Ak by sa okrem toho vyskytlo riziko zneužitia zo strany externého poskytovateľa IKT služieb, ktorý sa považuje za dominantného, finančné subjekty by zároveň mali mať možnosť podať formálnu alebo neformálnu sťažnosť Európskej komisii alebo vnútroštátnym orgánom na ochranu hospodárskej súťaže.

účinne prejsť k iným externým poskytovateľom IKT služieb alebo alternatívne začať využívať lokálne riešenia v prevádzkových priestoroch v závislosti od zložitosti poskytovanej služby.

(55) Dobrovoľné používanie štandardných zmluvných doložiek vypracovaných Komisiou pre služby cloud computingu môže navyše finančné subjekty a ich externých poskytovateľov IKT služieb ešte viac odbremeniť, konkrétne zvýšením úrovne právnej istoty, pokiaľ ide o využívanie služieb cloud computingu finančným sektorom, a to v plnom súlade s požiadavkami a očakávaniami, ktoré sú stanovené v nariadení o finančných službách. Táto práca vychádza z opatrení, ktoré už boli naplánované v akčnom pláne pre finančné technológie z roku 2018, v ktorom Komisia oznámila zámer podporiť a uľahčiť vypracovanie štandardných zmluvných doložiek o využívaní externe zabezpečovaných služieb cloud computingu finančnými subjektmi, a to na základe medziodvetvového úsilia zainteresovaných strán v oblasti služieb cloud computingu, ktoré Komisia uľahčila zapojením finančného sektora.

(56) S cieľom podporiť konvergenciu a efektívnosť, pokiaľ ide o prístupy dohľadu k IKT riziku tretej strany pre finančný sektor, posilniť digitálnu prevádzkovú odolnosť finančných subjektov, ktoré sa pri výkone prevádzkových funkcií spoliehajú na externých poskytovateľov kritických IKT služieb, a prispieť tak k zachovaniu stability finančného systému Únie, integrity jednotného trhu s finančnými službami, by externí poskytovatelia kritických IKT služieb mali podliehať rámcu dozoru Únie.

(57) Keďže osobitné zaobchádzanie si vyžadujú len externí poskytovatelia kritických služieb, mal by sa zaviesť mechanizmus označovania na účely uplatňovania rámca dozoru Únie s cieľom zohľadniť rozsah a povahu závislosti finančného sektora od takýchto externých poskytovateľov IKT služieb, čo sa premieta do súboru kvantitatívnych a kvalitatívnych kritérií, ktorými by sa stanovili parametre kritickosti ako základ pre začlenenie do rámca dozoru. Externí poskytovatelia kritických IKT služieb, ktorí nie sú automaticky označení na základe uplatňovania vyššie uvedených kritérií, by mali mať možnosť dobrovoľne sa zapojiť do rámca dozoru, zatiaľ čo tí externí poskytovatelia IKT služieb, na ktorých sa už vzťahujú rámce mechanizmov dozoru zriadené na úrovni Eurosystému s cieľom podporiť úlohy uvedené v článku 127 ods. 2 Zmluvy o fungovaní Európskej únie, by sa následne mali z rámca vyňať.

(58) Požiadavka právneho začlenenia externých poskytovateľov IKT služieb, ktorých služby boli označené za kritické, do Únie nepredstavuje lokalizáciu údajov, keďže toto nariadenie neobsahuje žiadnu ďalšiu požiadavku na uchovávanie alebo spracúvanie údajov, ktoré by sa vykonávali v Únii.

(59) Týmto rámcom by nemala byť dotknutá právomoc členských štátov vykonávať vlastné úlohy dozoru v súvislosti s externými poskytovateľmi IKT služieb, ktoré nie sú kritické podľa tohto nariadenia, ale mohli by sa považovať za dôležité na vnútroštátnej úrovni.

(60) V snahe využiť súčasnú viacvrstvovú inštitucionálnu architektúru v oblasti finančných služieb by spoločný výbor európskych orgánov dohľadu mal naďalej zabezpečovať celkovú medziodvetvovú koordináciu vo vzťahu ku všetkým záležitostiam týkajúcim sa IKT rizika, a to v súlade so svojimi úlohami v oblasti kybernetickej bezpečnosti, s podporou nového podvýboru (fórum dozoru), ktorý bude vykonávať prípravné práce pre jednotlivé rozhodnutia určené externým poskytovateľom kritických IKT služieb, ako aj pre kolektívne odporúčania, najmä pokiaľ ide o referenčné porovnávanie programov dozoru nad externými poskytovateľmi kritických IKT služieb, a určovať najlepšie postupy na riešenie rizika koncentrácie IKT.

(61) S cieľom zabezpečiť, aby externí poskytovatelia IKT služieb, ktorí plnia kritickú úlohu pri fungovaní finančného sektora, podliehali primeranému dozoru na úrovni Únie, by jeden z európskych orgánov dohľadu mal byť určený za hlavný orgán dozoru pre každého externého poskytovateľa kritických IKT služieb.

(62) Hlavné orgány dozoru by mali mať právomoci nevyhnutné na vykonávanie vyšetrovaní, kontrol na mieste i na diaľku u externých poskytovateľov kritických IKT služieb, mali by mať prístup do všetkých relevantných priestorov a lokalít a mali by dostávať úplné a aktualizované informácie, ktoré im umožnia získať skutočný prehľad o druhu, rozsahu a vplyve IKT rizika tretej strany, ktoré predstavujú pre samotné finančné subjekty a v konečnom dôsledku aj pre finančný systém Únie.

Poverenie európskych orgánov dohľadu úlohou hlavného orgánu dozoru je predpokladom na pochopenie a riešenie systémového rozmeru IKT rizika v oblasti financovania. Vplyv Únie na externých poskytovateľov kritických IKT služieb a súvisiace potenciálne otázky rizika koncentrácie IKT si vyžadujú prijatie kolektívneho prístupu, ktorý by sa uplatňoval na úrovni Únie. Ak by audity a prístupové práva naraz realizovali viaceré príslušné orgány oddelene, pričom by navzájom koordinovali minimálne alebo nekoordinovali vôbec, nezískal by sa úplný prehľad o IKT riziku tretej strany a zároveň by sa vytvorila zbytočná redundancia, zaťaženie a zložitosť na úrovni externých poskytovateľov kritických IKT služieb, ktorí by tak museli zvládať nespočet takýchto žiadostí.

(63) Hlavné orgány dozoru by okrem toho mali mať možnosť predkladať odporúčania týkajúce sa problematiky IKT rizika a vhodných nápravných opatrení vrátane námietok proti určitým zmluvným dojednaniam, ktoré v konečnom dôsledku ovplyvňujú stabilitu finančného subjektu alebo finančného systému. Dodržiavanie takýchto zásadných odporúčaní stanovených hlavnými orgánmi dozoru by mali príslušné vnútroštátne orgány náležite zohľadniť v rámci svojej funkcie týkajúcej sa prudenciálneho dohľadu nad finančnými subjektmi.

(64) Rámec dozoru žiadnym spôsobom nenahrádza, celkovo ani čiastočne, riadenie rizika súvisiaceho s využívaním externých poskytovateľov IKT služieb finančnými subjektmi vrátane povinnosti priebežného monitorovania ich zmluvných dojednaní uzavretých s externými poskytovateľmi kritických IKT služieb a nemá vplyv na plnú zodpovednosť finančných subjektov za dodržiavanie a plnenie všetkých požiadaviek podľa tohto nariadenia a príslušných právnych predpisov o finančných službách. Aby sa predišlo duplicite a prekrývaniu, príslušné orgány by sa mali zdržať individuálneho prijímania akýchkoľvek opatrení zameraných na monitorovanie rizík súvisiacich s externými poskytovateľmi kritických IKT služieb. Akékoľvek takéto opatrenia by sa mali vopred koordinovať a schváliť v kontexte rámca dozoru.

(65) V snahe podporiť na medzinárodnej úrovni zbližovanie najlepších postupov, ktoré sa majú používať pri preskúmavaní riadenia digitálnych rizík v súvislosti s externými poskytovateľmi IKT služieb, by sa európske orgány dohľadu mali nabádať k tomu, aby uzatvárali dohody o spolupráci s príslušnými orgánmi dohľadu a regulačnými orgánmi tretích krajín s cieľom uľahčiť rozvoj najlepších postupov v oblasti riešenia IKT rizika tretej strany.

(66) S cieľom využiť technické odborné znalosti expertov príslušných orgánov v oblasti riadenia operačných rizík a IKT rizika by hlavné orgány dozoru mali vychádzať zo skúseností vnútroštátneho dohľadu a vytvoriť špecializované prieskumné tímy pre každého jednotlivého externého poskytovateľa kritických IKT služieb, v rámci ktorých by sa spojili multidisciplinárne tímy na podporu prípravy aj skutočného vykonávania

činností dozoru vrátane kontrol na mieste u externých poskytovateľov kritických IKT služieb, ako aj potrebných následných opatrení.

(67) Príslušné orgány by mali mať všetky potrebné právomoci v oblasti dohľadu, vyšetrovania a ukladania sankcií na zabezpečenie uplatňovania tohto nariadenia. Administratívne sankcie by sa v zásade mali uverejňovať. Keďže finančné subjekty a externí poskytovatelia IKT služieb môžu byť usadení v rôznych členských štátoch a môžu podliehať dohľadu príslušných orgánov rôznych sektorov, úzka spolupráca medzi relevantnými príslušnými orgánmi vrátane ECB, pokiaľ ide o osobitné úlohy, ktoré sa na ňu preniesli v súlade s nariadením Rady (EÚ) č. 1024/2013[39], a konzultácia s európskymi orgánmi dohľadu, by sa mala zabezpečiť prostredníctvom vzájomnej výmeny informácií a poskytovania pomoci v kontexte činností dohľadu.

(68) S cieľom bližšie kvantifikovať a kvalifikovať kritériá označovania externých poskytovateľov kritických IKT služieb a harmonizovať poplatky za dozor by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 Zmluvy o fungovaní Európskej únie, pokiaľ ide o: bližšie určenie systémového vplyvu, ktorý by zlyhanie externého poskytovateľa IKT služby mohlo mať na finančné subjekty, ktorým slúži, počet globálne systémovo významných inštitúcií (G-SII) alebo inak systémovo významných inštitúcií (O-SII), ktoré sa spoliehajú na príslušného externého poskytovateľa IKT služieb, počet externých poskytovateľov IKT služieb pôsobiacich na konkrétnom trhu, náklady na prechod k inému externému poskytovateľovi IKT služieb, počet členských štátov, v ktorých príslušný externý poskytovateľ IKT služieb poskytuje služby a v ktorých pôsobia finančné subjekty využívajúce príslušného externého poskytovateľa IKT služieb, ako aj výška poplatkov za dozor a spôsob ich úhrady.

Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov, a aby tieto konzultácie vykonávala v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva[40]. Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov sa všetky dokumenty doručujú Európskemu parlamentu a Rade v rovnakom čase ako expertom z členských štátov a experti Európskeho parlamentu a Rady majú systematický prístup na zasadnutia expertných skupín Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(69) Keďže toto nariadenie spolu so smernicou Európskeho parlamentu a Rady (EÚ) 20xx/xx[41] zahŕňa konsolidáciu ustanovení o riadení IKT rizika, ktoré sa vzťahujú na viaceré nariadenia a smernice *acquis* Únie v oblasti finančných služieb vrátane nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014, s cieľom zabezpečiť úplný súlad by sa uvedené nariadenia mali zmeniť tak, aby sa v nich objasňovalo, že príslušné ustanovenia týkajúce sa IKT rizika sú stanovené v tomto nariadení.

Konzistentná harmonizácia požiadaviek stanovených v tomto nariadení by mala byť zabezpečená technickými predpismi. Európskym orgánom dohľadu by sa ako orgánom s vysoko špecializovanými odbornými poznatkami mala zveriť úloha vypracovať

---

39 Nariadenie Rady (EÚ) č. 1024/2013 z 15. októbra 2013, ktorým sa Európska centrálna banka poveruje osobitnými úlohami, pokiaľ ide o politiky týkajúce sa prudenciálneho dohľadu nad úverovými inštitúciami (Ú. v. EÚ L 287, 29.10.2013, s. 63).

40 Ú. v. EÚ L 123, 12.5.2016, s. 1.

41 [*Doplňte celý odkaz*]

návrh regulačných technických predpisov, ktoré nezahŕňajú politické rozhodnutia a ktoré sa predložia Komisii. Mali by sa vypracovať regulačné technické predpisy v oblasti riadenia IKT rizika, podávania správ, testovania a kľúčových požiadaviek na riadne monitorovanie IKT rizika tretej strany.

(70) Je osobitne dôležité, aby Komisia počas prípravných prác uskutočnila príslušné konzultácie, a to aj na úrovni expertov. Komisia a európske orgány dohľadu by mali zabezpečiť, aby uvedené predpisy a požiadavky mohli všetky finančné subjekty uplatňovať spôsobom, ktorý je primeraný povahe, rozsahu a zložitosti uvedených subjektov a ich činností.

(71) S cieľom uľahčiť porovnateľnosť správ o závažných incidentoch súvisiacich s IKT a zabezpečiť transparentnosť zmluvných dojednaní o využívaní IKT služieb poskytovaných externými poskytovateľmi IKT služieb by európske orgány dohľadu mali byť poverené vypracovaním návrhu vykonávacích technických predpisov, ktorými sa stanovia štandardizované vzory, formuláre a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT, ako aj štandardizované vzory registra informácií. Pri vypracúvaní uvedených predpisov by európske orgány dohľadu mali zohľadňovať veľkosť a zložitosť finančných subjektov, ako aj povahu a úroveň rizika ich činností. Komisia by mala byť splnomocnená prijať uvedené vykonávacie technické predpisy prostredníctvom vykonávacích aktov podľa článku 291 ZFEÚ a v súlade s článkom 15 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010, podľa konkrétneho prípadu. Keďže bližšie požiadavky už boli stanovené prostredníctvom delegovaných a vykonávacích aktov založených na regulačných technických a vykonávacích technických predpisoch v nariadeniach (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014 a (EÚ) č. 909/2014, je vhodné poveriť európske orgány dohľadu, či už jednotlivo alebo kolektívne prostredníctvom spoločného výboru, aby Komisii predložili regulačné a vykonávacie technické predpisy na prijatie delegovaných a vykonávacích aktov, ktorými sa prenášajú a aktualizujú existujúce pravidlá riadenia IKT rizika.

(72) Táto činnosť si bude vyžadovať následnú zmenu existujúcich delegovaných a vykonávacích aktov prijatých v rôznych oblastiach právnych predpisov o finančných službách. Rozsah pôsobnosti článkov o operačnom riziku, na základe ktorých splnomocnenia v uvedených aktoch viedli k prijatiu delegovaných a vykonávacích aktov, by sa mal upraviť s cieľom preniesť do tohto nariadenia všetky ustanovenia týkajúce sa digitálnej prevádzkovej odolnosti, ktoré sú dnes súčasťou uvedených nariadení.

(73) Keďže ciele tohto nariadenia, a to dosiahnutie vysokej úrovne digitálnej prevádzkovej odolnosti uplatniteľnej na všetky finančné subjekty, nie je možné uspokojivo dosiahnuť na úrovni jednotlivých členských štátov, pretože si vyžadujú harmonizáciu veľkého množstva rôznych predpisov, ktoré v súčasnosti existujú v buď v určitých aktoch Únie alebo v právnych systémoch rôznych členských štátov, ale ich možno z dôvodu ich rozsahu a účinkov lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa,

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy

1. Týmto nariadením sa stanovujú jednotné požiadavky týkajúce sa bezpečnosti sietí a informačných systémov, ktoré podporujú obchodné procesy finančných subjektov potrebné na dosiahnutie vysokej spoločnej úrovne digitálnej prevádzkovej odolnosti, a to takto:

   a) požiadavky, ktoré sa vzťahujú na finančné subjekty v súvislosti s týmito aspektmi:

   – riadenie rizika v oblasti informačných a komunikačných technológií (IKT);

   – nahlasovanie závažných incidentov súvisiacich s IKT príslušným orgánom;

   – testovanie digitálnej prevádzkovej odolnosti;

   – výmena informácií a spravodajských informácií v súvislosti s kybernetickými hrozbami a zraniteľnosťou;

   – opatrenia na správne riadenie IKT rizika tretej strany finančnými subjektmi;

   b) požiadavky súvisiace so zmluvnými dojednaniami uzavretými medzi externými poskytovateľmi IKT služieb a finančnými subjektmi;

   c) rámec dozoru nad externými poskytovateľmi kritických IKT služieb, keď sa tieto služby poskytujú finančným subjektom;

   d) pravidlá spolupráce medzi príslušnými orgánmi a pravidlá dohľadu a presadzovania príslušnými orgánmi vo všetkých záležitostiach, na ktoré sa vzťahuje toto nariadenie.

2. V súvislosti s finančnými subjektmi identifikovanými ako prevádzkovatelia základných služieb podľa vnútroštátnych predpisov, ktorými sa transponuje článok 5 smernice (EÚ) 2016/1148, sa toto nariadenie považuje za právny akt Únie špecifický pre určité odvetvie na účely článku 1 ods. 7 uvedenej smernice.

Článok 2

Osobný rozsah pôsobnosti

1. Toto nariadenie sa uplatňuje na tieto subjekty:

   a) úverové inštitúcie,

   b) platobné inštitúcie,

   c) inštitúcie elektronického peňažníctva,

   d) investičné spoločnosti,

   e) poskytovatelia služieb kryptoaktív, emitenti kryptoaktív, emitenti tokenov krytých aktívami a emitenti významných tokenov krytých aktívami,

   f) centrálne depozitáre cenných papierov,

g) centrálne protistrany,

h) obchodné miesta,

i) archívy obchodných údajov,

j) správcovia alternatívnych investičných fondov (AIF),

k) správcovské spoločnosti,

l) poskytovatelia služieb vykazovania údajov,

m) poisťovne a zaisťovne,

n) sprostredkovatelia poistenia, sprostredkovatelia zaistenia a sprostredkovatelia doplnkového poistenia,

o) inštitúcie zamestnaneckého dôchodkového zabezpečenia,

p) ratingové agentúry,

q) štatutárni audítori a audítorské spoločnosti,

r) správcovia kritických referenčných hodnôt,

s) poskytovatelia služieb kolektívneho financovania,

t) archívy sekuritizačných údajov,

u) externí poskytovatelia IKT služieb.

2. Na účely tohto nariadenia sa subjekty uvedené v písmenách a) až t) spoločne označujú ako „finančné subjekty“.

Článok 3

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „digitálna prevádzková odolnosť“ je schopnosť finančného subjektu budovať, zabezpečovať a preskúmavať svoju prevádzkovú integritu z technologického hľadiska tak, že priamo alebo nepriamo prostredníctvom využívania IKT služieb externých poskytovateľov zabezpečí celú škálu spôsobilostí súvisiacich s IKT, ktoré sú potrebné na zaistenie bezpečnosti sietí a informačných systémov, ktoré finančný subjekt využíva, a ktoré podporujú nepretržité poskytovanie finančných služieb a ich kvalitu;

2. „sieť a informačný systém“ je sieť a informačný systém v zmysle vymedzenia v článku 4 bode 1 smernice (EÚ) 2016/1148;

3. „bezpečnosť sietí a informačných systémov“ je bezpečnosť sietí a informačných systémov v zmysle vymedzenia v článku 4 bode 2 smernice (EÚ) 2016/1148;

4. „IKT riziko“ je každá primerane identifikovateľná okolnosť v súvislosti s používaním sietí a informačných systémov – vrátane poruchy, prekročenia kapacity, zlyhania, narušenia, poškodenia, nesprávneho používania, straty alebo iného druhu udalosti spôsobenej zlomyseľným zámerom alebo neúmyselne –, ktorá, ak k nej dôjde, môže ohroziť bezpečnosť sietí a informačných systémov, akéhokoľvek nástroja alebo procesu závislého od technológií, priebehu prevádzky a procesu alebo poskytovania služieb, čím dôjde k ohrozeniu integrity alebo dostupnosti údajov, softvéru alebo akýchkoľvek iných zložiek IKT služieb

a infraštruktúr, alebo ktorá spôsobí narušenie dôvernosti údajov, poškodenie fyzickej infraštruktúry IKT alebo má iné nepriaznivé účinky;

5. „informačné aktívum“ je súbor informácií, buď hmotných alebo nehmotných, ktoré sa oplatí chrániť;

6. „incident súvisiaci s IKT“ je nepredvídaná identifikovaná udalosť v sieti a informačných systémoch, vyplývajúca alebo nevyplývajúca zo zlomyseľnej činnosti, ktorá ohrozuje bezpečnosť sietí a informačných systémov, informácií, ktoré sa v takýchto systémoch spracúvajú, uchovávajú alebo prenášajú, alebo ktorá má nepriaznivé účinky na dostupnosť, dôvernosť, kontinuitu alebo pravosť finančných služieb, ktoré poskytuje finančný subjekt;

7. „závažný incident súvisiaci s IKT“ je incident súvisiaci s IKT, ktorý má potenciálne veľký nepriaznivý vplyv na sieť a informačné systémy, ktoré podporujú kritické funkcie finančného subjektu;

8. „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881[42];

9. „kybernetický útok“ je zlomyseľný incident súvisiaci s IKT uskutočnený formou pokusu o zničenie, odhalenie, zmenu, znefunkčnenie, krádež alebo získanie neoprávneného prístupu k aktívu alebo neoprávnené použitie aktíva, ktorého sa dopustil akýkoľvek aktér hrozby;

10. „spravodajské informácie o hrozbách“ sú informácie, ktoré boli agregované, transformované, analyzované, interpretované alebo obohatené tak, aby poskytovali potrebný kontext pre rozhodovanie a ktoré prinášajú relevantné a dostatočné chápanie na zmierňovanie vplyvu incidentu súvisiaceho s IKT alebo kybernetickej hrozby vrátane technických podrobností kybernetického útoku, subjektov zodpovedných za útok a ich spôsobu práce a motivácie;

11. „hĺbková ochrana“ je stratégia súvisiaca s IKT, v ktorej sú integrovaní ľudia, procesy a technológie s cieľom vytvoriť rozličné prekážky naprieč viacerými vrstvami a rozmermi subjektu;

12. „zraniteľnosť“ je slabé miesto, náchylnosť alebo chyba aktíva, systému, procesu alebo kontroly, ktoré môžu byť zneužité v rámci hrozby;

13. „penetračné testovanie na základe konkrétnej hrozby“ je rámec, ktorý simuluje taktiku, techniky a postupy reálnych aktérov hrozby považovaných za subjekty predstavujúce skutočnú kybernetickú hrozbu a ktorým sa realizuje kontrolovaný, individualizovaný test kritických živých produkčných systémov daného subjektu založený na spravodajských informáciách (červený tím);

14. „IKT riziko tretej strany“ je IKT riziko, ktoré môže finančnému subjektu vzniknúť v súvislosti s jeho využívaním IKT služieb, ktoré poskytujú externí poskytovatelia IKT služieb alebo ich ďalší subdodávatelia;

15. „externý poskytovateľ IKT služieb“ je podnik poskytujúci digitálne a dátové služby vrátane poskytovateľov služieb cloud computingu, softvéru, služieb analýzy dát,

[42] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15).

dátových centier, ale s výnimkou poskytovateľov hardvérových komponentov a podnikov, ktorým bolo udelené povolenie podľa práva Únie a ktorí poskytujú elektronické komunikačné služby v zmysle vymedzenia v článku 2 bode 4 smernice Európskeho parlamentu a Rady (EÚ) 2018/1972[43];

16. „IKT služby“ sú digitálne a dátové služby poskytované prostredníctvom IKT systémov jednému alebo viacerým interným alebo externým používateľom vrátane poskytovania údajov, vkladania údajov, uchovávania údajov, služieb spracúvania údajov a podávania správ, monitorovania údajov, ako aj služieb na podporu podnikania a rozhodovania na základe údajov;

17. „kritická alebo dôležitá funkcia“ je funkcia, ktorej ukončenie, chybné plnenie alebo neplnenie by podstatne narušilo nepretržité dodržiavanie podmienok a povinností finančného subjektu vyplývajúcich z jeho povolenia alebo jeho iných povinností podľa platných právnych predpisov o finančných službách, alebo jeho finančnej výkonnosti či správnosti alebo kontinuity jeho služieb a činností;

18. „externý poskytovateľ kritických IKT služieb“ je poskytovateľ IKT služieb, ktorý je treťou stranou, určený v súlade s článkom 29, na ktorého sa vzťahuje rámec dozoru uvedený v článkoch 30 až 37;

19. „externý poskytovateľ IKT služieb usadený v tretej krajine“ je poskytovateľ IKT služieb, ktorý je treťou stranou a ktorý je právnickou osobou usadenou v tretej krajine, nezaložil si podnikateľskú činnosť/zastúpenie v Únii a má s finančným subjektom uzavreté zmluvné dojednanie o poskytovaní IKT služieb;

20. „subdodávateľ IKT usadený v tretej krajine“ je subdodávateľ IKT, ktorý je právnickou osobou usadenou v tretej krajine, nezaložil si podnikateľskú činnosť/zastúpenie v Únii a má uzavreté zmluvné dojednanie buď s externým poskytovateľom IKT služieb alebo s externým poskytovateľom IKT služieb usadeným v tretej krajine;

21. „riziko koncentrácie IKT“ je expozícia voči jednotlivému externému poskytovateľovi kritických IKT služieb alebo viacerým súvisiacim externým poskytovateľom kritických IKT služieb, v dôsledku čoho vzniká určitá závislosť od takýchto poskytovateľov, takže nedostupnosť, zlyhanie alebo iný druh nedostatku takýchto poskytovateľov môže potenciálne ohroziť schopnosť finančného subjektu – a v konečnom dôsledku finančného systému Únie ako celku – plniť kritické funkcie alebo utrpieť iný druh nepriaznivých účinkov vrátane veľkých strát;

22. „riadiaci orgán“ je riadiaci orgán v zmysle vymedzenia v článku 4 ods. 1 bode 36 smernice 2014/65/EÚ, v článku 3 ods. 1 bode 7 smernice 2013/36/EÚ, v článku 2 ods. 1 písm. s) smernice 2009/65/ES, v článku 2 ods. 1 bode 45 nariadenia (EÚ) č. 909/2014, v článku 3 ods. 1 bode 20 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/1011[44], v článku 3 ods. 1 písm. u) nariadenia Európskeho parlamentu a Rady (EÚ) 20xx/xx[45] [MICA] alebo rovnocenné osoby, ktoré daný subjekt skutočne riadia

[43] Smernica Európskeho parlamentu a Rady (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií (prepracované znenie) (Ú. v. EÚ L 321, 17.12.2018, s. 36).

[44] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/1011 z 8. júna 2016 o indexoch používaných ako referenčné hodnoty vo finančných nástrojoch a finančných zmluvách alebo na meranie výkonnosti investičných fondov, ktorým sa menia smernice 2008/48/ES a 2014/17/EÚ a nariadenie (EÚ) č. 596/2014 (Ú. v. EÚ L 171, 29.6.2016, s. 1).

[45] [*doplňte celý názov a údaje o Ú. v. EÚ*]

alebo disponujú kľúčovými funkciami v súlade s príslušnými právnymi predpismi Únie alebo vnútroštátnymi právnymi predpismi;

23. „úverová inštitúcia“ je úverová inštitúcia v zmysle vymedzenia v článku 4 ods. 1 bodu 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013[46];

24. „investičná spoločnosť“ je investičná spoločnosť v zmysle vymedzenia v článku 4 ods. 1 bode 1 smernice 2014/65/EÚ;

25. „platobná inštitúcia“ je platobná inštitúcia v zmysle vymedzenia v článku 1 ods. 1 písm. d) smernice (EÚ) 2015/2366;

26. „inštitúcia elektronického peňažníctva“ je inštitúcia elektronického peňažníctva v zmysle vymedzenia v článku 2 bode 1 smernice Európskeho parlamentu a Rady 2009/110/ES[47];

27. „centrálna protistrana“ je centrálna protistrana v zmysle vymedzenia v článku 2 bode 1 nariadenia (EÚ) č. 648/2012;

28. „archív obchodných údajov“ je archív obchodných údajov v zmysle vymedzenia v článku 2 bode 2 nariadenia (EÚ) č. 648/2012;

29. „centrálny depozitár cenných papierov“ je centrálny depozitár cenných papierov v zmysle vymedzenia v článku 2 ods. 1 bode 1 nariadenia (EÚ) č. 909/2014;

30. „obchodné miesto“ je obchodné miesto v zmysle vymedzenia v článku 4 ods. 1 bode 24 smernice 2014/65/EÚ;

31. „správca AIF“ je správca alternatívnych investičných fondov v zmysle vymedzenia v článku 4 ods. 1 písm. b) smernice 2011/61/EÚ;

32. „správcovská spoločnosť“ je správcovská spoločnosť v zmysle vymedzenia v článku 2 ods. 1 písm. b) smernice 2009/65/ES;

33. „poskytovateľ služieb vykazovania údajov“ je poskytovateľ služieb vykazovania údajov v zmysle vymedzenia v článku 4 ods. 1 bode 63 smernice 2014/65/EÚ;

34. „poisťovňa“ je poisťovňa v zmysle vymedzenia v článku 13 bode 1 smernice 2009/138/ES;

35. „zaisťovňa“ je zaisťovňa v zmysle vymedzenia v článku 13 bode 4 smernice 2009/138/ES;

36. „sprostredkovateľ poistenia“ je sprostredkovateľ poistenia v zmysle vymedzenia v článku 2 bode 3 smernice (EÚ) 2016/97;

37. „sprostredkovateľ doplnkového poistenia“ je sprostredkovateľ doplnkového poistenia v zmysle vymedzenia v článku 2 bode 4 smernice (EÚ) 2016/97;

38. „sprostredkovateľ zaistenia“ je sprostredkovateľ zaistenia v zmysle vymedzenia v článku 2 bode 5 smernice (EÚ) 2016/97;

---

[46] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 575/2013 z 26. júna 2013 o prudenciálnych požiadavkách na úverové inštitúcie a investičné spoločnosti a o zmene nariadenia (EÚ) č. 648/2012 (Ú. v. EÚ L 176, 27.6.2013, s. 1).

[47] Smernica Európskeho parlamentu a Rady 2009/110/ES zo 16. septembra 2009 o začatí a vykonávaní činností a dohľade nad obozretným podnikaním inštitúcií elektronického peňažníctva, ktorou sa menia a dopĺňajú smernice 2005/60/ES a 2006/48/ES a zrušuje smernica 2000/46/ES (Ú. v. EÚ L 267, 10.10.2009, s. 7).

39. „inštitúcia zamestnaneckého dôchodkového zabezpečenia“ je inštitúcia zamestnaneckého dôchodkového zabezpečenia v zmysle vymedzenia v článku 6 bode 1 smernice (EÚ) 2016/2341;

40. „ratingová agentúra“ je ratingová agentúra v zmysle vymedzenia v článku 3 ods. 1 písm. b) nariadenia (ES) č. 1060/2009;

41. „štatutárny audítor“ je štatutárny audítor v zmysle vymedzenia v článku 2 bode 2 smernice 2006/43/ES;

42. „audítorská spoločnosť“ je audítorská spoločnosť v zmysle vymedzenia v článku 2 bode 3 smernice 2006/43/ES;

43. „poskytovateľ služieb kryptoaktív“ je poskytovateľ služieb v oblasti kryptoaktív v zmysle vymedzenia v článku 3 ods. 1 písm. n) nariadenia (EÚ) 202x/xx [*PO: vložiť odkaz na nariadenie MICA*];

44. „emitent kryptoaktív“ je emitent kryptoaktív v zmysle vymedzenia v článku 3 ods. 1 písm. h) [*Ú. v. EÚ: vložiť odkaz na nariadenie MICA*];

45. „emitent tokenov krytých aktívami“ je emitent platobných tokenov odkazujúcich na aktíva v zmysle vymedzenia v článku 3 ods. 1 písm. i) [*Ú. v. EÚ: vložiť odkaz na nariadenie MICA*];

46. „emitent významných tokenov krytých aktívami“ je emitent významných platobných tokenov odkazujúcich na aktíva v zmysle vymedzenia v článku 3 ods. 1 písm. j) [*Ú. v. EÚ: vložiť odkaz na nariadenie MICA*];

47. „správca kritických referenčných hodnôt“ je správca kritických referenčných hodnôt v zmysle vymedzenia v článku x písm. x) nariadenia xx/202x [*Ú. v. EÚ: vložiť odkaz na nariadenie o referenčných hodnotách*];

48. „poskytovateľ služieb kolektívneho financovania“ je poskytovateľ služieb kolektívneho financovania v zmysle vymedzenia v článku x písm. x) nariadenia (EÚ) 202x/xx [*PO: vložiť odkaz na nariadenie o kolektívnom financovaní*];

49. „archív sekuritizačných údajov“ je archív sekuritizačných údajov v zmysle vymedzenia v článku 2 bode 23 nariadenia (EÚ) 2017/2402;

50. „mikropodnik“ je finančný subjekt v zmysle vymedzenia v článku 2 ods. 3 prílohy k odporúčaniu 2003/361/ES.

KAPITOLA II

RIADENIE IKT RIZIKA

ODDIEL I

Článok 4

Správa, riadenie a organizácia

1. Finančné subjekty musia mať zavedené rámce vnútornej správy, riadenia a kontroly, ktorými sa zabezpečí účinné a obozretné riadenie všetkých IKT rizík.

2. Riadiaci orgán finančného subjektu vymedzuje a schvaľuje vykonávanie všetkých opatrení súvisiacich s rámcom riadenia IKT rizika uvedeným v článku 5 ods. 1, vykonáva nad ním dozor a zodpovedá zaň.

Na účely prvého pododseku riadiaci orgán:

a) nesie konečnú zodpovednosť za riadenie IKT rizika finančného subjektu;

b) stanovuje jasné úlohy a zodpovednosti pre všetky funkcie súvisiace s IKT;

c) určuje primeranú úroveň tolerancie voči IKT riziku finančného subjektu, ako sa uvádza v článku 5 ods. 9 písm. b);

d) schvaľuje vykonávanie politiky kontinuity činností finančného subjektu v oblasti IKT a plánu obnovy po havárii IKT uvedených v článku 10 ods. 1 a 3, vykonáva nad ním dozor a pravidelne ho preskúmava;

e) schvaľuje a pravidelne preskúmava plány auditov IKT, audity IKT a ich podstatné zmeny;

f) prideľuje a pravidelne preskúmava príslušný rozpočet s cieľom uspokojiť potreby finančného subjektu v oblasti digitálnej prevádzkovej odolnosti, pokiaľ ide o všetky druhy zdrojov vrátane odbornej prípravy v oblasti IKT rizík a zručností pre všetkých relevantných zamestnancov;

g) schvaľuje a pravidelne preskúmava politiku finančného subjektu týkajúcu sa opatrení súvisiacich s využívaním IKT služieb, ktoré poskytujú externí poskytovatelia IKT služieb;

h) musí byť riadne informovaný o dojednaniach uzavretých s externými poskytovateľmi IKT služieb v oblasti využívania IKT služieb, o všetkých relevantných plánovaných podstatných zmenách týkajúcich sa externých poskytovateľov IKT služieb a o možnom vplyve takýchto zmien na kritické alebo dôležité funkcie, ktoré sú predmetom uvedených dohôd, pričom zároveň musí dostať zhrnutie analýzy rizík, aby dokázal posúdiť vplyv týchto zmien;

i) musí byť riadne informovaný o incidentoch súvisiacich s IKT a ich vplyve, ako aj o reakcii, obnove a nápravných opatreniach.

3. Finančné subjekty iné než mikropodniky zriadia úlohu, ktorej cieľom je monitorovať dojednania o využívaní IKT služieb uzavreté s externými poskytovateľmi IKT služieb, alebo určia člena vrcholového manažmentu, ktorý bude zodpovedať za vykonávanie dozoru nad príslušnými rizikovými expozíciami a za relevantnú dokumentáciu.

4. Členovia riadiaceho orgánu pravidelne absolvujú osobitnú odbornú prípravu s cieľom získať a aktualizovať dostatočné znalosti a zručnosti na to, aby dokázali chápať a posudzovať IKT riziká a ich vplyv na operácie finančného subjektu.

ODDIEL II

Článok 5

Rámec riadenia IKT rizika

1. Finančné subjekty musia mať zavedený spoľahlivý, komplexný a dobre zdokumentovaný rámec riadenia IKT rizika, ktorý im umožňuje riešiť IKT riziko rýchlo, efektívne a komplexne a zabezpečiť vysokú úroveň digitálnej prevádzkovej odolnosti, ktorá zodpovedá druhu, veľkosti a zložitosti ich obchodných potrieb.

2. Rámec riadenia IKT rizika uvedený v odseku 1 zahŕňa stratégie, politiky, postupy, protokoly a nástroje IKT, ktoré sú potrebné na riadnu a účinnú ochranu všetkých relevantných fyzických komponentov a infraštruktúr vrátane počítačového hardvéru, serverov, ako aj všetkých príslušných priestorov, dátových centier a citlivých určených oblastí s cieľom zabezpečiť, aby boli všetky uvedené fyzické prvky primerane chránené pred rizikami vrátane poškodenia a neoprávneného prístupu či používania.

3. Finančné subjekty minimalizujú vplyv IKT rizika tak, že zavedú vhodné stratégie, politiky, postupy, protokoly a nástroje, ktoré boli určené v rámci riadenia IKT rizika. Poskytujú úplné a aktualizované informácie o IKT rizikách podľa požiadaviek príslušných orgánov.

4. Ako súčasť rámca riadenia IKT rizika uvedeného v odseku 1 finančné subjekty iné než mikropodniky zavedú systém riadenia informačnej bezpečnosti, ktorý je založený na uznávaných medzinárodných normách a v súlade s usmerneniami v oblasti dohľadu, a pravidelne ho preskúmavajú.

5. Finančné subjekty iné než mikropodniky zabezpečia v oblasti IKT primerané oddelenie riadiacich funkcií, kontrolných funkcií a funkcií vnútorného auditu, a to na základe modelu troch línií obrany alebo na základe interného modelu riadenia rizík a kontroly.

6. Rámec riadenia IKT rizika uvedený v odseku 1 sa zdokumentuje a preskúmava aspoň raz ročne, ako aj pri výskyte závažných incidentov súvisiacich s IKT, pričom sa riadi pokynmi alebo závermi dohľadu vyplývajúcimi z príslušných procesov testovania alebo auditu digitálnej prevádzkovej odolnosti. Na základe skúseností získaných pri vykonávaní a monitorovaní sa rámec neustále vylepšuje.

7. Rámec riadenia IKT rizika uvedený v odseku 1 pravidelne kontrolujú audítori IKT, ktorí disponujú dostatočnými znalosťami, zručnosťami a odbornými poznatkami v oblasti IKT rizika. Frekvencia a zameranie auditov IKT musí zodpovedať IKT rizikám daného finančného subjektu.

8. Zavedie sa formálny proces následných krokov vrátane pravidiel pre včasné overovanie a nápravu kritických zistení auditu IKT, pričom sa zohľadnia závery z audítorského preskúmania a náležite sa zohľadní povaha, rozsah a zložitosť služieb a činností finančných subjektov.

9. Rámec riadenia IKT rizika uvedený v odseku 1 zahŕňa stratégiu digitálnej odolnosti, v ktorej sa stanoví spôsob vykonávania rámca. Na tento účel rámec zahŕňa metódy na riešenie IKT rizika a dosiahnutie konkrétnych cieľov IKT, a to prostredníctvom týchto prvkov:

   a) vysvetlenie, ako rámec riadenia IKT rizika podporuje obchodnú stratégiu a ciele finančného subjektu;

   b) stanovenie úrovne tolerancie rizika v prípade IKT rizika v súlade s ochotou finančného subjektu podstupovať riziká a analýza tolerancie vplyvu narušení IKT;

   c) stanovenie jasných cieľov v oblasti informačnej bezpečnosti;

   d) vysvetlenie referenčnej architektúry IKT a akýchkoľvek zmien potrebných na dosiahnutie konkrétnych obchodných cieľov;

e) načrtnutie rôznych mechanizmov zavedených na účely odhaľovania, ochrany a prevencie vplyvu incidentov súvisiacich s IKT;

f) preukázanie počtu nahlásených závažných incidentov súvisiacich s IKT a účinnosti preventívnych opatrení;

g) vymedzenie holistickej stratégie viacerých dodávateľov IKT na úrovni subjektov, ktorá preukazuje kľúčové závislosti od externých poskytovateľov IKT služieb a vysvetľuje dôvody, na ktorých je založený príslušný obstarávací mix externých poskytovateľov služieb;

h) vykonávanie testovania digitálnej prevádzkovej odolnosti;

i) stanovenie komunikačnej stratégie v prípade incidentov súvisiacich s IKT.

10. Po tom, ako to schvália príslušné orgány, môžu finančné subjekty delegovať úlohy overovania súladu s požiadavkami na riadenie IKT rizika na podniky vo vnútri skupiny alebo na externé podniky.

Článok 6

Systémy, protokoly a nástroje IKT

1. Finančné subjekty používajú a udržiavajú aktualizované IKT systémy a nástroje, ktoré spĺňajú tieto podmienky:

a) systémy a nástroje sú primerané povahe, rôznorodosti, zložitosti a rozsahu operácií, ktoré podporujú vykonávanie ich činností;

b) sú spoľahlivé;

c) majú dostatočnú kapacitu na to, aby sa nimi presne spracúvali údaje potrebné na včasné vykonávanie činností a poskytovanie služieb a na to, aby v čase prevádzkovej špičky dokázali podľa potreby zvládať objednávky, správy alebo objemy transakcií, a to aj v prípade zavedenia novej technológie;

d) sú dostatočne technologicky odolné na to, aby primerane zvládali dodatočné potreby v oblasti spracovania informácií, ak si to vyžadujú stresové trhové podmienky alebo iné nepriaznivé situácie.

2. Ak finančné subjekty používajú medzinárodne uznávané technické normy a popredné priemyselné postupy v oblasti informačnej bezpečnosti a vnútorných kontrol IKT, uvedené normy a postupy používajú v súlade s akýmikoľvek príslušnými odporúčaniami orgánu dohľadu týkajúcimi sa ich začlenenia.

Článok 7

Identifikácia

1. Ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 finančné subjekty identifikujú, klasifikujú a primerane dokumentujú všetky obchodné funkcie súvisiace s IKT, informačné aktíva podporujúce tieto funkcie a konfigurácie a vzájomné prepojenia IKT systémov s internými a externými IKT systémami. Finančné subjekty podľa potreby, najmenej však raz ročne preskúmavajú primeranosť klasifikácie informačných aktív a akejkoľvek relevantnej dokumentácie.

2. Finančné subjekty nepretržite identifikujú všetky zdroje IKT rizika, najmä rizikovú expozíciu voči iným finančným subjektom a pochádzajúcu od nich, a posudzujú kybernetické hrozby a zraniteľné miesta v oblasti IKT relevantné z hľadiska ich obchodných funkcií a informačných aktív súvisiacich s IKT. Finančné subjekty pravidelne a aspoň raz ročne preskúmavajú rizikové scenáre, ktoré na ne majú vplyv.

3. Finančné subjekty iné než mikropodniky vykonávajú posúdenie rizík pri každej rozsiahlej zmene infraštruktúry siete a informačných systémov, pokiaľ ide o procesy alebo postupy, ktoré majú vplyv na ich funkcie, podporujú ich procesy alebo informačné aktíva.

4. Finančné subjekty identifikujú všetky účty IKT systémov vrátane účtov na vzdialených miestach, sieťové zdroje a hardvérové zariadenia a zmapujú fyzické zariadenia, ktoré sa považujú za kritické. Zmapujú konfiguráciu aktív IKT, ako aj prepojenia a vzájomné závislosti medzi jednotlivými aktívami IKT.

5. Finančné subjekty identifikujú a zdokumentujú všetky procesy, ktoré sú závislé od externých poskytovateľov IKT služieb, a identifikujú vzájomné prepojenia s externými poskytovateľmi IKT služieb.

6. Na účely odsekov 1, 4 a 5 finančné subjekty vedú a pravidelne aktualizujú príslušné stavy zásob.

7. Finančné subjekty iné než mikropodniky pravidelne a aspoň raz ročne vykonávajú osobitné posúdenie IKT rizika vo všetkých pôvodných IKT systémoch, najmä pred prepojením starých a nových technológií, aplikácií alebo systémov a po takomto prepojení.

Článok 8

Ochrana a prevencia

1. Na účely primeranej ochrany IKT systémov a s cieľom organizovať opatrenia v oblasti reakcie finančné subjekty nepretržite monitorujú a kontrolujú fungovanie IKT systémov a nástrojov a minimalizujú vplyv takýchto rizík tak, že zavedú vhodné nástroje, politiky a postupy v oblasti bezpečnosti IKT.

2. Finančné subjekty navrhujú, obstarávajú a realizujú stratégie, politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, ktorých cieľom je najmä zabezpečiť odolnosť, kontinuitu a dostupnosť IKT systémov a zachovať vysoké štandardy bezpečnosti, dôvernosti a integrity údajov či už v pokoji, v prevádzke alebo v tranzite.

3. Na dosiahnutie cieľov uvedených v odseku 2 používajú finančné subjekty najmodernejšie IKT technológie a postupy, ktoré:

   a) zaručujú bezpečnosť prostriedkov prenosu informácií;

   b) minimalizujú riziko poškodenia alebo straty údajov, neoprávneného prístupu a technických nedostatkov, ktoré môžu brániť podnikateľskej činnosti;

   c) zabraňujú úniku informácií;

   d) zabezpečujú, aby boli údaje chránené pred nedostatočnými administratívnymi postupmi alebo rizikami v oblasti spracovania vrátane neprimeraného vedenia záznamov.

4. Ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 finančné subjekty:

a) vypracujú a zdokumentujú politiku v oblasti informačnej bezpečnosti, v ktorej sa vymedzia pravidlá ochrany dôvernosti, integrity a dostupnosti ich IKT zdrojov, údajov a informačných prostriedkov a IKT zdrojov, údajov a informačných prostriedkov ich zákazníkov;

b) na základe prístupu založeného na rizikách zavedú spoľahlivé riadenie siete a infraštruktúry pomocou vhodných techník, metód a protokolov vrátane zavedenia automatizovaných mechanizmov na izolovanie dotknutých informačných aktív v prípade kybernetických útokov;

c) vykonávajú politiky, ktoré obmedzujú fyzický a virtuálny prístup k zdrojom a údajom IKT systému len na to, čo je nevyhnutné pre legitímne a schválené funkcie a činnosti, a na tento účel zavedú súbor politík, postupov a kontrol, ktoré sa zaoberajú oprávneniami na prístup a ich riadnou správou;

d) vykonávajú politiky a protokoly pre silné mechanizmy autentifikácie založené na príslušných normách a špecializovaných kontrolných systémoch s cieľom zabrániť prístupu k šifrovacím kľúčom, pričom údaje sú šifrované na základe výsledkov schválenej klasifikácie údajov a procesov posudzovania rizík;

e) vykonávajú politiky, postupy a kontroly riadenia zmien IKT vrátane zmien komponentov softvéru, hardvéru, firmvéru, systémov alebo bezpečnostných zmien, ktoré sú založené na prístupe posudzovania rizík a sú neoddeliteľnou súčasťou celkového procesu riadenia zmien finančného subjektu s cieľom zabezpečiť, aby sa všetky zmeny IKT systémov zaznamenávali, testovali, posudzovali, schvaľovali, vykonávali a overovali kontrolovaným spôsobom;

f) musia mať vhodné a komplexné politiky týkajúce sa opráv a aktualizácií.

Na účely písmena b) finančné subjekty navrhnú infraštruktúru sieťového pripojenia tak, aby umožňovala jej okamžité odpojenie, a zabezpečia jej kompartmentalizáciu a segmentáciu s cieľom minimalizovať šírenie nákazy a predchádzať mu, a to najmä v prípade vzájomne prepojených finančných procesov.

Proces riadenia zmien IKT na účely písmena e) schvaľujú príslušné riadiace línie, ktoré majú k dispozícii osobitné protokoly pre núdzové zmeny.

Článok 9

Detekcia

1. Finančné subjekty musia mať zavedené mechanizmy na rýchle odhaľovanie anomálnych činností v súlade s článkom 15 vrátane problémov s výkonnosťou IKT siete a incidentov súvisiacich s IKT, ako aj na identifikáciu všetkých potenciálnych závažných jednotlivých miest zlyhania.

   Všetky detekčné mechanizmy uvedené v prvom pododseku sa pravidelne testujú v súlade s článkom 22.

2. Detekčné mechanizmy uvedené v odseku 1 umožňujú viaceré úrovne kontroly, vymedzujú sa v nich varovné prahové hodnoty a kritériá na spustenie procesov odhaľovania incidentov súvisiacich s IKT a reakcie na ne a zavádzajú sa nimi automatické mechanizmy varovania pre príslušných zamestnancov zodpovedných za reakciu na incidenty súvisiace s IKT.

3. Finančné subjekty venujú dostatočné zdroje a spôsobilosti, s náležitým ohľadom na svoju veľkosť, obchodný a rizikový profil, na monitorovanie činnosti používateľov, výskytu anomálií IKT a incidentov súvisiacich s IKT, a to najmä kybernetických útokov.

4. Finančné subjekty uvedené v článku 2 ods. 1 písm. l) musia mať navyše zavedené systémy, ktoré dokážu účinne kontrolovať úplnosť správ o obchode, identifikovať vynechania a zjavné chyby a požiadať o opätovné zaslanie všetkých takýchto chybných správ.

Článok 10

Reakcieschopnosť a obnova

1. Finančné subjekty ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 a na základe požiadaviek na identifikáciu stanovených v článku 7 zavedú špecializovanú a komplexnú politiku kontinuity činností v oblasti IKT ako neoddeliteľnú súčasť politiky prevádzkovej kontinuity činností finančného subjektu.

2. Finančné subjekty vykonávajú politiku kontinuity činností v oblasti IKT uvedenú v odseku 1 prostredníctvom špecializovaných, primeraných a zdokumentovaných opatrení, plánov, postupov a mechanizmov zameraných na:

   a) zaznamenávanie všetkých incidentov súvisiacich s IKT;

   b) zabezpečenie kontinuity kritických funkcií finančného subjektu;

   c) rýchlu, primeranú a účinnú reakciu na všetky incidenty súvisiace s IKT a ich riešenie, najmä – ale nie výlučne – kybernetické útoky, a to spôsobom, ktorý obmedzuje škody a uprednostňuje obnovenie činností a opatrenia zamerané na obnovu;

   d) bezodkladnú aktiváciu špecializovaných plánov, ktoré umožňujú uplatniť opatrenia, procesy a technológie na zamedzenie šírenia vhodné pre každý typ incidentu súvisiaceho s IKT, a predchádzanie ďalším škodám, ako aj prispôsobené postupy reakcie a obnovy stanovené v súlade s článkom 11;

   e) odhad predbežných vplyvov, škôd a strát;

   f) stanovenie opatrení v oblasti komunikácie a krízového riadenia, ktorými sa zabezpečí, aby sa aktualizované informácie zasielali všetkým príslušným interným zamestnancom a externým zainteresovaným stranám v súlade s článkom 13 a aby sa o nich podávali správy príslušným orgánom v súlade s článkom 17.

3. Finančné subjekty ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 vykonávajú súvisiaci plán obnovy po havárii v oblasti IKT, ktorý v prípade finančných subjektov iných než mikropodniky podlieha nezávislému audítorskému preskúmaniu.

4. Finančné subjekty zavedú, udržiavajú a pravidelne testujú príslušné plány na zabezpečenie kontinuity činností v oblasti IKT, najmä pokiaľ ide o kritické alebo dôležité funkcie externe zabezpečované alebo zmluvne dohodnuté v rámci dojednaní s externými poskytovateľmi IKT služieb.

5. Finančné subjekty v rámci svojho komplexného riadenia IKT rizika:

a) testujú politiku kontinuity činností v oblasti IKT a plán obnovy po havárii v oblasti IKT aspoň raz ročne a po podstatných zmenách IKT systémov;

b) testujú plány krízovej komunikácie vypracované v súlade s článkom 13.

Na účely písmena a) finančné subjekty iné než mikropodniky zahrnú do testovacích plánov scenáre kybernetických útokov a prepnutia medzi primárnou infraštruktúrou IKT a redundantnou kapacitou, zálohami a redundantnými zariadeniami potrebnými na splnenie povinností stanovených v článku 11.

Finančné subjekty pravidelne preskúmavajú svoju politiku kontinuity činností v oblasti IKT a plán obnovy po havárii v oblasti IKT, pričom zohľadňujú výsledky testov vykonaných v súlade s prvým pododsekom a odporúčania vyplývajúce z auditorských kontrol alebo preskúmaní orgánmi dohľadu.

6. Finančné subjekty iné než mikropodniky musia mať funkciu krízového riadenia, ktorá v prípade aktivácie ich politiky kontinuity činností v oblasti IKT alebo plánu obnovy po havárii v oblasti IKT stanoví jasné postupy riadenia vnútornej a vonkajšej krízovej komunikácie v súlade s článkom 13.

7. Finančné subjekty vedú záznamy o činnostiach pred udalosťami narušenia a počas nich, keď sa aktivuje ich politika kontinuity činností v oblasti IKT alebo plán obnovy po havárii v oblasti IKT. Takéto záznamy musia byť ľahko dostupné.

8. Finančné subjekty uvedené v článku 2 ods. 1 písm. f) poskytnú príslušným orgánom kópie výsledkov testov kontinuity činností v oblasti IKT alebo podobných cvičení vykonaných počas posudzovaného obdobia.

9. Finančné subjekty iné než mikropodniky nahlasujú príslušným orgánom všetky náklady a straty spôsobené narušeniami IKT a incidentmi súvisiacimi s IKT.

Článok 11

Politika zálohovania a metódy obnovy

1. Na účely zabezpečenia obnovy IKT systémov s minimálnym výpadkom služieb a obmedzeným narušením v ich rámci riadenia IKT rizika finančné subjekty vypracujú:

a) politiku zálohovania, v ktorej sa špecifikuje rozsah údajov, ktoré sú predmetom zálohovania, a minimálna frekvencia zálohovania na základe kritického charakteru informácií alebo citlivosti údajov;

b) metódy obnovy.

2. Záložné systémy musia začať fungovať bez zbytočného odkladu s výnimkou prípadu, ak by takéto spustenie ohrozovalo bezpečnosť sietí a informačných systémov alebo integritu či dôvernosť údajov.

3. Pri obnovovaní záložných údajov pomocou vlastných systémov finančné subjekty používajú IKT systémy, ktoré majú iné prevádzkové prostredie než hlavný systém, ktoré nie je priamo spojené s hlavným systémom a ktoré je bezpečne chránené pred akýmkoľvek neoprávneným prístupom alebo poškodením IKT.

V prípade finančných subjektov uvedených v článku 2 ods. 1 písm. g) musia plány obnovy umožňovať obnovu všetkých transakcií v čase narušenia, aby centrálna protistrana mohla naďalej fungovať s istotou a aby vyrovnanie dokončila k plánovanému dátumu.

4. Finančné subjekty udržiavajú redundantné kapacity IKT vybavené zdrojmi, spôsobilosťami a funkciami, ktoré sú dostatočné a primerané na zabezpečenie obchodných potrieb.

5. Finančné subjekty uvedené v článku 2 ods. 1 písm. f) udržiavajú alebo zabezpečujú, aby ich externí poskytovatelia IKT služieb udržiavali aspoň jedno sekundárne miesto spracovania vybavené zdrojmi, spôsobilosťami, funkciami a personálnymi opatreniami, ktoré sú dostatočné a primerané na zabezpečenie obchodných potrieb.

   Sekundárne miesto spracovania musí:

   a) byť umiestnené v lokalite geograficky vzdialenej od primárneho miesta spracovania s cieľom zabezpečiť, aby malo odlišný rizikový profil, a zabrániť tomu, aby bol ovplyvnený udalosťou, ktorá ovplyvnila primárne miesto;

   b) byť schopné zabezpečiť kontinuitu kritických služieb rovnako ako primárne miesto alebo poskytovať úroveň služieb potrebnú na zabezpečenie toho, aby finančný subjekt vykonával svoje kritické operácie v rámci cieľov obnovy;

   c) byť okamžite prístupné pre zamestnancov finančného subjektu, aby sa zabezpečila kontinuita kritických služieb v prípade, že sa primárne miesto spracovania stalo nedostupným.

6. Pri určovaní času obnovy a bodových cieľov pre každú funkciu finančné subjekty zohľadňujú potenciálny celkový vplyv na efektívnosť trhu. Takéto časové ciele zabezpečia, aby sa v extrémnych scenároch dosiahli dohodnuté úrovne služieb.

7. Pri obnovovaní po incidente súvisiacom s IKT vykonávajú finančné subjekty viaceré kontroly vrátane zosúhlasení údajov s cieľom zabezpečiť, aby úroveň integrity údajov bola na čo najvyššej úrovni. Tieto kontroly sa vykonávajú aj pri rekonštrukcii údajov od externých zainteresovaných strán s cieľom zabezpečiť konzistentnosť všetkých údajov medzi jednotlivými systémami.

Článok 12

Učenie sa a vývoj

1. Finančné subjekty musia mať zavedené spôsobilosti a personál, ktoré sú vhodné vzhľadom na ich veľkosť, obchodný a rizikový profil, aby zhromažďovali informácie o zraniteľných miestach a kybernetických hrozbách, incidentoch súvisiacich s IKT, najmä kybernetických útokoch, a analyzovali ich pravdepodobný vplyv na ich digitálnu prevádzkovú odolnosť.

2. Finančné subjekty zavedú preskúmania, ktoré sa realizujú po incidentoch súvisiacich s IKT a ku ktorým dochádza po výraznom narušení hlavných činností IKT, pričom analyzujú príčiny narušenia a identifikujú požadované zlepšenia operácií IKT alebo zlepšenia v rámci politiky kontinuity činností v oblasti IKT uvedenej v článku 10.

   Pri vykonávaní zmien finančné subjekty iné než mikropodniky tieto zmeny oznamujú príslušným orgánom.

   V preskúmaniach po incidentoch súvisiacich s IKT uvedených v prvom pododseku sa určí, či sa dodržali zavedené postupy a či boli prijaté opatrenia účinné, a to aj pokiaľ ide o:

   a) promptnosť reakcie na bezpečnostné varovania a určovania vplyvu incidentov súvisiacich s IKT a ich závažnosti;

b) kvalitu a rýchlosť vykonávania forenznej analýzy;

c) účinnosť eskalácie incidentu v rámci finančného subjektu;

d) účinnosť vnútornej a vonkajšej komunikácie.

3. Poznatky získané z testovania digitálnej prevádzkovej odolnosti, ktoré sa vykonalo v súlade s článkami 23 a 24, a z reálnych incidentov súvisiacich s IKT, najmä kybernetických útokov, spolu s výzvami, ktorým čelí aktivácia plánov na zabezpečenie kontinuity činnosti alebo plánov obnovy spolu s príslušnými informáciami vymieňanými s protistranami a posudzovanými počas preskúmaní orgánmi dohľadu, sa náležite a nepretržite začleňujú do procesu posudzovania IKT rizika. Tieto zistenia sa premietnu do vhodných preskúmaní príslušných zložiek rámca riadenia IKT rizika uvedeného v článku 5 ods. 1.

4. Finančné subjekty monitorujú účinnosť vykonávania svojej stratégie digitálnej odolnosti stanovenej v článku 5 ods. 9. Mapujú vývoj v oblasti IKT rizík v priebehu času, analyzujú frekvenciu, druhy, rozsah a vývoj incidentov súvisiacich s IKT, najmä kybernetických útokov a ich vzorcov, s cieľom pochopiť úroveň vystavenia IKT riziku a zlepšiť kybernetickú vyspelosť a pripravenosť finančného subjektu.

5. Vedúci pracovníci v oblasti IKT podávajú aspoň raz ročne riadiacemu orgánu správu o zisteniach uvedených v odseku 3 a predkladajú odporúčania.

6. Finančné subjekty vypracujú programy zvyšovania informovanosti o bezpečnosti v oblasti IKT a školenia o digitálnej prevádzkovej odolnosti ako povinné moduly vo svojich systémoch odbornej prípravy zamestnancov. Toto sa vzťahuje na všetkých zamestnancov a na pracovníkov vrcholového manažmentu.

Finančné subjekty priebežne monitorujú príslušný technologický vývoj, a to aj s cieľom pochopiť možné vplyvy zavádzania takýchto nových technológií na bezpečnostné požiadavky v oblasti IKT a digitálnu prevádzkovú odolnosť. Musia držať krok s najnovšími procesmi riadenia IKT rizika a zároveň účinne bojovať proti súčasným alebo novým formám kybernetických útokov.

Článok 13

Komunikácia

1. Finančné subjekty majú ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 zavedené komunikačné plány, ktoré umožňujú zodpovedné zverejňovanie incidentov súvisiacich s IKT alebo závažných zraniteľných miest pre klientov a protistrany, ako aj pre verejnosť, podľa konkrétneho prípadu.

2. Finančné subjekty vykonávajú ako súčasť rámca riadenia IKT rizika uvedeného v článku 5 ods. 1 komunikačné politiky pre zamestnancov a externé zainteresované strany. V komunikačných politikách pre zamestnancov sa zohľadňuje potreba rozlišovať medzi zamestnancami, ktorí sú zapojení do riadenia IKT rizika, najmä pokiaľ ide o reakciu a obnovu, a pracovníkmi, ktorí musia byť informovaní.

3. Aspoň jedna osoba v subjekte musí byť poverená vykonávaním komunikačnej stratégie pre incidenty súvisiace s IKT a na tento účel plní pre verejnosť a médiá úlohu hovorcu subjektu.

Článok 14

Ďalšia harmonizácia nástrojov, metód, postupov a politík riadenia IKT rizika

Európsky orgán pre bankovníctvo (EBA), Európsky orgán pre cenné papiere a trhy (ESMA) a Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (EIOPA) vypracujú po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ENISA) návrh regulačných technických predpisov na tieto účely:

a) bližšie spresniť ďalšie prvky, ktoré sa majú zahrnúť do bezpečnostných politík, postupov, protokolov a nástrojov v oblasti IKT uvedených v článku 8 ods. 2, aby sa zaistila bezpečnosť sietí, umožnili primerané záruky proti neoprávneným vniknutiam a zneužitiu údajov, zachovala autentickosť a integrita údajov vrátane kryptografických techník, ako aj zaručil presný a rýchly prenos údajov bez závažných narušení;

b) stanoviť, ako sa v bezpečnostných politikách, postupoch a nástrojoch v oblasti IKT uvedených v článku 8 ods. 2 zabudujú bezpečnostné kontroly do systémov od začiatku (bezpečnosť už v štádiu návrhu), zohľadnia úpravy v dôsledku vyvíjajúceho sa prostredia hrozieb a stanoví používanie technológie hĺbkovej ochrany;

c) bližšie spresniť vhodné techniky, metódy a protokoly uvedené v článku 8 ods. 4 písm. b);

d) vypracovať ďalšie zložky kontrol práv na riadenie prístupu uvedené v článku 8 ods. 4 písm. c) a súvisiacej politiky v oblasti ľudských zdrojov, ktorými sa upresnia prístupové práva, postupy udeľovania a odoberania práv, monitorovanie anomálneho správania vo vzťahu k IKT rizikám prostredníctvom vhodných ukazovateľov, a to aj pokiaľ ide o modely využívania siete, hodiny, činnosť v oblasti IT a neznáme zariadenia;

e) ďalej rozvíjať prvky uvedené v článku 9 ods. 1, ktoré umožňujú rýchle odhalenie anomálnych činností, a kritériá uvedené v článku 9 ods. 2, ktoré spúšťajú procesy zisťovania a reakcie na incidenty súvisiace s IKT;

f) bližšie spresniť zložky politiky kontinuity činností v oblasti IKT uvedenej v článku 10 ods. 1;

g) bližšie spresniť testovanie plánov kontinuity činností v oblasti IKT uvedené v článku 10 ods. 5 s cieľom zabezpečiť, aby sa v nich náležite zohľadnili scenáre, v ktorých sa kvalita poskytovania kritickej alebo dôležitej funkcie zhoršuje na neprijateľnú úroveň alebo zlyháva, ako aj náležite zvážil potenciálny vplyv platobnej neschopnosti alebo iných zlyhaní ktoréhokoľvek príslušného externého poskytovateľa IKT služieb a prípadne politické riziká v jurisdikciách príslušných poskytovateľov;

h) bližšie spresniť zložky plánu obnovy po havárii v oblasti IKT uvedeného v článku 10 ods. 3.

Orgány EBA, ESMA a EIOPA predložia Komisii návrh týchto regulačných technických predpisov do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc prijať regulačné technické predpisy uvedené v prvom pododseku v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

KAPITOLA III

INCIDENTY SÚVISIACE S IKT

RIADENIE, KLASIFIKÁCIA a NAHLASOVANIE ÚDAJOV

Článok 15

Postup riadenia incidentov súvisiacich s IKT

1. Finančné subjekty stanovia a vykonávajú postup riadenia incidentov súvisiacich s IKT s cieľom odhaľovať, riadiť a oznamovať incidenty súvisiace s IKT a zavedú ukazovatele včasného varovania ako upozornenia.

2. Finančné subjekty stanovia vhodné postupy na zaistenie konzistentného a integrovaného monitorovania, riešenia a následných opatrení v prípade incidentov súvisiacich s IKT s cieľom zabezpečiť, aby sa identifikovali a odstránili hlavné príčiny a zabránilo výskytu takýchto incidentov.

3. Procesom riadenia incidentov súvisiacich s IKT uvedeným v odseku 1 sa:

   a) v súlade s kritériami uvedenými v článku 16 ods. 1 stanovujú postupy na identifikáciu, sledovanie, zaznamenávanie, kategorizáciu a klasifikáciu incidentov súvisiacich s IKT podľa ich priority a závažnosti a kritickosti zasiahnutých služieb;

   b) prideľujú úlohy a zodpovednosti, ktoré treba aktivovať pre jednotlivé druhy a scenáre incidentov súvisiacich s IKT;

   c) stanovujú plány komunikácie so zamestnancami, externými zainteresovanými stranami a médiami v súlade s článkom 13, oznamovania klientom, interných eskalačných postupov vrátane sťažností zákazníkov súvisiacich s IKT, ako aj prípadne poskytovania informácií finančným subjektom, ktoré konajú ako protistrany;

   d) zabezpečuje, aby sa závažné incidenty súvisiace s IKT nahlasovali príslušnému vrcholovému manažmentu, ako aj že je riadiaci orgán informovaný o závažných incidentoch súvisiacich s IKT, pričom je vysvetlený vplyv, reakcia a dodatočné kontroly, ktoré sa majú zaviesť v dôsledku incidentov súvisiacich s IKT;

   e) stanovujú postupy reakcie na incidenty súvisiace s IKT s cieľom zmierniť vplyvy a zabezpečiť včasné sfunkčnenie a bezpečnosť služieb.

Článok 16

Klasifikácia incidentov súvisiacich s IKT

1. Finančné subjekty klasifikujú incidenty súvisiace s IKT a určujú ich vplyv na základe týchto kritérií:

   a) počet používateľov alebo finančných protistrán, ktoré sú ovplyvnené narušením spôsobeným incidentom súvisiacim s IKT, a to, či incident súvisiaci s IKT mal vplyv na dobré meno;

   b) trvanie incidentu súvisiaceho s IKT vrátane výpadku služby;

c) geografické rozloženie, pokiaľ ide o oblasti postihnuté incidentom súvisiacim s IKT, najmä ak sa týka viac ako dvoch členských štátov;

d) straty údajov spôsobené incidentom súvisiacim s IKT, ako je strata integrity, strata dôvernosti alebo strata dostupnosti;

e) závažnosť vplyvu incidentu súvisiaceho s IKT na IKT systémy finančného subjektu;

f) kritickosť zasiahnutých služieb vrátane transakcií a operácií finančného subjektu;

g) hospodársky vplyv incidentu súvisiaceho s IKT v absolútnom aj relatívnom vyjadrení.

2. Európske orgány dohľadu vypracujú prostredníctvom Spoločného výboru európskych orgánov dohľadu („spoločný výbor“) a po konzultáciách s Európskou centrálnou bankou (ECB) a agentúrou ENISA spoločný návrh regulačných technických predpisov, v ktorých sa bližšie spresnia:

a) kritériá stanovené v odseku 1 vrátane prahových hodnôt významnosti na určenie závažných incidentov súvisiacich s IKT, na ktoré sa vzťahuje ohlasovacia povinnosť stanovená v článku 17 ods. 1;

b) kritériá, ktoré majú príslušné orgány uplatňovať na účely posúdenia relevantnosti závažných incidentov súvisiacich s IKT pre jurisdikcie iných členských štátov, ako aj podrobnosti týkajúce sa správ o incidentoch súvisiacich s IKT, ktoré sa majú poskytnúť iným príslušným orgánom podľa článku 17 ods. 5 a 6.

3. Pri vypracúvaní spoločného návrhu regulačných technických predpisov uvedeného v odseku 2 európske orgány dohľadu zohľadňujú medzinárodné normy, ako aj špecifikácie vypracované a uverejnené agentúrou ENISA vrátane prípadných špecifikácií pre iné hospodárske odvetvia.

Európske orgány dohľadu predložia tento spoločný návrh regulačných technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v odseku 2 v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

Článok 17

Nahlasovanie závažných incidentov súvisiacich s IKT

1. Finančné subjekty nahlasujú závažné incidenty súvisiace s IKT dotknutému príslušnému orgánu uvedenému v článku 41 v lehotách stanovených v odseku 3.

Na účely prvého pododseku finančné subjekty vypracujú po zhromaždení a analýze všetkých relevantných informácií správu o incidente s použitím vzoru uvedeného v článku 18 a predložia ju príslušnému orgánu.

Správa obsahuje všetky informácie, ktoré príslušný orgán potrebuje na určenie významnosti závažného incidentu súvisiaceho s IKT a posúdenie možných cezhraničných vplyvov.

2. Ak závažný incident súvisiaci s IKT má alebo môže mať vplyv na finančné záujmy používateľov služieb a klientov, finančné subjekty bez zbytočného odkladu informujú svojich používateľov služieb a klientov o závažnom incidente súvisiacom s IKT a čo najskôr ich informujú o všetkých opatreniach, ktoré boli prijaté na zmiernenie nepriaznivých účinkov takéhoto incidentu.

3. Finančné subjekty predložia príslušnému orgánu uvedenému v článku 41:

   a) pôvodné oznámenie bezodkladne, najneskôr však do konca pracovného dňa, alebo v prípade závažného incidentu súvisiaceho s IKT, ku ktorému došlo najneskôr 2 hodiny pred koncom pracovného dňa, najneskôr do 4 hodín od začiatku nasledujúceho pracovného dňa alebo, ak kanály nahlasovania nie sú k dispozícii, hneď, ako budú k dispozícii;

   b) priebežnú správu najneskôr 1 týždeň po pôvodnom oznámení uvedenom v písmene a), po ktorej prípadne nasledujú aktualizované oznámenia vždy, keď je k dispozícii príslušná aktualizácia stavu, ako aj na základe osobitnej žiadosti príslušného orgánu;

   c) záverečnú správu po dokončení analýzy hlavných príčin, bez ohľadu na to, či už boli alebo neboli vykonané zmierňujúce opatrenia, a keď sú k dispozícii skutočné údaje o vplyve, aby sa nahradili odhady, najneskôr však do jedného mesiaca od zaslania pôvodnej správy.

4. Finančné subjekty môžu delegovať ohlasovacie povinnosti podľa tohto článku na externého poskytovateľa služieb len na základe schválenia delegovania dotknutým príslušným orgánom uvedeným v článku 41.

5. Po prijatí správy uvedenej v odseku 1 príslušný orgán bez zbytočného odkladu poskytne podrobné informácie o incidente:

   a) orgánom EBA, ESMA alebo EIOPA, a to podľa konkrétneho prípadu;

   b) ECB, podľa potreby, v prípade finančných subjektov uvedených v článku 2 ods. 1 písm. a), b) a c); a

   c) jednotnému kontaktnému miestu určenému podľa článku 8 smernice (EÚ) 2016/1148.

6. Orgány EBA, ESMA alebo EIOPA, ako aj ECB posúdia relevantnosť závažného incidentu súvisiaceho s IKT pre iné príslušné verejné orgány a čo najskôr ich informujú. ECB informuje členov Európskeho systému centrálnych bánk o otázkach relevantných pre platobné systémy. Na základe uvedeného oznámenia príslušné orgány v relevantných prípadoch prijmú všetky nevyhnutné opatrenia s cieľom ochrániť bezprostrednú stabilitu finančného systému.

Článok 18

Harmonizácia obsahu a vzorov nahlasovania

1. Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultáciách s agentúrou ENISA a s ECB vypracujú:

   a) spoločný návrh regulačných technických predpisov s cieľom:

      1. stanoviť obsah nahlasovania závažných incidentov súvisiacich s IKT;

      2. bližšie spresniť podmienky, za ktorých finančné subjekty môžu na základe predchádzajúceho súhlasu príslušného orgánu delegovať na

externého poskytovateľa služieb ohlasovacie povinnosti stanovené v tejto kapitole;

b) spoločný návrh vykonávacích technických predpisov s cieľom stanoviť štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT.

Európske orgány dohľadu predložia Komisii spoločný návrh regulačných technických predpisov uvedený v odseku 1 písm. a) a spoločný návrh vykonávacích technických predpisov uvedený v odseku 1 písm. b) do xx 202x [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v odseku 1 písm. a) v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

Komisii sa udeľuje právomoc prijať spoločné vykonávacie technické predpisy uvedené v odseku 1 písm. b) v súlade s článkom 15 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

Článok 19

Centralizácia nahlasovania závažných incidentov súvisiacich s IKT

1. Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s ECB a agentúrou ENISA vypracujú spoločnú správu, v ktorej posúdia uskutočniteľnosť ďalšej centralizácie nahlasovania incidentov pomocou zriadenia jednotného centra EÚ pre nahlasovanie závažných incidentov súvisiacich s IKT finančnými subjektmi. V správe sa preskúmajú spôsoby, ako uľahčiť tok nahlasovania údajov o incidentoch súvisiacich s IKT, znížiť súvisiace náklady a podporiť tematické analýzy s cieľom posilniť konvergenciu dohľadu.

2. Správa uvedená v odseku 1 musí obsahovať aspoň tieto prvky:

a) predpoklady na zriadenie takéhoto centra EÚ;

b) prínosy, obmedzenia a možné riziká;

c) prvky prevádzkového riadenia;

d) podmienky členstva;

e) spôsoby prístupu finančných subjektov a príslušných vnútroštátnych orgánov k centru EÚ;

f) predbežné posúdenie finančných nákladov spojených so zriadením prevádzkovej platformy na podporu centra EÚ vrátane požadovaných odborných znalostí.

3. Európske orgány dohľadu predložia správu uvedenú v odseku 1 Komisii, Európskemu parlamentu a Rade do xx 202x [*Úrad pre publikácie: vložte dátum 3 roky po nadobudnutí účinnosti*].

Článok 20

Spätná väzba orgánov dohľadu

1. Po prijatí správy uvedenej v článku 17 ods. 1 príslušný orgán potvrdí prijatie oznámenia a čo najskôr poskytne všetku potrebnú spätnú väzbu alebo usmernenia

finančnému subjektu, najmä s cieľom prediskutovať nápravné opatrenia na úrovni subjektu alebo spôsoby minimalizovania nepriaznivého vplyvu v jednotlivých sektoroch.

2. Európske orgány dohľadu podávajú každoročne prostredníctvom spoločného výboru anonymizované a súhrnné správy o oznámeniach o incidentoch súvisiacich s IKT, ktoré dostali od príslušných orgánov, pričom uvedú aspoň počet závažných incidentov súvisiacich s IKT, ich povahu, vplyv na operácie finančných subjektov alebo zákazníkov, náklady a prijaté nápravné opatrenia.

   Európske orgány dohľadu vydávajú varovania a vypracúvajú štatistiky na vysokej úrovni na podporu posudzovania hrozieb a zraniteľnosti IKT.

KAPITOLA IV

TESTOVANIE DIGITÁLNEJ PREVÁDZKOVEJ ODOLNOSTI

Článok 21

Všeobecné požiadavky na vykonávanie testovania digitálnej prevádzkovej odolnosti

1. Na účely posúdenia pripravenosti na incidenty súvisiace s IKT, identifikácie nedostatkov a slabých miest digitálnej prevádzkovej odolnosti a urýchleného vykonania nápravných opatrení finančné subjekty zriadia, udržiavajú a preskúmavajú so zreteľom na svoju veľkosť, obchodný a rizikový profil spoľahlivý a komplexný program na testovanie digitálnej prevádzkovej odolnosti ako integrálnu súčasť rámca riadenia IKT rizika uvedeného v článku 5.

2. Program na testovanie digitálnej prevádzkovej odolnosti zahŕňa celý rad posúdení, testov, metodík, postupov a nástrojov, ktoré sa majú uplatňovať v súlade s ustanoveniami článkov 22 a 23.

3. Finančné subjekty sa pri vykonávaní programu na testovanie digitálnej prevádzkovej odolnosti uvedeného v odseku 1 riadia prístupom založeným na rizikách, pričom zohľadňujú vyvíjajúce sa prostredie v oblasti IKT rizík, akékoľvek špecifické riziká, ktorým finančný subjekt je alebo môže byť vystavený, kritickosť informačných aktív a poskytovaných služieb, ako aj akýkoľvek iný faktor, ktorý finančný subjekt považuje za vhodný.

4. Finančné subjekty zabezpečia, aby testy vykonávali nezávislé strany, či už interné alebo externé.

5. Finančné subjekty stanovia postupy a politiky na stanovenie priorít, klasifikáciu a nápravu všetkých problémov potvrdených počas vykonávania testov a zavedú interné metodiky validácie s cieľom zabezpečiť úplné riešenie všetkých zistených nedostatkov a slabých miest.

6. Finančné subjekty testujú všetky kritické IKT systémy a aplikácie aspoň raz ročne.

Článok 22

Testovanie IKT nástrojov a systémov

1. V rámci programu na testovanie digitálnej prevádzkovej odolnosti uvedeného v článku 21 sa zabezpečí vykonanie celej škály vhodných testov vrátane posúdení a prehľadov zraniteľnosti, analýz otvorených zdrojov, posúdení bezpečnosti sietí,

analýz nedostatkov, preskúmaní fyzickej bezpečnosti, dotazníkov a skenovacích softvérových riešení, preskúmaní zdrojových kódov, ak je to možné, testov založených na konkrétnych scenároch, testovania kompatibility, testovania výkonnosti, testovania medzi koncovými bodmi alebo penetračného testovania.

2. Finančné subjekty uvedené v článku 2 ods. 1 písm. f) a g) vykonávajú posúdenia zraniteľnosti pred každým nasadením alebo presunom nových alebo existujúcich služieb podporujúcich kritické funkcie, aplikácie a zložky infraštruktúry finančného subjektu.

Článok 23

Pokročilé testovanie IKT nástrojov, systémov a procesov vychádzajúce z penetračného testovania na základe konkrétnej hrozby

1. Finančné subjekty identifikované v súlade s odsekom 4 vykonávajú najmenej každé tri roky pokročilé testovanie prostredníctvom penetračného testovania na základe konkrétnej hrozby.

2. Penetračné testovanie na základe konkrétnej hrozby zahŕňa prinajmenej kritické funkcie a služby finančného subjektu a vykonáva sa na živých produkčných systémoch podporujúcich takéto funkcie. Presný rozsah penetračného testovania na základe konkrétnej hrozby, ktoré vychádza z posúdenia kritických funkcií a služieb, určujú finančné subjekty a overujú ho príslušné orgány.

   Na účely prvého pododseku finančné subjekty identifikujú všetky relevantné súvisiace IKT procesy, systémy a technológie podporujúce kritické funkcie a služby vrátane funkcií a služieb, ktoré sú externe zabezpečované alebo zmluvne dohodnuté s externým poskytovateľom IKT služieb.

   Ak sú externí poskytovatelia IKT služieb zahrnutí do pôsobnosti penetračného testovania na základe konkrétnej hrozby, finančný subjekt prijme potrebné opatrenia na zabezpečenie účasti týchto poskytovateľov.

   Finančné subjekty uplatňujú účinné kontroly riadenia rizík s cieľom znížiť riziká akéhokoľvek potenciálneho vplyvu na údaje, poškodenie aktív a narušenie kritických služieb alebo operácií v samotnom finančnom subjekte, jeho protistranách alebo vo finančnom sektore.

   Na konci testovania, po schválení správ a plánov nápravy, finančný subjekt a externé testovacie subjekty poskytnú príslušnému orgánu dokumentáciu potvrdzujúcu, že penetračné testovanie na základe konkrétnej hrozby bolo vykonané v súlade s požiadavkami. Príslušné orgány overujú dokumentáciu a vydávajú osvedčenie.

3. Finančné subjekty uzatvárajú zmluvy s testovacími subjektmi v súlade s článkom 24 na účely vykonania penetračného testovania na základe konkrétnej hrozby.

   Príslušné orgány určia finančné subjekty, ktoré majú vykonávať penetračné testovanie na základe konkrétnej hrozby, spôsobom, ktorý je úmerný veľkosti, rozsahu, činnosti a celkovému rizikovému profilu finančného subjektu, a to na základe posúdenia:

   a) faktorov súvisiacich s vplyvom, najmä kritickosti poskytovaných služieb a činností vykonávaných finančným subjektom;

   b) prípadných obáv o finančnú stabilitu vrátane systémového charakteru finančného subjektu na vnútroštátnej úrovni alebo prípadne na úrovni Únie;

c) špecifického profilu IKT rizika, úrovne vyspelosti IKT finančného subjektu alebo súvisiacich technologických prvkov.

4. Orgány EBA, ESMA a EIOPA po konzultácii s ECB a po zohľadnení príslušných rámcov v Únii, ktoré sa uplatňujú na penetračné testovania založené na spravodajských informáciách, vypracujú návrh regulačných technických predpisov s cieľom bližšie spresniť:

a) kritériá používané na účely uplatňovania odseku 6 tohto článku;

b) požiadavky v súvislosti s:

a) rozsahom penetračného testovania na základe konkrétnej hrozby uvedeného v odseku 2 tohto článku;

b) metodikou testovania a prístupom, ktoré sa majú dodržiavať pre každú konkrétnu fázu testovania;

c) výsledkami, záverečnými a nápravnými štádiami testovania;

c) druh spolupráce medzi orgánmi dohľadu potrebný na vykonávanie penetračného testovania na základe konkrétnej hrozby v kontexte finančných subjektov, ktoré pôsobia vo viac ako jednom členskom štáte, aby sa umožnila primeraná úroveň zapojenia orgánov dohľadu a pružné vykonávanie s cieľom zohľadniť osobitosti finančných podsektorov alebo miestnych finančných trhov.

Európske orgány dohľadu predložia tento návrh regulačných technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 2 mesiace pred nadobudnutím účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v druhom pododseku v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

Článok 24

Požiadavky na testovacie subjekty

1. Finančné subjekty využívajú na realizáciu penetračného testovania na základe konkrétnej hrozby iba testovacie subjekty, ktoré:

a) sú najvhodnejšie a najuznávanejšie;

b) disponujú technickými a organizačnými schopnosťami a preukazujú osobitné odborné znalosti v oblasti spravodajských informácií o hrozbách, penetračného testovania alebo testovania prostredníctvom červeného tímu;

c) sú certifikované akreditačným orgánom v členskom štáte alebo dodržiavajú formálne kódexy správania alebo etické rámce;

d) v prípade externých testovacích subjektov poskytujú nezávislé uistenie alebo audítorskú správu v súvislosti so správnym riadením rizík spojených s vykonávaním penetračného testovania na základe konkrétnej hrozby vrátane riadnej ochrany dôverných informácií finančného subjektu a nápravy obchodných rizík finančného subjektu;

e) v prípade externých testovacích subjektov sú riadne a v plnom rozsahu kryté príslušnými poistením zodpovednosti za škodu spôsobenú pri výkone povolania, a to aj pre prípad pochybenia a nedbanlivosti.

2. Finančné subjekty zabezpečia, aby sa v dohodách uzavretých s externými testovacími subjektmi vyžadovalo správne riadenie výsledkov penetračného testovania na základe konkrétnej hrozby a aby akékoľvek ich spracovanie vrátane akéhokoľvek generovania, navrhovania, uchovávania, agregácie, podávania správ, komunikácie alebo likvidácie nevytváralo pre finančný subjekt riziká.

KAPITOLA V

RIADENIE IKT RIZIKA TRETEJ STRANY

ODDIEL I

KĽÚČOVÉ ZÁSADY SPRÁVNEHO RIADENIA IKT RIZIKA TRETEJ STRANY

Článok 25

Všeobecné zásady

Finančné subjekty riadia IKT riziko tretej strany ako integrálnu súčasť IKT rizika v medziach svojho rámca riadenia IKT rizika a v súlade s týmito zásadami:

1. Finančné subjekty, ktoré majú uzavreté zmluvné dojednania o využívaní IKT služieb na vykonávanie svojich obchodných činností, sú vždy plne zodpovedné za dodržiavanie a plnenie všetkých povinností vyplývajúcich z tohto nariadenia a uplatniteľných právnych predpisov o finančných službách.

2. Riadenie IKT rizika tretej strany finančnými subjektmi sa vykonáva so zreteľom na zásadu proporcionality, pričom sa zohľadňujú tieto aspekty:

   a) rozsah, zložitosť a význam závislostí súvisiacich s IKT;

   b) riziká vyplývajúce zo zmluvných dojednaní o využívaní IKT služieb uzavretých s externými poskytovateľmi IKT služieb, pričom sa zohľadňuje kritickosť alebo význam príslušnej služby, procesu alebo funkcie, ako aj potenciálny vplyv na kontinuitu a kvalitu finančných služieb a činností na individuálnej úrovni a na úrovni skupiny.

3. Finančné subjekty ako súčasť svojho rámca riadenia IKT rizika prijímajú a pravidelne preskúmavajú stratégiu týkajúcu sa IKT rizika tretej strany, pričom zohľadňujú stratégiu viacerých dodávateľov uvedenú v článku 5 ods. 9 písm. g). Uvedená stratégia zahŕňa politiku využívania IKT služieb poskytovaných externými poskytovateľmi IKT služieb a uplatňuje sa na individuálnom, ako aj podľa potreby na subkonsolidovanom a konsolidovanom základe. Riadiaci orgán pravidelne preskúmava riziká zistené v súvislosti s externým zabezpečovaním kritických alebo dôležitých funkcií.

4. Finančné subjekty ako súčasť svojho rámca riadenia IKT rizika vedú a aktualizujú na úrovni subjektu, ako aj na subkonsolidovanej a konsolidovanej úrovni register informácií v súvislosti so všetkými zmluvnými dojednaniami o využívaní IKT služieb poskytovaných externými poskytovateľmi IKT služieb.

   Zmluvné dojednania uvedené v prvom pododseku musia byť náležite zdokumentované, pričom sa rozlišuje medzi tými, ktoré sa vzťahujú na kritické alebo dôležité funkcie, a tými, ktoré sa na ne nevzťahujú.

Finančné subjekty aspoň raz ročne nahlasujú príslušným orgánom informácie o počte nových dojednaní o využívaní IKT služieb, kategóriách externých poskytovateľov IKT služieb, druhu zmluvných dojednaní a poskytovaných službách a funkciách.

Finančné subjekty sprístupnia príslušnému orgánu na jeho žiadosť úplný register informácií alebo na požiadanie jeho konkrétne oddiely spolu so všetkými informáciami, ktoré sa považujú za potrebné na umožnenie účinného dohľadu nad finančným subjektom.

Finančné subjekty včas informujú príslušný orgán o plánovanom uzatvorení zmlúv týkajúcich sa kritických alebo dôležitých funkcií a o tom, kedy sa funkcia stala kritickou alebo dôležitou.

5. Pred uzavretím zmluvného dojednania o využívaní IKT služieb finančné subjekty:

   a) posúdia, či sa zmluvné dojednanie vzťahuje na kritickú alebo dôležitú funkciu;

   b) posúdia, či sú splnené podmienky dohľadu pre uzatváranie zmlúv;

   c) určia a posúdia všetky relevantné riziká v súvislosti so zmluvným dojednaním vrátane možnosti, že takéto zmluvné dojednania môžu prispieť k posilneniu rizika koncentrácie IKT;

   d) vykonajú všetku náležitú starostlivosť v súvislosti s potenciálnymi externými poskytovateľmi IKT služieb a zabezpečia vhodnosť externého poskytovateľa IKT služieb počas celého procesu výberu a posudzovania;

   e) určia a posúdia konflikty záujmov, ktoré môže zmluvné dojednanie spôsobiť.

6. Finančné subjekty môžu uzatvárať zmluvné dojednania len s externými poskytovateľmi IKT služieb, ktorí spĺňajú prísne, primerané a najnovšie normy v oblasti informačnej bezpečnosti.

7. Pri vykonávaní práv na prístup, kontrolu a audit, pokiaľ ide o externého poskytovateľa IKT služieb, finančné subjekty na základe prístupu založeného na rizikách vopred určia frekvenciu auditov a kontrol, ako aj oblasti, v ktorých sa má audit vykonať dodržiavaním všeobecne uznávaných audítorských štandardov v súlade s pokynmi orgánov dohľadu o používaní a začlenení týchto audítorských štandardov.

   V prípade zmluvných dojednaní, ktoré so sebou prinášajú vysokú úroveň technologickej zložitosti, finančný subjekt overí, či audítori, a to interní, skupiny audítorov alebo externí audítori, majú primerané zručnosti a znalosti na účinné vykonávanie príslušných auditov a posúdení.

8. Finančné subjekty zabezpečia, aby sa zmluvné dojednania o využívaní IKT služieb ukončili aspoň za týchto okolností:

   a) porušenie uplatniteľných zákonov, iných právnych predpisov alebo zmluvných podmienok zo strany externého poskytovateľa IKT služieb;

   b) okolnosti zistené počas monitorovania IKT rizika tretej strany, ktoré sa považujú za schopné zmeniť výkon funkcií poskytovaných prostredníctvom zmluvného dojednania vrátane závažných zmien, ktoré majú vplyv na dojednanie alebo situáciu externého poskytovateľa IKT služieb;

   c) preukázané nedostatky externého poskytovateľa IKT služieb, pokiaľ ide o celkové riadenie IKT rizika, a najmä spôsob zaisťovania bezpečnosti

a integrity dôverných, osobných alebo inak citlivých údajov alebo iných ako osobných informácií;

d) okolnosti, za ktorých príslušný orgán už nemôže účinne vykonávať dohľad nad finančným subjektom v dôsledku príslušného zmluvného dojednania.

9. Finančné subjekty zavedú stratégie ukončenia angažovanosti s cieľom zohľadniť riziká, ktoré môžu vzniknúť na úrovni externého poskytovateľa IKT služieb, najmä jeho možné zlyhanie, zhoršenie kvality poskytovaných funkcií, akékoľvek narušenie obchodnej činnosti v dôsledku neprimeraného alebo neúspešného poskytovania služieb alebo závažného rizika vyplývajúceho z primeraného a nepretržitého zavádzania funkcie.

Finančné subjekty zabezpečia, aby mohli ukončiť zmluvné dojednania bez:

a) narušenia svojej obchodnej činnosti;

b) obmedzenia dodržiavania regulačných požiadaviek;

c) ohrozenia kontinuity a kvality poskytovania služieb klientom.

Plány ukončenia angažovanosti musia byť komplexné, zdokumentované a v prípade potreby dostatočne otestované.

Finančné subjekty určia alternatívne riešenia a vypracujú prechodné plány, ktoré im umožnia odstrániť zmluvne dohodnuté funkcie a príslušné údaje od externého poskytovateľa IKT služieb a bezpečne a úplne ich preniesť na alternatívnych poskytovateľov alebo ich opätovne začleniť medzi interne zabezpečované funkcie.

Finančné subjekty prijmú primerané krízové opatrenia na zachovanie kontinuity činnosti za všetkých okolností uvedených v prvom pododseku.

10. Európske orgány dohľadu vypracujú prostredníctvom spoločného výboru návrh vykonávacích technických predpisov na stanovenie štandardných vzorov na účely registra informácií uvedeného v odseku 4.

Európske orgány dohľadu predložia tento návrh vykonávacích technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti tohto nariadenia*].

Komisii sa udeľuje právomoc, aby prijala vykonávacie technické predpisy uvedené v prvom pododseku v súlade s článkom 15 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

11. Európske orgány dohľadu vypracujú prostredníctvom spoločného výboru návrh regulačných predpisov s cieľom:

a) bližšie spresniť podrobný obsah politiky uvedenej v odseku 3 v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb poskytovaných externými poskytovateľmi IKT služieb s odkazom na hlavné fázy životného cyklu príslušných dojednaní o využívaní IKT služieb;

b) bližšie spresniť druhy informácií, ktoré majú byť zahrnuté do registra informácií uvedeného v odseku 4.

Európske orgány dohľadu predložia tento návrh regulačných technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v druhom pododseku v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

Článok 26

Predbežné posúdenie rizika koncentrácie IKT a ďalšie dojednania týkajúce sa dohôd o sub-outsorcingu

1. Pri určovaní a posudzovaní rizika koncentrácie IKT uvedeného v článku 25 ods. 5 písm. c) finančné subjekty zohľadňujú, či by uzavretie zmluvného dojednania v súvislosti s IKT službami viedlo k niektorej z týchto skutočností:

   a) uzatvorenie zmluvy s externým poskytovateľom IKT služieb, ktorý nie je ľahko nahraditeľný, alebo

   b) uzatvorenie viacerých zmluvných dojednaní v súvislosti s poskytovaním IKT služieb s tým istým externým poskytovateľom IKT služieb alebo s úzko prepojenými externými poskytovateľmi IKT služieb.

   Finančné subjekty zvážia prínosy a náklady alternatívnych riešení, ako je využívanie rôznych externých poskytovateľov IKT služieb, a súčasne zohľadnia, či a ako plánované riešenia zodpovedajú obchodným potrebám a cieľom stanoveným v ich stratégii digitálnej odolnosti.

2. Ak zmluvné dojednanie o využívaní IKT služieb zahŕňa možnosť, že externý poskytovateľ IKT služieb ďalej zadá subdodávateľskú zákazku týkajúcu sa kritickej alebo dôležitej funkcie iným externým poskytovateľom IKT služieb, finančné subjekty zvážia prínosy a riziká, ktoré môžu vzniknúť v súvislosti s takouto možnou subdodávateľskou zákazkou, najmä v prípade subdodávateľa IKT usadeného v tretej krajine.

   Ak sa zmluvné dojednania o využívaní IKT služieb uzatvárajú s externým poskytovateľom IKT služieb usadeným v tretej krajine, finančné subjekty považujú za relevantné aspoň tieto faktory:

   a) dodržiavanie práv na ochranu údajov;

   b) účinné presadzovanie práva;

   c) ustanovenia zákona o platobnej neschopnosti, ktoré by sa uplatňovali v prípade konkurzu externého poskytovateľa IKT služieb;

   d) akékoľvek obmedzenia, ktoré môžu vzniknúť v súvislosti s naliehavým obnovovaním údajov finančného subjektu.

   Finančné subjekty posúdia, či a ako môžu potenciálne dlhé alebo zložité subdodávateľské reťazce ovplyvniť ich schopnosť plne monitorovať zmluvne dohodnuté funkcie a schopnosť príslušného orgánu vykonávať účinný dohľad nad finančným subjektom v tejto súvislosti.

Článok 27

Kľúčové zmluvné ustanovenia

1. Práva a povinnosti finančného subjektu a externého poskytovateľa IKT služieb sa jasne pridelia a stanovia písomne. Úplná zmluva, ktorá zahŕňa dohody o úrovni poskytovaných služieb, sa zdokumentuje v jednom písomnom dokumente, ktorý

majú zmluvné strany k dispozícii v papierovej forme alebo v stiahnuteľnom a prístupnom formáte.

2. Zmluvné dojednania o využívaní IKT služieb zahŕňajú aspoň:

a) jasný a úplný opis všetkých funkcií a služieb, ktoré má externý poskytovateľ IKT služieb poskytovať, pričom sa uvedie, či je povolené zadávanie kritickej alebo dôležitej funkcie alebo jej závažných častí subdodávateľovi, a ak áno, podmienky vzťahujúce sa na takéto využívanie subdodávateľa;

b) miesta, kde sa majú poskytovať zmluvne dohodnuté alebo subdodávateľské funkcie a služby a kde sa majú údaje spracúvať vrátane miesta uloženia, ako aj požiadavka, aby externý poskytovateľ IKT služieb informoval finančný subjekt, ak plánuje zmeniť takéto miesta;

c) ustanovenia o prístupnosti, dostupnosti, integrite, bezpečnosti a ochrane osobných údajov, ako aj o zabezpečení prístupu, obnovy a návratu k osobným údajom a iným ako osobným údajom spracúvaným finančným subjektom v ľahko prístupnom formáte v prípade platobnej neschopnosti, riešenia krízových situácií alebo ukončenia obchodných operácií externého poskytovateľa IKT služieb;

d) úplné opisy úrovne služieb vrátane ich aktualizácií a revízií, ako aj presné kvantitatívne a kvalitatívne výkonnostné ciele v rámci dohodnutých úrovní služieb, aby ich finančný subjekt mohol účinne monitorovať a mal možnosť bez zbytočného odkladu vykonať primerané nápravné opatrenia v prípade nesplnenia dohodnutých úrovní služieb;

e) výpovedné lehoty a ohlasovacie povinnosti externého poskytovateľa IKT služieb voči finančnému subjektu vrátane oznamovania akéhokoľvek vývoja, ktorý môže mať významný vplyv na schopnosť externého poskytovateľa IKT služieb účinne vykonávať kritické alebo dôležité funkcie v súlade s dohodnutými úrovňami služieb;

f) povinnosť externého poskytovateľa IKT služieb poskytnúť pomoc v prípade incidentu súvisiaceho s IKT bez toho, aby vznikli dodatočné náklady, alebo aby vznikli len náklady, ktoré boli stanovené *ex ante*;

g) požiadavky na externého poskytovateľa IKT služieb na vykonávanie a testovanie obchodných krízových plánov a na zavedenie bezpečnostných opatrení, nástrojov a politík v oblasti IKT, ktoré primerane zaručujú bezpečné poskytovanie služieb finančným subjektom v súlade s jeho regulačným rámcom;

h) právo priebežne monitorovať výkonnosť externého poskytovateľa IKT služieb, ktoré zahŕňa:

i) práva na prístup, kontrolu a audit vykonávané finančným subjektom alebo vymenovanou treťou stranou, ako aj právo vyhotovovať kópie príslušnej dokumentácie, ktorého účinnému vykonávaniu nebránia ani ho neobmedzujú iné zmluvné dojednania alebo vykonávacie politiky;

ii) právo dohodnúť sa na alternatívnych úrovniach zabezpečenia, ak sú dotknuté práva iných klientov;

iii) záväzok plne spolupracovať počas kontrol na mieste vykonávaných finančným subjektom a podrobnosti o rozsahu, spôsoboch a frekvencii auditov na diaľku;

i) povinnosť externého poskytovateľa IKT služieb plne spolupracovať s príslušnými orgánmi a orgánmi pre riešenie krízových situácií finančného subjektu vrátane osôb nimi vymenovaných;

j) práva na ukončenie zmluvy a súvisiacu minimálnu výpovednú lehotu na ukončenie zmluvy v súlade s očakávaniami príslušných orgánov;

k) stratégie ukončenia angažovanosti, najmä zavedenie primeraného povinného prechodného obdobia:

a) počas ktorého bude externý poskytovateľ IKT služieb naďalej poskytovať príslušné funkcie alebo služby s cieľom znížiť riziko narušení na úrovni finančného subjektu;

b) ktoré umožňuje finančnému subjektu prejsť na iného externého poskytovateľa IKT služieb alebo začať využívať lokálne riešenia v prevádzkových priestoroch v závislosti od zložitosti poskytovanej služby.

3. Pri rokovaniach o zmluvných dojednaniach finančné subjekty a externí poskytovatelia IKT služieb zvážia použitie štandardných zmluvných doložiek vypracovaných pre konkrétne služby.

4. Európske orgány dohľadu vypracujú prostredníctvom spoločného výboru návrh regulačných technických predpisov na bližšie spresnenie prvkov, ktoré finančný subjekt musí určiť a posúdiť, keď zadáva kritické alebo dôležité funkcie subdodávateľovi, s cieľom náležite uplatniť ustanovenia odseku 2 písm. a).

Európske orgány dohľadu predložia tento návrh regulačných technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v prvom pododseku v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010.

ODDIEL II

RÁMEC DOZORU NAD EXTERNÝMI POSKYTOVATEĽMI KRITICKÝCH IKT SLUŽIEB

Článok 28

Určenie externých poskytovateľov kritických IKT služieb

1. Európske orgány dohľadu prostredníctvom spoločného výboru a na základe odporúčania fóra pre dozor zriadeného podľa článku 29 ods. 1:

a) určia externých poskytovateľov IKT služieb, ktorí sú pre finančné subjekty kritické, pričom zohľadnia kritériá uvedené v odseku 2;

b) určia buď orgány EBA, ESMA alebo EIOPA za hlavný orgán dozoru pre každého externého poskytovateľa kritických IKT služieb, a to v závislosti od toho, či celková hodnota aktív finančných subjektov využívajúcich služby

tohto externého poskytovateľa kritických IKT služieb, na ktorého sa vzťahuje jedno z nariadení (EÚ) č. 1093/2010 (EÚ), č. 1094/2010 alebo (EÚ) č. 1095/2010, predstavuje viac ako polovicu hodnoty celkových aktív všetkých finančných subjektov využívajúcich služby externého poskytovateľa kritických IKT služieb, ako je vykázané v konsolidovaných súvahách alebo v individuálnych súvahách, ak súvahy nie sú konsolidované, uvedených finančných subjektov.

2. Určenie uvedené v odseku 1 písm. a) musí vychádzať zo všetkých týchto kritérií:

a) systémový vplyv na stabilitu, kontinuitu alebo kvalitu poskytovania finančných služieb, ak by príslušný externý poskytovateľ IKT služieb čelil rozsiahlemu prevádzkovému zlyhaniu svojich služieb, so zohľadnením počtu finančných subjektov, ktorým príslušný externý poskytovateľ IKT služieb poskytuje služby;

b) systémový charakter alebo význam finančných subjektov, ktoré závisia od príslušného externého poskytovateľa IKT služieb, posudzovaný v súlade s týmito parametrami:

i) počet globálne systémovo významných inštitúcií (G-SII) alebo inak systémovo významných inštitúcií (O-SII), ktoré závisia od príslušného externého poskytovateľa IKT služieb;

ii) vzájomná závislosť medzi G-SII alebo O-SII uvedených v bode i) a inými finančnými subjektmi vrátane situácií, keď G-SII alebo O-SII poskytujú služby finančnej infraštruktúry iným finančným subjektom;

c) závislosť finančných subjektov od služieb, ktoré poskytuje príslušný externý poskytovateľ IKT služieb v súvislosti s kritickými alebo dôležitými funkciami finančných subjektov, ktoré v konečnom dôsledku zahŕňajú toho istého externého poskytovateľa IKT služieb, a to bez ohľadu na to, či finančné subjekty závisia od uvedených služieb priamo alebo nepriamo alebo prostredníctvom subdodávateľských dohôd;

d) stupeň nahraditeľnosti externého poskytovateľa IKT služieb pri zohľadnení týchto parametrov:

i) neexistencia skutočných, aj čiastočných, alternatív z dôvodu obmedzeného počtu externých poskytovateľov IKT služieb na konkrétnom trhu, alebo trhový podiel príslušného externého poskytovateľa IKT služieb, alebo súvisiaca technická zložitosť či prepracovanosť, a to aj vo vzťahu k akejkoľvek proprietárnej technológii, alebo osobitosti organizácie alebo činnosti daného externého poskytovateľa IKT služieb;

ii) ťažkosti s čiastočným alebo úplným presunom príslušných údajov a pracovným zaťažením príslušného externého poskytovateľa IKT služieb na iného externého poskytovateľa IKT služieb, a to buď z dôvodu značných finančných nákladov, času alebo iného druhu zdrojov, ktoré môže takýto presun predstavovať, alebo z dôvodu zvýšených IKT rizík alebo iných prevádzkových rizík, ktorým môže byť finančný subjekt vystavený pri takomto presune;

e) počet členských štátov, v ktorých príslušný externý poskytovateľ IKT služieb poskytuje služby;

f) počet členských štátov, v ktorých finančné subjekty využívajúce služby príslušného externého poskytovateľa IKT služieb pôsobia.

3. Komisia je splnomocnená prijímať delegované akty v súlade s článkom 50 s cieľom doplniť kritériá uvedené v odseku 2.

4. Mechanizmus určovania uvedený v odseku 1 písm. a) sa nepoužije dovtedy, kým Komisia neprijme delegovaný akt v súlade s odsekom 3.

5. Mechanizmus určovania uvedený v odseku 1 písm. a) sa neuplatňuje v súvislosti s externými poskytovateľmi IKT služieb, ktorí podliehajú rámcom dozoru zriadeným na účely podpory úloh uvedených v článku 127 ods. 2 Zmluvy o fungovaní Európskej únie.

6. Európske orgány dohľadu prostredníctvom spoločného výboru vypracujú, uverejnia a každoročne aktualizujú zoznam externých poskytovateľov kritických IKT služieb na úrovni Únie.

7. Na účely odseku 1 písm. a) príslušné orgány každoročne a súhrnne zasielajú správy uvedené v článku 25 ods. 4 fóru pre dozor zriadenému podľa článku 29. Fórum pre dozor posudzuje závislosť IKT finančných subjektov od tretej strany na základe informácií získaných od príslušných orgánov.

8. Externí poskytovatelia IKT služieb, ktorí nie sú zahrnutí v zozname uvedenom v odseku 6, môžu požiadať o zaradenie do tohto zoznamu.

Na účely prvého pododseku externý poskytovateľ IKT služieb predloží odôvodnenú žiadosť orgánom EBA, ESMA alebo EIOPA, ktoré prostredníctvom spoločného výboru rozhodnú o tom, či zaradiť tohto externého poskytovateľa IKT služieb do uvedeného zoznamu v súlade s odsekom 1 písm. a).

Rozhodnutie uvedené v druhom pododseku sa prijme a oznámi externému poskytovateľovi IKT služieb do šiestich mesiacov od prijatia žiadosti.

9. Finančné subjekty nesmú využívať externého poskytovateľa IKT služieb usadeného v tretej krajine, ktorý by bol označený za kritického podľa odseku 1 písm. a), ak by bol usadený v Únii.

Článok 29

Štruktúra rámca dozoru

1. Spoločný výbor v súlade s článkom 57 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 zriadi fórum pre dozor ako podvýbor na účely podpory práce spoločného výboru a hlavného orgánu dozoru uvedeného v článku 28 ods. 1 písm. b) v oblasti IKT rizika tretej strany vo všetkých finančných sektoroch. Fórum pre dozor pripravuje návrhy spoločných pozícií a spoločných aktov spoločného výboru v tejto oblasti.

Fórum pre dozor pravidelne rokuje o relevantnom vývoji v oblasti IKT rizík a zraniteľností a podporuje konzistentný prístup pri monitorovaní IKT rizika tretej strany na úrovni Únie.

2. Fórum pre dozor vykonáva každoročne kolektívne posudzovanie výsledkov a zistení činností dozoru vykonávaných v prípade všetkých externých poskytovateľov kritických IKT služieb a podporuje koordinačné opatrenia s cieľom zvýšiť digitálnu prevádzkovú odolnosť finančných subjektov, podporovať najlepšie postupy týkajúce

sa riešenia rizika koncentrácie IKT a skúmať zmierňujúce faktory v prípade medzisektorových presunov rizika.

3. Fórum pre dozor predkladá komplexné referenčné hodnoty externých poskytovateľov kritických IKT služieb, ktoré má spoločný výbor prijať ako spoločné pozície európskych orgánov dohľadu v súlade s článkom 56 ods. 1 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

4. Fórum pre dozor tvoria predsedovia európskych orgánov dohľadu a jeden zástupca na vysokej úrovni zo súčasných zamestnancov relevantného príslušného orgánu z každého členského štátu. Na práci fóra pre dozor sa ako pozorovatelia zúčastňujú výkonní riaditelia každého európskeho orgánu dohľadu a jeden zástupca Európskej komisie, výboru ESRB, ECB a agentúry ENISA.

5. V súlade s článkom 16 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 európske orgány dohľadu vydajú usmernenia o spolupráci medzi európskymi orgánmi dohľadu a príslušnými orgánmi na účely tohto oddielu týkajúce sa podrobných postupov a podmienok v súvislosti s vykonávaním úloh medzi príslušnými orgánmi a európskymi orgánmi dohľadu, ako aj podrobností o výmene informácií potrebných na to, aby príslušné orgány zabezpečili kroky nadväzujúce na odporúčania adresované hlavnými orgánmi dozoru podľa článku 31 ods. 1 písm. d) externým poskytovateľom kritických IKT služieb.

6. Požiadavkami stanovenými v tomto oddiele nie je dotknuté uplatňovanie smernice (EÚ) 2016/1148 ani iných pravidiel Únie o dozore, ktoré sa vzťahujú na poskytovateľov v oblasti služieb cloud computingu.

7. Európske orgány dohľadu prostredníctvom spoločného výboru a na základe prípravnej práce vykonanej fórom pre dozor každoročne predkladajú Európskemu parlamentu, Rade a Komisii správu o uplatňovaní tohto oddielu.

Článok 30

Úlohy hlavného orgánu dozoru

1. Hlavný orgán dozoru posudzuje, či každý externý poskytovateľ kritických IKT služieb zaviedol komplexné, riadne a účinné pravidlá, postupy, mechanizmy a opatrenia na riadenie IKT rizika, ktoré externý poskytovateľ kritických IKT služieb môže predstavovať pre finančné subjekty.

2. Posúdenie uvedené v odseku 1 zahŕňa:

   a) požiadavky na IKT s cieľom zaistiť najmä bezpečnosť, dostupnosť, kontinuitu, škálovateľnosť a kvalitu služieb, ktoré externý poskytovateľ kritických IKT služieb poskytuje finančným subjektom, ako aj schopnosť neustále zachovávať vysokú úroveň bezpečnosti, dôvernosti a integrity údajov;

   b) fyzickú bezpečnosť prispievajúcu k zaisteniu bezpečnosti IKT vrátane bezpečnosti priestorov, zariadení a dátových centier;

   c) procesy riadenia rizika vrátane politík riadenia IKT rizika, kontinuity činností v oblasti IKT a plánov obnovy po havárii v oblasti IKT;

   d) mechanizmy správy a riadenia vrátane organizačnej štruktúry s jasnými, transparentnými a konzistentnými líniami zodpovednosti a pravidlami zodpovednosti umožňujúcimi účinné riadenie IKT rizika;

e) identifikáciu, monitorovanie a okamžité nahlasovanie incidentov súvisiacich s IKT finančným subjektom, riadenie a riešenie týchto incidentov, najmä kybernetických útokov;

f) mechanizmy prenosnosti údajov, prenosnosti a interoperability aplikácií, ktoré zabezpečujú účinný výkon práv na ukončenie zmluvy finančnými subjektmi;

g) testovanie IKT systémov, infraštruktúry a kontrol;

h) audity IKT;

i) používanie príslušných vnútroštátnych a medzinárodných noriem uplatniteľných na poskytovanie IKT služieb externého poskytovateľa kritických IKT služieb finančným subjektom.

3. Vychádzajúc z posúdenia uvedeného v odseku 1 hlavný orgán dozoru prijme jasný, podrobný a odôvodnený individuálny plán dozoru v prípade každého externého poskytovateľa kritických IKT služieb. Tento plán sa každoročne oznamuje externému poskytovateľovi kritických IKT služieb.

4. Keď sa ročné plány dozoru uvedené v odseku 3 dohodnú a oznámia externým poskytovateľom kritických IKT služieb, príslušné orgány môžu prijať opatrenia týkajúce sa externých poskytovateľov kritických IKT služieb len po dohode s hlavným orgánom dozoru.

Článok 31

Právomoci hlavného orgánu dozoru

1. Hlavný orgán dozoru má na účely plnenia povinností stanovených v tomto oddiele tieto právomoci:

a) požadovať všetky relevantné informácie a dokumentáciu v súlade s článkom 32;

b) vykonávať všeobecné vyšetrovania a kontroly v súlade s článkami 33 a 34;

c) žiadať o správy po ukončení činností dozoru, v ktorých sa bližšie spresnia prijaté opatrenia alebo nápravné opatrenia vykonané externými poskytovateľmi kritických IKT služieb v súvislosti s odporúčaniami uvedenými v písmene d) tohto odseku;

d) adresovať odporúčania týkajúce sa oblastí uvedených v článku 30 ods. 2, najmä pokiaľ ide o:

i) používanie osobitných požiadaviek alebo postupov v oblasti bezpečnosti a kvality IKT, najmä v súvislosti so zavádzaním opráv, aktualizácií, šifrovania a iných bezpečnostných opatrení, ktoré hlavný orgán dozoru považuje za dôležité na zaistenie bezpečnosti IKT služieb poskytovaných finančným subjektom;

ii) uplatňovanie podmienok vrátane ich technického vykonávania, na základe ktorých externí poskytovatelia kritických IKT služieb poskytujú služby finančným subjektom, ktoré hlavný orgán dozoru považuje za dôležité na zabránenie vytvoreniu jednotlivých miest zlyhania alebo ich rozšírenie, alebo na minimalizovanie možného systémového vplyvu v celom finančnom sektore Únie v prípade rizika koncentrácie IKT;

iii) po preskúmaní subdodávateľských dohôd vykonanom v súlade s článkami 32 a 33 vrátane dohôd o sub-outsorcingu, ktoré externí poskytovatelia kritických IKT služieb plánujú vykonať spolu s inými externými poskytovateľmi IKT služieb alebo so subdodávateľmi IKT usadenými v tretej krajine, akékoľvek plánované zadávanie zákaziek subdodávateľom vrátane sub-outsorcingu, ak sa hlavný orgán dozoru domnieva, že ďalšie zadávanie zákaziek subdodávateľom môže vyvolať riziká pre poskytovanie služieb finančným subjektom alebo riziká pre finančnú stabilitu;

iv) odstúpenie od uzatvorenia ďalších subdodávateľských dohôd, ak sú splnené tieto kumulatívne podmienky:

– plánovaný subdodávateľ je externým poskytovateľom IKT služieb alebo subdodávateľom IKT usadeným v tretej krajine;

– zadávanie zákaziek subdodávateľom sa týka kritickej alebo dôležitej funkcie finančného subjektu.

2. Hlavný orgán dozoru konzultuje fórum pre dozor pred vykonávaním právomocí uvedených v odseku 1.

3. Externí poskytovatelia kritických IKT služieb spolupracujú v dobrej viere s hlavným orgánom dozoru a pomáhajú hlavnému orgánu dozoru pri plnení jeho úloh.

4. Hlavný orgán dozoru môže uložiť pravidelnú platbu penále s cieľom prinútiť externého poskytovateľa kritických IKT služieb, aby dodržiaval ustanovenia odseku 1 písm. a), b) a c).

5. Pravidelná platba penále uvedená v odseku 4 sa ukladá za každý deň až do dosiahnutia súladu a nie dlhšie ako šesť mesiacov po oznámení externému poskytovateľovi kritických IKT služieb.

6. Výška pravidelnej platby penále vypočítaná od dátumu stanoveného v rozhodnutí, ktorým sa ukladá pravidelná platba penále, predstavuje 1 % priemerného denného celosvetového obratu externého poskytovateľa kritických IKT služieb v predchádzajúcom finančnom roku.

7. Platba penále je administratívnej povahy a je vymáhateľná. Vymáhanie sa riadi platnými predpismi občianskeho práva procesného toho členského štátu, na území ktorého sa kontroly a prístup uskutočňujú. Súdy dotknutého členského štátu majú právomoc rozhodovať o sťažnostiach týkajúcich sa protiprávneho výkonu vymáhania. Platby penále sa odvádzajú do všeobecného rozpočtu Európskej únie.

8. Európske orgány dohľadu zverejňujú všetky pravidelné platby penále, ktoré boli uložené, pokiaľ by ich zverejnenie vážne neohrozilo finančné trhy alebo nespôsobilo neprimeranú škodu zúčastneným stranám.

9. Pred uložením pravidelnej platby penále podľa odseku 4 hlavný orgán dozoru poskytne zástupcom externého poskytovateľa kritických IKT služieb, voči ktorému sa vedie konanie, príležitosť vyjadriť sa k zisteniam a pri svojich rozhodnutiach vychádza len zo zistení, ku ktorým mal externý poskytovateľ kritických IKT služieb, voči ktorému sa vedie konanie, možnosť vyjadriť sa. Právo na obhajobu osôb, voči ktorým sa vedie konanie, sa počas konania plne rešpektuje. Majú právo na prístup k spisu s výhradou oprávnených záujmov iných osôb na ochranu ich obchodného tajomstva. Právo na prístup k spisu sa nevzťahuje na dôverné informácie alebo interné prípravné dokumenty hlavného orgánu dozoru.

Článok 32

Žiadosť o informácie

1. Hlavný orgán dozoru môže jednoduchou žiadosťou alebo rozhodnutím požadovať od externých poskytovateľov kritických IKT služieb, aby poskytli všetky informácie, ktoré hlavný orgán dozoru potrebuje na vykonávanie svojich povinností podľa tohto nariadenia, vrátane všetkých príslušných obchodných alebo prevádzkových dokumentov, zmlúv, dokumentácie o politikách, auditorských správ o bezpečnosti IKT, správ o incidentoch súvisiacich s IKT, ako aj akýchkoľvek informácií týkajúcich sa strán, prostredníctvom ktorých externý poskytovateľ kritických IKT služieb externe zabezpečuje prevádzkové funkcie alebo činnosti.

2. Pri zasielaní jednoduchej žiadosti o informácie podľa odseku 1 hlavný orgán dozoru:

   a) uvedie odkaz na tento článok ako právny základ žiadosti;

   b) uvedie dôvod žiadosti;

   c) uvedie, ktoré informácie žiada;

   d) stanoví lehotu na poskytnutie informácií;

   e) informuje zástupcu externého poskytovateľa kritických IKT služieb, od ktorého požaduje informácie, že nie je povinný tieto informácie poskytnúť, ale ak na žiadosť dobrovoľne odpovie, poskytnuté informácie nesmú byť nesprávne alebo zavádzajúce.

3. Pri žiadosti o poskytnutie informácií podľa odseku 1 hlavný orgán dozoru:

   a) uvedie odkaz na tento článok ako právny základ žiadosti;

   b) uvedie dôvod žiadosti;

   c) uvedie, ktoré informácie žiada;

   d) stanoví lehotu na poskytnutie informácií;

   e) upozorní na pravidelné platby penále stanovené v článku 31 ods. 4 za poskytnutie neúplných požadovaných informácií;

   f) upozorní na právo odvolať sa voči rozhodnutiu na odvolaciu radu európskeho orgánu dohľadu a na právo žiadať o preskúmanie rozhodnutia Súdnym dvorom Európskej únie (ďalej len „Súdny dvor“) v súlade s článkami 60 a 61 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

4. Zástupcovia externého poskytovateľa kritických IKT služieb poskytujú požadované informácie. Riadne splnomocnení právnici môžu poskytovať informácie v mene svojich klientov. Za poskytnutie neúplných, nesprávnych alebo zavádzajúcich informácií ostávajú plne zodpovední externí poskytovatelia kritických IKT služieb.

5. Hlavný orgán dozoru bezodkladne zašle kópiu rozhodnutia o poskytnutí informácií príslušným orgánom finančných subjektov, ktoré využívajú služby externých poskytovateľov kritických IKT služieb.

Článok 33

Všeobecné vyšetrovania

1. Hlavný orgán dozoru, ktorému pomáha prieskumný tím uvedený v článku 34 ods. 1, môže na účely plnenia svojich povinností podľa tohto nariadenia vykonávať potrebné vyšetrovania externých poskytovateľov IKT služieb.

2. Hlavný orgán dozoru je oprávnený:

a) preskúmavať záznamy, údaje, postupy a akékoľvek iné materiály vzťahujúce sa na plnenie ich úloh bez ohľadu na médium, na ktorom sú uložené;

b) robiť alebo získavať overené kópie alebo výpisy z týchto záznamov, údajov, postupov a iných materiálov;

c) predvolávať zástupcov externého poskytovateľa IKT služieb, aby podali ústne alebo písomné vysvetlenie k skutočnostiam alebo dokumentom týkajúcim sa predmetu a dôvodu vyšetrovania, a zaznamenávať odpovede;

d) vypočuť akúkoľvek inú fyzickú alebo právnickú osobu, ktorá s týmto vypočutím súhlasí, s cieľom zhromaždiť informácie týkajúce sa predmetu vyšetrovania;

e) žiadať záznamy telefonickej a dátovej prevádzky.

3. Úradníci a iné osoby poverené hlavným orgánom dozoru na účely vyšetrovania uvedeného v odseku 1 vykonávajú svoje právomoci na základe písomného poverenia, v ktorom je uvedený predmet a dôvod vyšetrovania.

V uvedenom poverení sa takisto upozorní na pravidelné platby penále stanovené v článku 31 ods. 4, ak zástupcovia externého poskytovateľa IKT služieb neposkytli alebo poskytli len neúplné požadované záznamy, údaje, postupy alebo akékoľvek iné materiály či odpovede na položené otázky.

4. Zástupcovia externých poskytovateľov IKT služieb sú povinní podrobiť sa vyšetrovaniu na základe rozhodnutia hlavného orgánu dozoru. V rozhodnutí sa uvádza predmet a dôvod vyšetrovania, pravidelné platby penále stanovené v článku 31 ods. 4, opravné prostriedky dostupné na základe nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010, ako aj právo požiadať o preskúmanie rozhodnutia Súdnym dvorom.

5. Hlavný orgán dozoru informuje príslušné orgány finančných subjektov, ktoré využívajú služby externého poskytovateľa IKT služieb, o vyšetrovaní a o totožnosti poverených osôb, a to v primeranom čase pred vyšetrovaním.

Článok 34
Kontroly na mieste

1. Na účely vykonávania svojich povinností podľa tohto nariadenia môže hlavný orgán dozoru za pomoci prieskumných tímov uvedených v článku 35 ods. 1 vykonávať všetky potrebné kontroly na mieste a vstupovať do akýchkoľvek obchodných priestorov, na pozemky alebo majetok externých poskytovateľov IKT služieb, ako sú napríklad ústredia, prevádzkové strediská, vedľajšie priestory, ako aj vykonávať kontroly mimo internetu, a vykonávať všetky potrebné kontroly mimo miesta.

2. Úradníci a iné osoby poverené hlavným orgánom dozoru vykonávať kontroly na mieste môžu vstúpiť do všetkých takýchto obchodných priestorov, na pozemky alebo majetok a majú všetky právomoci zapečatiť všetky obchodné priestory a účtovné knihy alebo záznamy počas obdobia kontroly a v potrebnom rozsahu.

Svoje právomoci vykonávajú na základe písomného poverenia, v ktorom sa uvádza predmet a dôvod kontroly a pravidelné platby penále stanovené v článku 31 ods. 4, ak sa zástupcovia dotknutých externých poskytovateľov IKT služieb nepodrobia kontrole.

3. Hlavný orgán dozoru informuje príslušné orgány finančných subjektov, ktoré využívajú služby externého poskytovateľa IKT služieb, v primeranom čase pred kontrolou.

4. Kontroly sa vzťahujú na celú škálu príslušných IKT systémov, sietí, zariadení, informácií a údajov, ktoré sa používajú na poskytovanie služieb finančným subjektom alebo k nemu prispievajú.

5. Pred každou plánovanou návštevou na mieste hlavný orgán dozoru primerane informuje externých poskytovateľov kritických IKT služieb s výnimkou prípadu, keď takéto oznámenie nie je možné z dôvodu núdzovej alebo krízovej situácie, alebo ak by to viedlo k situácii, keď by kontrola alebo audit už neboli účinné.

6. Externý poskytovateľ kritických IKT služieb sa podrobí kontrolám na mieste nariadeným na základe rozhodnutia hlavného orgánu dozoru. V rozhodnutí sa uvádza predmet a dôvod kontroly, stanoví sa v ňom dátum jej začatia a upozorní sa na pravidelné platby penále stanovené v článku 31 ods. 4, opravné prostriedky dostupné na základe nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010, ako aj na právo požiadať o preskúmanie rozhodnutia Súdnym dvorom.

7. Ak úradníci a iné osoby poverené hlavným orgánom dozoru zistia, že externý poskytovateľ kritických IKT služieb sa bráni kontrole nariadenej podľa tohto článku, hlavný orgán dozoru informuje externého poskytovateľa kritických IKT služieb o dôsledkoch takéhoto správania vrátane možnosti, aby príslušné orgány príslušných finančných subjektov ukončili zmluvné dojednania uzavreté s týmto externým poskytovateľom kritických IKT služieb.

Článok 35
Priebežný dozor

1. Pri vykonávaní všeobecných vyšetrovaní alebo kontrol na mieste hlavným orgánom dozoru pomáha prieskumný tím zriadený pre každého externého poskytovateľa kritických IKT služieb.

2. Spoločný prieskumný tím uvedený v odseku 1 tvoria zamestnanci hlavného orgánu dozoru a dotknutých príslušných orgánov vykonávajúcich dohľad nad finančnými subjektmi, ktorým externý poskytovateľ kritických IKT služieb poskytuje služby, pričom do prípravy a vykonávania činností dozoru je zapojených a vykonáva ich maximálne 10 členov spoločného prieskumného tímu. Všetci členovia spoločného prieskumného tímu musia mať odborné znalosti v oblasti IKT rizika a prevádzkového rizika. Prácu spoločného prieskumného tímu koordinuje určený zamestnanec európskeho orgánu dohľadu (ďalej len „koordinátor hlavného orgánu dozoru“).

3. Európske orgány dohľadu prostredníctvom spoločného výboru vypracujú spoločný návrh regulačných technických predpisov s cieľom bližšie spresniť vymenúvanie členov spoločného prieskumného tímu pochádzajúcich z relevantných príslušných orgánov, ako aj úlohy a pracovné podmienky prieskumného tímu. Európske orgány dohľadu predložia tento návrh regulačných technických predpisov Komisii do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc prijať regulačné technické predpisy uvedené v prvom pododseku v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

4. Hlavný orgán dozoru po konzultácii s fórom pre dozor prijme do troch mesiacov od ukončenia vyšetrovania alebo kontroly na mieste odporúčania, ktoré má hlavný orgán dozoru adresovať externému poskytovateľovi kritických IKT služieb v súlade s právomocami uvedenými v článku 31.

5. Odporúčania uvedené v odseku 4 sa okamžite oznámia externému poskytovateľovi kritických IKT služieb a príslušným orgánom finančných subjektov, ktorým tento externý poskytovateľ kritických IKT služieb poskytuje služby.

Hlavný orgán dozoru môže na účely plnenia činností dozoru zohľadniť akékoľvek príslušné certifikácie tretej strany a správy o internom alebo externom audite IKT tretej strany, ktoré sprístupnil externý poskytovateľ kritických IKT služieb.

Článok 36

Harmonizácia podmienok umožňujúcich vykonávanie dozoru

1. Európske orgány dohľadu vypracujú prostredníctvom spoločného výboru návrh regulačných technických predpisov s cieľom bližšie spresniť:

a) informácie, ktoré má poskytnúť externý poskytovateľ kritických IKT služieb v žiadosti o dobrovoľné zapojenie do rámca dozoru, ako sa stanovuje v článku 28 ods. 8;

b) obsah a formát správ, ktoré sa môžu požadovať na účely článku 31 ods. 1 písm. c);

c) predkladanie informácií vrátane štruktúry, formátov a metód, ktoré sa vyžadujú, aby ich externý poskytovateľ kritických IKT služieb predložil, zverejnil alebo nahlasoval podľa článku 31 ods. 1;

d) podrobnosti o tom, ako príslušné orgány posudzujú opatrenia prijaté externými poskytovateľmi kritických IKT služieb na základe odporúčaní hlavných orgánov dozoru podľa článku 37 ods. 2.

2. Európske orgány dohľadu predložia tento návrh regulačných technických predpisov Komisii do 1. januára 20xx [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*].

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v prvom pododseku v súlade postupmi stanovenými v článkoch 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

Článok 37

Následné opatrenia príslušných orgánov

1. Do 30 kalendárnych dní od prijatia odporúčaní vydaných hlavnými orgánmi dozoru podľa článku 31 ods. 1 písm. d) externí poskytovatelia kritických IKT služieb oznámia hlavnému orgánu dozoru, či majú v úmysle postupovať podľa týchto odporúčaní. Hlavné orgány dozoru okamžite postúpia tieto informácie príslušným orgánom.

2. Príslušné orgány monitorujú, či finančné subjekty zohľadňujú riziká identifikované v odporúčaniach, ktoré hlavný orgán dozoru adresoval externým poskytovateľom kritických IKT služieb v súlade s článkom 31 ods. 1 písm. d).

3. Príslušné orgány môžu v súlade s článkom 44 požadovať od finančných subjektov, aby čiastočne alebo úplne dočasne pozastavili používanie alebo zavádzanie služby poskytovanej externým poskytovateľom kritických IKT služieb, a to dovtedy, pokiaľ sa nevyriešia riziká identifikované v odporúčaniach adresovaných externým poskytovateľom kritických IKT služieb. Príslušné orgány môžu v prípade potreby od finančných subjektov požadovať, aby čiastočne alebo úplne ukončili príslušné zmluvné dojednania uzavreté s externými poskytovateľmi kritických IKT služieb.

4. Pri prijímaní rozhodnutí uvedených v odseku 3 príslušné orgány zohľadňujú druh a rozsah rizika, ktoré externý poskytovateľ kritických IKT služieb nerieši, ako aj závažnosť nedodržiavania odporúčaní, a to so zreteľom na tieto kritériá:

   a) závažnosť a trvanie nedodržiavania odporúčaní;

   b) či sa nedodržiavaním odporúčaní odhalili závažné nedostatky v postupoch, systémoch riadenia, riadení rizík a vnútorných kontrolách externého poskytovateľa kritických IKT služieb;

   c) či sa uľahčilo alebo umožnilo spáchanie finančného trestného činu alebo či tento trestný čin možno inak pripísať nedodržiavaniu odporúčaní;

   d) či k nedodržiavaniu odporúčaní došlo úmyselne alebo z nedbanlivosti.

5. Príslušné orgány pravidelne informujú hlavné orgány dozoru o prístupoch a opatreniach prijatých v rámci ich úloh dohľadu vo vzťahu k finančným subjektom, ako aj o zmluvných opatreniach prijatých týmito finančnými subjektmi, ak externý poskytovateľ kritických IKT služieb čiastočne alebo úplne nesplnil odporúčania hlavných orgánov dozoru.

Článok 38
Poplatky za dozor

1. Európske orgány dohľadu účtujú externým poskytovateľom kritických IKT služieb poplatky, ktoré v plnej miere pokrývajú potrebné výdavky európskych orgánov dohľadu v súvislosti s vykonávaním úloh dozoru podľa tohto nariadenia, vrátane úhrady všetkých nákladov, ktoré môžu vzniknúť v dôsledku práce vykonanej príslušnými orgánmi zapojenými do činností dozoru v súlade s článkom 35.

   Výška poplatku účtovaného externému poskytovateľovi kritických IKT služieb pokrýva všetky administratívne náklady a je úmerná jeho obratu.

2. Komisia je splnomocnená prijať delegovaný akt v súlade s článkom 50 s cieľom doplniť toto nariadenie určením výšky poplatkov a spôsobu ich úhrady.

Článok 39
Medzinárodná spolupráca

1. Orgány EBA, ESMA a EIOPA môžu v súlade s článkom 33 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 uzatvárať administratívne dojednania s regulačnými orgánmi a orgánmi dohľadu tretích krajín s cieľom posilniť medzinárodnú spoluprácu v oblasti IKT rizika tretej strany v rôznych finančných

sektoroch, a to najmä vypracovaním najlepších postupov na preskúmanie postupov a kontrol riadenia IKT rizika, zmierňujúcich opatrení a reakcií na incidenty.

2. Európske orgány dohľadu predkladajú prostredníctvom spoločného výboru každých päť rokov Európskemu parlamentu, Rade a Komisii spoločnú dôvernú správu, v ktorej zhrnú zistenia príslušných diskusií s orgánmi tretích krajín uvedenými v odseku 1, pričom sa zamerajú na vývoj IKT rizika tretej strany a dôsledky pre finančnú stabilitu, integritu trhu, ochranu investorov alebo fungovanie jednotného trhu.

KAPITOLA VI

DOJEDNANIA O VÝMENE INFORMÁCIÍ

Článok 40

Dojednania o výmene informácií týkajúce informácií a spravodajských informácií o kybernetických hrozbách

1. Finančné subjekty si môžu medzi sebou vymieňať informácie a spravodajské informácie o kybernetických hrozbách vrátane ukazovateľov ohrozenia, taktík, techník a postupov, kybernetických bezpečnostných varovaní a konfiguračných nástrojov v takom rozsahu, aby sa takáto výmena informácií a spravodajských informácií:

   a) zameriavala na posilňovanie digitálnej prevádzkovej odolnosti finančných subjektov, najmä zvyšovaním informovanosti o kybernetických hrozbách, obmedzovaním alebo zabránením schopnosti šírenia kybernetických hrozieb, podporou škály obranných spôsobilostí finančných subjektov, techník odhaľovania hrozieb, stratégií zmierňovania alebo fáz reakcie a obnovy;

   b) uskutočňovala v rámci dôveryhodných komunít finančných subjektov;

   c) vykonávala prostredníctvom dojednaní o výmene informácií, ktoré chránia potenciálne citlivú povahu vymieňaných informácií a ktoré sa riadia pravidlami správania pri plnom rešpektovaní obchodného tajomstva, ochrany osobných údajov[48] a usmernení pre politiku hospodárskej súťaže[49].

2. Na účely odseku 1 písm. c) sa v dojednaniach o výmene informácií vymedzia podmienky účasti a podľa vhodnosti sa v nich stanovia podrobnosti o zapojení verejných orgánov a rozsah, v ktorom sa tieto orgány môžu pridružiť k dojednaniam o výmene informácií, ako aj o prevádzkových prvkoch vrátane využívania špecializovaných platforiem IT.

3. Finančné subjekty oznámia príslušným orgánom svoju účasť na dojednaniach o výmene informácií uvedených v odseku 1 po potvrdení ich členstva alebo prípadne ukončení ich členstva, keď nadobudne účinnosť.

---

[48] V súlade s nariadením 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).

[49] Oznámenie Komisie – Usmernenia o uplatňovaní článku 101 Zmluvy o fungovaní Európskej únie na dohody o horizontálnej spolupráci (2011/C 11/01).

KAPITOLA VII

PRÍSLUŠNÉ ORGÁNY

Článok 41

Príslušné orgány

Bez toho, aby boli dotknuté ustanovenia týkajúce sa rámca dozoru pre externých poskytovateľov kritických IKT služieb uvedené v oddiele II kapitoly V tohto nariadenia, súlad s povinnosťami stanovenými v tomto nariadení zabezpečujú tieto príslušné orgány v súlade s právomocami udelenými príslušnými právnymi aktmi:

a) v prípade úverových inštitúcií: príslušný orgán určený v súlade s článkom 4 smernice 2013/36/EÚ bez toho, aby boli dotknuté osobitné úlohy, ktoré boli ECB udelené nariadením (EÚ) č. 1024/2013;

b) v prípade poskytovateľov platobných služieb: príslušný orgán určený v súlade s článkom 22 smernice (EÚ) 2015/2366;

c) v prípade inštitúcií pre elektronické platby: príslušný orgán určený v súlade s článkom 37 smernice 2009/110/ES;

d) v prípade investičných spoločností: príslušný orgán určený v súlade s článkom 4 smernice (EÚ) 2019/2034;

e) v prípade poskytovateľov služieb kryptoaktív, emitentov kryptoaktív, emitentov tokenov krytých aktívami a emitentov významných tokenov krytých aktívami: príslušný orgán určený v súlade s článkom 3 ods. 1 písm. ee) prvou zarážkou [*nariadenia (EÚ) 20xx MICA*];

f) v prípade centrálnych depozitárov cenných papierov: príslušný orgán určený v súlade s článkom 11 nariadenia (EÚ) č. 909/2014;

g) v prípade centrálnych protistrán: príslušný orgán určený v súlade s článkom 22 nariadenia (EÚ) č. 648/2012;

h) v prípade obchodných miest a poskytovateľov služieb nahlasovania údajov: príslušný orgán určený v súlade s článkom 67 smernice 2014/65/ES;

i) v prípade archívov obchodných údajov: príslušný orgán určený v súlade s článkom 55 nariadenia (EÚ) č. 648/2012;

j) v prípade správcov alternatívnych investičných fondov: príslušný orgán určený v súlade s článkom 44 smernice 2011/61/EÚ;

k) v prípade správcovských spoločností: príslušný orgán určený v súlade s článkom 97 smernice 2009/65/ES;

l) v prípade poisťovní a zaisťovní: príslušný orgán určený v súlade s článkom 30 smernice 2009/138/ES;

m) v prípade sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia: príslušný orgán určený v súlade s článkom 12 smernice (EÚ) 2016/97;

n) v prípade inštitúcií zamestnaneckého dôchodkového zabezpečenia: príslušný orgán určený v súlade s článkom 47 smernice (EÚ) 2016/2341;

o) v prípade ratingových agentúr: príslušný orgán určený v súlade s článkom 21 nariadenia (ES) č. 1060/2009;

p) v prípade štatutárnych audítorov a audítorských spoločností: príslušný orgán určený v súlade s článkom 3 ods. 2 a článkom 32 smernice 2006/43/ES;

q) v prípade správcov kritických referenčných hodnôt: príslušný orgán určený v súlade s článkami 40 a 41 *nariadenia xx/202x*;

r) v prípade poskytovateľov služieb kolektívneho financovania: príslušný orgán určený v súlade s *článkom x nariadenia xx/202x*;

s) v prípade archívov sekuritizačných údajov: príslušný orgán určený v súlade s článkom 10 a článkom 14 ods. 1 nariadenia (EÚ) 2017/2402.

Článok 42

Spolupráca so štruktúrami a orgánmi zriadenými smernicou (EÚ) 2016/1148

1. S cieľom podporiť spoluprácu a umožniť výmenu informácií v oblasti dohľadu medzi príslušnými orgánmi určenými podľa tohto nariadenia a skupinou pre spoluprácu zriadenou článkom 11 smernice (EÚ) 2016/1148 európske orgány dohľadu a príslušné orgány môžu požiadať, aby boli prizvané do činností skupiny pre spoluprácu.

2. Príslušné orgány môžu podľa vhodnosti vykonávať konzultácie s jednotným kontaktným miestom uvedeným v článku 8 smernice (EÚ) 2016/1148 a vnútroštátnymi jednotkami pre riešenie počítačových bezpečnostných incidentov uvedenými v článku 9 smernice (EÚ) 2016/1148.

Článok 43

Finančné medzisektorové cvičenia, komunikácia a spolupráca

1. Európske orgány dohľadu môžu prostredníctvom spoločného výboru a v spolupráci s príslušnými orgánmi, ECB a výborom ESRB vytvoriť mechanizmy, ktoré umožnia výmenu účinných postupov vo finančných sektoroch s cieľom zlepšiť situačnú informovanosť a identifikovať spoločné kybernetické zraniteľnosti a riziká naprieč sektormi.

   Môžu vypracovať cvičenia týkajúce sa krízového riadenia, ako aj krízových udalostí zahŕňajúce scenáre kybernetického útoku, aby sa vyvinuli komunikačné kanály a postupne umožnila účinná koordinovaná reakcia na úrovni EÚ v prípade závažného cezhraničného incidentu súvisiaceho s IKT alebo súvisiacej hrozby majúcej systémový vplyv na finančný sektor Únie ako celok.

   Týmito cvičeniami sa môžu v prípade potreby takisto testovať závislosti finančného sektora od ostatných hospodárskych odvetví.

2. Príslušné orgány, orgány EBA, ESMA alebo EIOPA, ako aj ECB navzájom úzko spolupracujú a vymieňajú si informácie na plnenie svojich povinností podľa článkov 42 až 48. Úzko koordinujú dohľad, ktorý vykonávajú, s cieľom identifikovať a odstrániť porušenia tohto nariadenia, rozvíjať a podporovať najlepšie postupy, uľahčovať spoluprácu, posilňovať jednotnosť výkladu a v prípade akýchkoľvek sporov vykonávať posúdenia na základe viacerých jurisdikcií.

Článok 44

Administratívne sankcie a nápravné opatrenia

1. Príslušné orgány musia mať všetky potrebné právomoci v oblasti dohľadu, vyšetrovania a ukladania sankcií na zabezpečenie uplatňovania tohto nariadenia.

2. Právomoci uvedené v odseku 1 zahŕňajú prinajmenšom právomoci:

   a) mať prístup ku každému dokumentu alebo údaju v akejkoľvek forme, ktorý príslušný orgán považuje za dôležitý pre výkon svojich úloh, a dostať alebo si urobiť jeho kópiu;

   b) vykonávať kontroly alebo vyšetrovania na mieste;

   c) požadovať nápravné a opravné opatrenia v prípade porušení požiadaviek tohto nariadenia.

3. Bez toho, aby bolo dotknuté právo členských štátov ukladať trestnoprávne sankcie podľa článku 46, členské štáty stanovia pravidlá, ktorými sa zavádzajú primerané administratívne sankcie a nápravné opatrenia za porušenia tohto nariadenia, a zabezpečia ich účinné vykonávanie.

   Tieto sankcie a opatrenia musia byť účinné, primerané a odrádzajúce.

4. Členské štáty udelia príslušným orgánom právomoc uplatňovať aspoň tieto administratívne sankcie alebo nápravné opatrenia za porušenia tohto nariadenia:

   a) vydať príkaz, ktorým sa od fyzickej alebo právnickej osoby požaduje, aby upustila od konania a zdržala sa opakovania tohto konania;

   b) požadovať dočasné alebo trvalé ukončenie uplatňovania akéhokoľvek postupu alebo správania, ktoré sú podľa príslušného orgánu v rozpore s ustanoveniami tohto nariadenia, a zabrániť opakovanému uplatneniu takéhoto postupu alebo správania;

   c) prijať akýkoľvek druh opatrenia vrátane opatrenia peňažnej povahy s cieľom zabezpečiť, aby finančné subjekty naďalej dodržiavali právne požiadavky;

   d) požadovať, ak to povoľuje vnútroštátne právo, existujúce záznamy o prenose údajov, ktoré má telekomunikačný operátor, ak existuje dôvodné podozrenie porušenia tohto nariadenia a ak takéto záznamy môžu byť relevantné pri vyšetrovaní porušení tohto nariadenia; a

   e) vydávať verejné oznámenia vrátane verejných vyhlásení, v ktorých sa uvádza totožnosť fyzickej alebo právnickej osoby a povaha porušenia.

5. Ak sa ustanovenia uvedené v odseku 2 písm. c) a v odseku 4 vzťahujú na právnické osoby, členské štáty udelia príslušným orgánom právomoc uplatňovať administratívne sankcie a nápravné opatrenia, s výhradou podmienok stanovených vo vnútroštátnom práve, voči členom riadiaceho orgánu a voči ďalším osobám, ktoré sú podľa vnútroštátneho práva zodpovedné za porušenie.

6. Členské štáty zabezpečia, aby každé rozhodnutie o uložení administratívnych sankcií alebo nápravných opatrení stanovených v odseku 2 písm. c) bolo riadne odôvodnené a podliehalo právu odvolať sa.

Článok 45

Výkon právomoci ukladať administratívne sankcie a nápravné opatrenia

1. Príslušné orgány vykonávajú právomoc ukladať administratívne sankcie a nápravné opatrenia uvedené v článku 44 v súlade so svojimi vnútroštátnymi právnymi rámcami, ak je to vhodné:

   a) priamo;

   b) v spolupráci s inými orgánmi;

   c) v rámci svojej zodpovednosti delegovaním na iné orgány;

   d) podaním žiadosti na príslušné súdne orgány.

2. Pri určovaní druhu a úrovne administratívnej sankcie alebo nápravného opatrenia, ktoré sa majú uložiť podľa článku 44, príslušné orgány zohľadňujú rozsah, v ktorom je porušenie úmyselné alebo vyplýva z nedbanlivosti, a všetky iné relevantné okolnosti, a to aj, ak je to relevantné:

   a) významnosť, závažnosť a trvanie porušenia;

   b) mieru zodpovednosti fyzickej alebo právnickej osoby, ktorá je zodpovedná za porušenie;

   c) finančnú silu zodpovednej fyzickej alebo právnickej osoby;

   d) rozsah ziskov, ktoré zodpovedná fyzická alebo právnická osoba dosiahla, alebo strát, ktorým zabránila, pokiaľ ich možno určiť;

   e) straty tretích strán spôsobené porušením, pokiaľ ich možno určiť;

   f) úroveň spolupráce zodpovednej fyzickej alebo právnickej osoby s príslušným orgánom bez toho, aby tým bola dotknutá potreba zabezpečiť vrátenie ziskov, ktoré táto osoba dosiahla, alebo strát, ktorým zabránila;

   g) predchádzajúce porušenia, ktorých sa dopustila zodpovedná fyzická alebo právnická osoba.

Článok 46

Trestnoprávne sankcie

1. Členské štáty sa môžu rozhodnúť, že nestanovia pravidlá týkajúce sa administratívnych sankcií alebo nápravných opatrení za porušenia, na ktoré sa podľa ich vnútroštátneho práva vzťahujú trestnoprávne sankcie.

2. Ak sa členské štáty rozhodli, že stanovia trestnoprávne sankcie za porušenia tohto nariadenia, zabezpečia zavedenie primeraných opatrení, aby príslušné orgány mali všetky právomoci potrebné na spoluprácu so súdnymi orgánmi, orgánmi prokuratúry alebo trestnoprávnymi orgánmi v rámci ich jurisdikcie na získanie konkrétnych informácií týkajúcich sa vyšetrovaní trestných činov alebo konaní začatých v prípade porušení tohto nariadenia a na poskytovanie rovnakých informácií ostatným príslušným orgánom, ako aj orgánom EBA, ESMA alebo EIOPA, aby si splnili povinnosť spolupracovať na účely tohto nariadenia.

Článok 47

Oznamovacie povinnosti

Členské štáty oznámia Komisii a orgánom ESMA, EBA a EIOPA zákony, iné právne predpisy a správne opatrenia na vykonávanie tejto kapitoly vrátane všetkých relevantných ustanovení trestného práva do [*Úrad pre publikácie: vložte dátum 1 rok po nadobudnutí účinnosti*]. Členské štáty oznámia Komisii a orgánom ESMA, EBA a EIOPA bez zbytočného odkladu akékoľvek ďalšie súvisiace zmeny.

Článok 48

Uverejnenie administratívnych sankcií

1. Príslušné orgány uverejnia na svojich úradných webových sídlach bez zbytočného odkladu každé rozhodnutie o uložení administratívnej sankcie, proti ktorému nie je možné podať odvolanie po tom, ako bol adresát sankcie informovaný o tomto rozhodnutí.

2. Uverejnenie uvedené v odseku 1 musí obsahovať informácie o druhu a povahe porušenia, o totožnosti zodpovedných osôb a o uložených sankciách.

3. Ak sa príslušný orgán po individuálnom posúdení domnieva, že zverejnenie totožnosti v prípade právnických osôb alebo totožnosti a osobných údajov v prípade fyzických osôb by bolo neprimerané, ohrozilo by stabilitu finančných trhov alebo prebiehajúce vyšetrovanie trestného činu, alebo by spôsobilo dotknutej osobe neprimeranú škodu, pokiaľ túto možno určiť, prijme v súvislosti s rozhodnutím o uložení administratívnej sankcie jedno z týchto riešení:

   a) odložiť jeho uverejnenie dovtedy, kým prestanú existovať všetky dôvody na neuverejnenie;

   b) uverejniť ho anonymne v súlade s vnútroštátnym právom; alebo

   c) upustiť od jeho uverejnenia, ak sa možnosti uvedené v písmenách a) a b) považujú buď za nedostatočné na to, aby zaručili, že neexistuje nebezpečenstvo pre stabilitu finančných trhov, alebo ak by takéto uverejnenie nebolo primerané z hľadiska princípu zhovievavosti uloženej sankcie.

4. V prípade rozhodnutia uverejniť administratívnu sankciu alebo iné opatrenie anonymne podľa odseku 3 písm. b) uverejnenie príslušných informácií možno odložiť.

5. Ak príslušný orgán uverejní rozhodnutie o uložení administratívnej sankcie, voči ktorému sa podalo odvolanie na príslušné súdne orgány, príslušné orgány takisto okamžite uvedú na svojom úradnom webovom sídle túto informáciu a neskôr akékoľvek následné informácie o výsledku takéhoto odvolania. Takisto sa uverejní každé súdne rozhodnutie o zrušení rozhodnutia o uložení administratívnej sankcie.

6. Príslušné orgány zabezpečia, aby akékoľvek informácie uverejnené v súlade s odsekmi 1 až 4 zostali na ich úradných webových sídlach aspoň počas piatich rokov po ich uverejnení. Osobné údaje obsiahnuté v uverejnení sa uchovajú na úradnom webovom sídle príslušného orgánu na obdobie, ktoré je potrebné v súlade s príslušnými predpismi o ochrane údajov.

Článok 49

Služobné tajomstvo

1. Na všetky dôverné informácie prijaté, vymieňané alebo prenášané podľa tohto nariadenia sa vzťahujú podmienky služobného tajomstva stanovené v odseku 2.
2. Povinnosť služobného tajomstva sa vzťahuje na všetky osoby, ktoré pracujú alebo pracovali pre príslušné orgány podľa tohto nariadenia, alebo pre akýkoľvek orgán, trhový podnik, fyzickú alebo právnickú osobu, na ktoré príslušné orgány delegovali právomoci, vrátane zmluvných audítorov a expertov príslušných orgánov.
3. Informácie, na ktoré sa vzťahuje služobné tajomstvo, sa nesmú poskytnúť žiadnej inej osobe ani orgánu s výnimkou poskytnutia na základe ustanovení práva Únie alebo vnútroštátneho práva.
4. Všetky informácie vymieňané medzi príslušnými orgánmi podľa tohto nariadenia, ktoré sa týkajú obchodných alebo prevádzkových podmienok a iných ekonomických či personálnych záležitostí, sa považujú za dôverné a vzťahujú sa na ne požiadavky na služobné tajomstvo s výnimkou prípadov, keď príslušný orgán v čase oznámenia uvedie, že takéto informácie môžu byť zverejnené, alebo ak je takéto zverejnenie potrebné pre súdne konanie.

KAPITOLA VIII

DELEGOVANÉ AKTY

Článok 50

Vykonávanie delegovania právomoci

1. Komisii sa udeľuje právomoc prijímať delegované akty za podmienok stanovených v tomto článku.
2. Právomoc prijímať delegované akty uvedené v článku 28 ods. 3 a článku 38 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od [*Úrad pre publikácie: vložte dátum 5 rokov po nadobudnutí účinnosti tohto nariadenia*].
3. Delegovanie právomoci uvedené v článku 28 ods. 3 a článku 38 ods. 2 môže Európsky parlament alebo Rada kedykoľvek odvolať. Rozhodnutím o odvolaní sa ukončuje delegovanie právomoci, ktoré sa v ňom uvádza. Rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie* alebo k neskoršiemu dátumu, ktorý je v ňom určený. Nie je ním dotknutá platnosť delegovaných aktov, ktoré už nadobudli účinnosť.
4. Komisia pred prijatím delegovaného aktu konzultuje s odborníkmi určenými jednotlivými členskými štátmi v súlade so zásadami stanovenými v Medziinštitucionálnej dohode z 13. apríla 2016 o lepšej tvorbe práva.
5. Komisia oznamuje delegovaný akt hneď po jeho prijatí súčasne Európskemu parlamentu a Rade.
6. Delegovaný akt prijatý podľa článku 28 ods. 3 a článku 38 ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote dvoch mesiacov odo dňa oznámenia uvedeného aktu Európskemu

parlamentu a Rade, alebo ak pred uplynutím uvedenej lehoty Európsky parlament a Rada informovali Komisiu o svojom rozhodnutí nevzniesť námietku. Na podnet Európskeho parlamentu alebo Rady sa táto lehota predĺži o dva mesiace.

KAPITOLA IX

PRECHODNÉ A ZÁVEREČNÉ USTANOVENIA

ODDIEL I

Článok 51

Doložka o preskúmaní

Do [*Úrad pre publikácie: vložte dátum 5 rokov po nadobudnutí účinnosti tohto nariadenia*] Komisia po konzultáciách s orgánmi EBA, ESMA, EIOPA a prípadne s výborom ESRB vykoná preskúmanie a predloží Európskemu parlamentu a Rade správu, ku ktorej v prípade potreby pripojí legislatívny návrh týkajúci sa kritérií na určenie externých poskytovateľov kritických IKT služieb podľa článku 28 ods. 2.

ODDIEL II

ZMENY

Článok 52

Zmeny nariadenia (ES) č. 1060/2009

V prílohe I k nariadeniu (ES) č. 1060/2009 sa v oddiele A bod 4 prvý pododsek nahrádza takto:

„Ratingová agentúra má správne administratívne a účtovné postupy, mechanizmy vnútornej kontroly, účinné postupy hodnotenia rizika a účinné kontrolné a ochranné mechanizmy riadenia systémov IKT v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2021/xx* [DORA].

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/xx [...] (Ú. v. EÚ XX, DD.MM.RRRR, s. X).“.

Článok 53

Zmeny nariadenia (EÚ) č. 648/2012

Nariadenie (EÚ) č. 648/2012 sa mení takto:

1. Článok 26 sa mení takto:

a) Odsek 3 sa nahrádza takto:

„3. Centrálna protistrana udržiava a riadi organizačnú štruktúru, ktorá zaisťuje kontinuitu a riadne fungovanie pri výkone jej služieb a činností. Používa vhodné a primerané systémy, zdroje a postupy vrátane systémov

IKT riadených v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2021/xx* [DORA].

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/xx [...] (Ú. v. EÚ XX, DD.MM.RRRR, s. X).“;

b) Odsek 6 sa vypúšťa;

2. Článok 34 sa mení takto:

a) Odsek 1 sa nahrádza takto:

„1. Centrálna protistrana zavedie, vykonáva a udržiava primeranú politiku zabezpečovania kontinuity podnikateľskej činnosti a plán obnovy po havárii, ktorý zahŕňa plán zabezpečovania kontinuity činnosti v oblasti IKT a plán obnovy po havárii v oblasti IKT, ktoré sú vypracované v súlade s nariadením (EÚ) 2021/xx [DORA], s cieľom zaistiť zachovanie svojich funkcií, včasnú obnovu činnosti a plnenie povinností centrálnej protistrany.“;

b) V odseku 3 sa prvý pododsek nahrádza takto:

„S cieľom zabezpečiť konzistentné uplatňovanie tohto článku ESMA po konzultácii s členmi ESCB vypracuje návrh regulačných technických noriem, v ktorých sa s výnimkou plánu zabezpečovania kontinuity činnosti v oblasti IKT a plánu obnovy po havárii v oblasti IKT stanoví minimálny obsah politiky kontinuity podnikateľskej činnosti a plánu obnovy po havárii a požiadavky na ne.“;

3. V článku 56 ods. 3 sa prvý pododsek nahrádza takto:

„3. S cieľom zaistiť konzistentné uplatňovanie tohto článku ESMA vypracuje návrh regulačných technických noriem, v ktorých sa stanovia podrobnosti, okrem požiadaviek týkajúcich sa riadenia IKT rizika, žiadosti o registráciu uvedenej v odseku 1.“;

4. V článku 79 sa odseky 1 a 2 nahrádzajú takto:

„1. Archív obchodných údajov určí zdroje prevádzkového rizika a minimalizuje ich prostredníctvom vývoja vhodných systémov, kontrolných mechanizmov a postupov vrátane systémov IKT riadených v súlade s nariadením (EÚ) 2021/xx *[DORA]*.

2. Archív obchodných údajov zavedie, vykonáva a udržiava zodpovedajúcu politiku kontinuity podnikateľskej činnosti a plán obnovy po havárii vrátane plánu zabezpečovania kontinuity činnosti v oblasti IKT a plánu obnovy po havárii v oblasti IKT zavedených v súlade s nariadením (EÚ) 2021/xx *[DORA]* a zameraných na zabezpečenie zachovania jeho funkcií, včasnú obnovu činnosti a plnenie povinností archívu obchodných údajov.“;

5. V článku 80 sa vypúšťa odsek 1.

Článok 54

Zmeny nariadenia (EÚ) č. 909/2014

Článok 45 nariadenia (EÚ) č. 909/2014 sa mení takto:

1. Odsek 1 sa nahrádza takto:

„1. Centrálny depozitár určí zdroje prevádzkového rizika, vnútorné aj vonkajšie, a minimalizuje ich vplyv aj prostredníctvom zavedenia vhodných nástrojov, postupov a politík IKT stanovených a riadených v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2021/xx* [*DORA*], ako aj prostredníctvom akýchkoľvek iných príslušných vhodných nástrojov, kontrol a postupov pre iné druhy prevádzkového rizika, a to aj pre všetky systémy vyrovnania transakcií s cennými papiermi, ktoré prevádzkuje.

* Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/xx [...] (Ú. v. EÚ XX, DD.MM.RRRR, s. X).“;

2. Odsek 2 sa vypúšťa.

3. Odseky 3 a 4 sa nahrádzajú takto:

„3. Centrálny depozitár pre služby, ktoré poskytuje, ako aj pre každý systém vyrovnania transakcií s cennými papiermi, ktorý prevádzkuje, zavedie, uplatňuje a zachováva primeranú politiku kontinuity činnosti a plán obnovy po katastrofe vrátane plánu zabezpečovania kontinuity činnosti v oblasti IKT a plánu obnovy po havárii v oblasti IKT v súlade s nariadením (EÚ) 2021/xx [DORA], a to s cieľom zabezpečiť poskytovanie svojich služieb, včasnú obnovu prevádzky a plnenie záväzkov centrálnym depozitárom v prípade udalostí, ktoré predstavujú významné riziko prerušenia prevádzky.

4. Plán uvedený v odseku 3 umožňuje obnovu všetkých transakcií a pozícií účastníkov v okamihu prerušenia s cieľom umožniť účastníkom centrálneho depozitára pokračovať v činnosti s istotou a dokončiť vyrovnanie k určenému dátumu, a to aj prostredníctvom zabezpečenia toho, aby kritické IT systémy mohli obnoviť prevádzku od okamihu prerušenia, ako sa stanovuje v článku 11 ods. 5 a 7 nariadenia (EÚ) 2021/xx [DORA].“;

4. V odseku 6 sa prvý pododsek nahrádza takto:

„Centrálny depozitár zisťuje, monitoruje a riadi riziká, ktoré by pre jeho prevádzku mohli predstavovať kľúčoví účastníci systémov vyrovnania transakcií s cennými papiermi, ktoré centrálny depozitár prevádzkuje, ako aj poskytovatelia služieb, sieťové odvetvia a iné centrálne depozitáre alebo iné trhové infraštruktúry. Na požiadanie informuje príslušné a relevantné orgány o všetkých takýchto zistených rizikách. Príslušný orgán a relevantné orgány bezodkladne informuje aj o všetkých prevádzkových incidentoch vyplývajúcich z iných rizík, než je IKT riziko.“;

5. V odseku 7 sa prvý pododsek nahrádza takto:

„ESMA vypracuje v úzkej spolupráci s členmi ESCB návrh regulačných technických predpisov s cieľom vymedziť prevádzkové riziká uvedené v odsekoch 1 a 6, ktoré sú iné než IKT riziká, ako aj metódy na testovanie, odstránenie alebo minimalizáciu týchto rizík vrátane politík kontinuity činnosti a plánov obnovy po katastrofe uvedených v odsekoch 3 a 4 a spôsobov ich posudzovania.“.

Článok 55

Zmeny nariadenia (EÚ) č. 600/2014

Nariadenie (EÚ) č. 600/2014 sa mení takto:

1. Článok 27g sa mení takto:

   a) Odsek 4 sa vypúšťa;

   b) V odseku 8 sa písmeno c) nahrádza takto:

   c) „c) konkrétne organizačné požiadavky uvedené v odsekoch 3 a 5.“;

2. Článok 27h sa mení takto:

   a) Odsek 5 sa vypúšťa;

   b) V odseku 8 sa písmeno e) nahrádza takto:

   „e) konkrétne organizačné požiadavky uvedené v odseku 4.“;

3. Článok 27i sa mení takto:

   a) Odsek 3 sa vypúšťa;

   b) V odseku 5 sa písmeno b) nahrádza takto:

   „b) konkrétne organizačné požiadavky uvedené v odsekoch 2 a 4.“.

Článok 56

Nadobudnutie účinnosti a uplatňovanie

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

Uplatňuje sa od [*Úrad pre publikácie: vložte dátum 12 mesiacov po nadobudnutí účinnosti*].

Články 23 a 24 sa uplatňujú od [*Úrad pre publikácie: vložte dátum 36 mesiacov po nadobudnutí účinnosti tohto nariadenia*].

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

V Bruseli

Za Európsky parlament	*Za Radu*
predseda	*predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky

1.3. Druh návrhu/iniciatívy

1.4. Ciele

1.5. Dôvody návrhu/iniciatívy

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

1.7. Plánovaný spôsob riadenia

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

2.2. Systémy riadenia a kontroly

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

3.2.2. Odhadovaný vplyv na rozpočtové prostriedky

3.2.3. Odhadovaný vplyv na ľudské zdroje

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Príspevky od tretích strán

3.3. Odhadovaný vplyv na príjmy

Príloha

Všeobecné predpoklady

Právomoci dozoru

LEGISLATÍVNY FINANČNÝ VÝKAZ „AGENTÚRY“

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Návrh nariadenia Európskeho parlamentu a Rady o digitálnej prevádzkovej odolnosti finančného sektora.

1.2. Príslušné oblasti politiky

Oblasť politiky: Finančná stabilita, finančné služby a únia kapitálových trhov

Činnosť: Digitálna prevádzková odolnosť

1.3. Návrh sa týka

☑ **novej akcie**

☐ **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[50]

☐ **predĺženia trvania existujúcej akcie**

☐ **zlúčenia jednej alebo viacerých akcií do ďalšej/novej akcie**

1.4. Ciele

1.4.1. Všeobecné ciele

Všeobecným cieľom iniciatívy je posilniť digitálnu prevádzkovú odolnosť subjektov finančného sektora EÚ zjednotením a modernizáciou existujúcich pravidiel a doplnením nových požiadaviek tam, kde chýbajú. Zlepšil by sa tak aj jednotný súbor pravidiel, pokiaľ ide o jeho digitálny rozmer.

Celkový cieľ je možné rozčleniť na tri všeobecné ciele: 1. zníženie rizika finančného narušenia a nestability, 2. zníženie administratívnej záťaže a zvýšenie účinnosti dohľadu a 3. zvýšenie ochrany spotrebiteľov a investorov.

1.4.2. Špecifické ciele

Návrh má tieto špecifické ciele:

komplexnejšie riešiť riziká informačných a komunikačných technológií („IKT riziká“) a posilniť celkovú úroveň digitálnej odolnosti finančného sektora;

zjednotiť hlásenie incidentov súvisiacich s IKT a riešiť prekrývajúce sa požiadavky na hlásenie;

umožniť orgánom finančného dohľadu prístup k informáciám o incidentoch súvisiacich s IKT;

zabezpečiť, aby finančné subjekty, na ktoré sa vzťahuje tento návrh, posúdili účinnosť svojich preventívnych opatrení a opatrení týkajúcich sa odolnosti a identifikovali zraniteľné miesta súvisiace s IKT;

[50] Podľa článku 58 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

znížiť fragmentáciu jednotného trhu a umožniť cezhraničné akceptovanie výsledkov testovania; posilniť zmluvné záruky pre finančné subjekty pri využívaní IKT služieb vrátane pravidiel outsourcingu (riadenie monitorovania externých poskytovateľov IKT služieb); umožniť dozor nad činnosťami externých poskytovateľov kritických IKT služieb; zintenzívniť výmenu spravodajských informácií o hrozbách vo finančnom sektore.

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na príjemcov/cieľové skupiny.

Aktom o digitálnej prevádzkovej odolnosti pre finančný sektor by sa zabezpečil komplexný rámec vzťahujúci sa na všetky aspekty digitálnej prevádzkovej odolnosti a bol by účinný v zlepšovaní celkovej prevádzkovej odolnosti finančného sektora. Chránil by zrozumiteľnosť a koherentnosť v rámci jednotného súboru pravidiel.

Vďaka nemu by bolo vzájomné pôsobenie so smernicou NIS a jej preskúmaním jasnejšie a jednotnejšie. Priniesol by ozrejmenie finančným subjektom v súvislosti s rôznymi pravidlami digitálnej prevádzkovej odolnosti, ktoré treba dodržiavať, najmä v prípade tých finančných subjektov, ktoré sú držiteľmi viacerých povolení a pôsobia na rôznych trhoch v rámci EÚ.

1.4.4. Ukazovatele výkonnosti

Uveďte ukazovatele na monitorovanie pokroku a dosiahnutých výsledkov.

Možné ukazovatele:

počet incidentov súvisiacich s IKT vo finančnom sektore EÚ a ich vplyv,

počet závažných incidentov súvisiacich s IKT nahlásených prudenciálnym orgánom dohľadu,

počet finančných subjektov, ktoré by boli povinné vykonávať penetračné testy na základe konkrétnej hrozby („TLPT“),

počet finančných subjektov používajúcich štandardné zmluvné doložky pri uzatváraní zmluvných vzťahov s externými poskytovateľmi IKT služieb,

počet externých poskytovateľov kritických IKT služieb, nad ktorými vykonávajú dozor európske orgány dohľadu/prudenciálne orgány dohľadu,

počet finančných subjektov zapojených v riešeniach výmeny spravodajských informácií o hrozbách,

počet orgánov, ktorý má dostávať správy o tom istom incidente súvisiacom s IKT,

počet cezhraničných penetračných testov na základe konkrétnej hrozby.

1.5. Dôvody návrhu/iniciatívy

1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte vrátane podrobného harmonogramu prvotnej fázy vykonávania iniciatívy

Finančný sektor vo veľkej miere využíva informačné a komunikačné technológie (IKT). Napriek významnému pokroku, ktorý sa dosiahol prostredníctvom vnútroštátnych a európskych cielených politických a legislatívnych iniciatív, predstavujú IKT riziká naďalej výzvu pre prevádzkovú odolnosť, výkonnosť a stabilitu finančného systému EÚ. Reforma, ktorá nasledovala po finančnej kríze v roku 2008, v prvom rade posilnila finančnú odolnosť finančného sektora EÚ a bola zameraná na ochranu konkurencieschopnosti a stability EÚ z hospodárskej, prudenciálnej perspektívy a perspektívy trhového správania. Bezpečnosť IKT a celková digitálna prevádzková odolnosť sú súčasťou prevádzkového rizika, ale boli menej ťažiskové v regulačnom programe po kríze a vyvíjali sa len v niektorých oblastiach politiky a regulácie finančných trhov EÚ alebo len v niekoľkých členských štátoch. Táto skutočnosť sa pretavuje do nasledujúcich výziev, ktoré by sa návrhom mali riešiť:

Právny rámec EÚ vzťahujúci sa na IKT riziko a prevádzkovú odolnosť v rámci finančného sektora je fragmentovaný a nie je úplne jednotný.

Neexistencia jednotných požiadaviek na hlásenie incidentov súvisiacich s IKT vedie orgány dohľadu k tomu, že nemajú úplný prehľad o povahe, frekvencii, významnosti a vplyve incidentov.

Niektoré finančné subjekty znášajú zložité, prekrývajúce sa a potenciálne nejednotné požiadavky na hlásenie týkajúce sa toho istého incidentu súvisiaceho s IKT.

Nedostatočná výmena informácií a spolupráca v oblasti spravodajských informácií o kybernetických hrozbách na strategickej, taktickej a prevádzkovej úrovni bránia jednotlivým finančným subjektom v primeranom posudzovaní, monitorovaní kybernetických hrozieb, v ochrane proti nim a reakcii na ne.

V niektorých finančných podsektoroch môže existovať viacero a nekoordinovaných rámcov pre penetračné testovanie a testovanie odolnosti v kombinácii s neexistenciou cezhraničného uznávania výsledkov, pričom v iných podsektoroch tieto testovacie rámce chýbajú.

Chýbajúci prehľad orgánov dohľadu o činnostiach finančných subjektov, ktoré poskytujú externí poskytovatelia IKT, vystavujú finančné subjekty jednotlivo a finančný systém ako celok prevádzkovým rizikám.

Orgány finančného dohľadu nie sú vybavené dostatočným mandátom alebo nástrojmi na monitorovanie a riadenie rizík koncentrácie a systémových rizík vyplývajúcich z toho, že sa finančné subjekty spoliehajú na tretie strany v oblasti IKT.

1.5.2. Prínos zapojenia Únie (môže byť výsledkom rôznych faktorov, napr. lepšej koordinácie, právnej istoty, väčšej účinnosti alebo komplementárnosti). Na účely tohto bodu je „prínos zapojenia Únie“ hodnota vyplývajúca zo zásahu Únie, ktorá dopĺňa hodnotu, ktorú by inak vytvorili len samotné členské štáty.

Dôvody na akciu na európskej úrovni (*ex ante*):

Digitálna prevádzková odolnosť je predmetom spoločného záujmu finančných trhov EÚ. Opatrenie na úrovni EÚ by prinieslo viac výhod a väčšiu hodnotu ako opatrenie prijaté samostatne na vnútroštátnej úrovni. Bez doplnenia týchto prevádzkových ustanovení o IKT riziku by jednotný súbor pravidiel obsahoval nástroje na boj proti všetkým ostatným druhom rizík na európskej úrovni, ale aspekty digitálnej prevádzkovej odolnosti by ostali vynechané alebo by boli predmetom fragmentovaných a nekoordinovaných iniciatív na vnútroštátnej úrovni. Týmto návrhom by sa poskytla právna zrozumiteľnosť v tom, či a ako sa uplatňujú ustanovenia o digitálnej prevádzke, najmä na cezhraničné finančné subjekty, a odstránila by sa potreba, aby členské štáty jednotlivo zlepšovali pravidlá, normy a očakávania týkajúce sa prevádzkovej odolnosti a kybernetickej bezpečnosti v reakcii na súčasné obmedzené pokrytie pravidlami EÚ a všeobecnú povahu smernice NIS.

Očakávaný prínos vytvorený Úniou (*ex-post*):

Intervenciou Únie by sa zvýšila účinnosť politiky pri súčasnom znížení zložitosti a odľahčení finančnej a administratívnej záťaže pre všetky finančné subjekty. Harmonizovala by sa oblasť hospodárstva, ktorá je hlboko vzájomne prepojená a integrovaná a ktorá už využíva jednotný súbor pravidiel a dohľad. Z hľadiska hlásenia incidentov súvisiacich s IKT by sa návrhom obmedzila záťaž spojená s hlásením a implicitné náklady na to, že sa ten istý incident súvisiaci s IKT nahlasuje rôznym orgánom EÚ a/alebo vnútroštátnym orgánom. Zjednoduší sa aj

vzájomne uznávanie/akceptovanie výsledkov testovania subjektov pôsobiacich cezhranične, ktoré podliehajú viacerým rámcom pre testovanie v rôznych členských štátoch.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Nová iniciatíva

1.5.4. Zlučiteľnosť s viacročným finančným rámcom a možná synergia s inými vhodnými nástrojmi

Cieľ tohto návrhu je v súlade s niekoľkými inými politikami a prebiehajúcimi iniciatívami EÚ, najmä smernicou o sieťovej a informačnej bezpečnosti (NIS) a smernicou o európskej kritickej infraštruktúre (ECI). Návrh by zachoval výhody spojené s horizontálnym rámcom pre kybernetickú bezpečnosť tým, že by tri finančné podsektory zostali v rozsahu pôsobnosti smernice NIS. Keďže by orgány finančného dohľadu zostali spojené s ekosystémom NIS, mohli by si vymieňať relevantné informácie s orgánmi NIS a zúčastňovať sa na práci v skupine pre spoluprácu v oblasti kybernetickej bezpečnosti. Návrh by nemal vplyv na smernicu NIS, skôr by z nech vychádzal a riešil možné prekrytia prostredníctvom výnimky *lex specialis*. Vzájomné pôsobenie medzi nariadením o finančných službách a smernicou NIS by sa naďalej riadilo ustanovením *lex specialis*, na základe čoho by finančné subjekty boli vyňaté z hmotnoprávnych požiadaviek uvedených v smernici NIS a zabránilo by sa prekrývaniam medzi týmito dvomi aktmi. Okrem toho je návrh v súlade so smernicou o európskej kritickej infraštruktúre (ECI), ktorá je v súčasnosti predmetom revízie, aby sa zlepšila ochrana a odolnosť kritickej infraštruktúry proti iným ako kybernetickým hrozbám.

Tento návrh by nemal vplyv na viacročný finančný rámec (VFR). Po prvé, rámec dozor nad externými poskytovateľmi kritických IKT služieb bude plne financovaný z poplatkov vybraných od týchto poskytovateľov; po druhé, dodatočné regulačné úlohy súvisiace s digitálnou prevádzkovou odolnosťou zverené európskym orgánom dohľadu budú zabezpečené interným prerozdelením existujúcich zamestnancov.

Toto bude mať za následok návrh na zvýšenie počtu oprávnených zamestnancov agentúry počas budúceho ročného rozpočtového postupu. Agentúra bude naďalej pracovať s cieľom maximalizovať synergie a zvýšenú efektivitu (okrem iného prostredníctvom informačných systémov) a dôsledne monitorovať ďalšiu pracovnú záťaž súvisiacu s týmto návrhom, čo sa zohľadní v úrovni počtu oprávnených zamestnancov požadovaných agentúrou v ročnom rozpočtovom postupe.

1.5.5. Posúdenie rôznych disponibilných možností financovania vrátane možnosti prerozdelenia

Zvážilo sa viacero možností financovania:

Po prvé, dodatočné náklady by sa financovali prostredníctvom zvyčajného mechanizmu financovania európskych orgánov dohľadu. To by však spôsobilo podstatné zvýšenie príspevku EÚ k finančným zdrojom európskych orgánov dohľadu.

Táto možnosť sa vyberá v prípade nákladov týkajúcich sa regulačných úloh súvisiacich s týmto návrhom. Európske orgány dohľadu budú skutočne požiadané, aby prerozdelili existujúcich zamestnancov v záujme vypracovania niekoľkých technických noriem. Ďalšie náklady súvisiace s dozorom nad externými poskytovateľmi kritických IKT služieb by však nebolo možné vyplniť prerozdelením zdrojov v rámci európskych orgánov dohľadu, ktoré majú aj iné úlohy okrem tých, ktoré sú plánované na základe tohto návrhu, ako aj podľa iných právnych predpisov Únie. Okrem toho, úlohy dohľadu súvisiace s digitálnou prevádzkovou odolnosťou si vyžadujú osobitné technické znalosti a odborné znalosti. Keďže súčasná úroveň týchto zdrojov nie je v európskych orgánoch dohľadu dostatočná, sú potrebné dodatočné zdroje.

Na záver, podľa návrhu sa budú vyberať poplatky od externých poskytovateľov kritických IKT služieb, ktorí budú podliehať dozoru. Tieto poplatky sú určené na pokrytie všetkých dodatočných zdrojov, ktoré budú európske orgány dohľadu potrebovať na vykonávanie svojich nových úloh a právomocí.

1.6. Trvanie a finančný vplyv návrhu/iniciatívy

☐ **obmedzené trvanie**

☐ Návrh/iniciatíva je v platnosti od [DD/MM]RRRR do [DD/MM]RRRR.

☐ Finančný vplyv trvá od RRRR do RRRR.

☑ **neobmedzené trvanie**

Počiatočná fáza vykonávania bude trvať od roku 2021

a potom bude implementácia pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia[51]

Priame riadenie na úrovni Komisie

☐ prostredníctvom výkonných agentúr

☐ **Zdieľané riadenie** s členskými štátmi

☑ **Nepriame riadenie**, pri ktorom sa plnením rozpočtu poveria:

☐ medzinárodné organizácie a ich agentúry (uveďte),

☐ Európska investičná banka (EIB) a Európsky investičný fond,

☑ subjekty uvedené v článkoch 70 a 71,

☐ verejnoprávne subjekty,

☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,

☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

Poznámky

Neuvádza sa.

[51] Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

V súlade s existujúcimi opatreniami európske orgány dohľadu pripravujú pravidelné správy o svojej činnosti (vrátane interných správ pre vrcholový manažment, správ pre rady a výročnej správy), pričom ich využívanie zdrojov a ich výkonnosť podliehajú auditom Dvora audítorov a Útvaru Komisie pre vnútorný audit. Monitorovanie a podávanie správ o činnostiach zahrnutých v návrhu bude v súlade s už existujúcimi požiadavkami, ako aj s akýmikoľvek novými požiadavkami vyplývajúcimi z tohto návrhu.

2.2. Systémy riadenia a kontroly

2.2.1. Opodstatnenie navrhovaných spôsobov riadenia, mechanizmov vykonávania financovania, spôsobov platby a stratégie kontroly

Riadenie bude nepriame prostredníctvom európskych orgánov dohľadu. Mechanizmus financovania by sa realizoval prostredníctvom poplatkov vyberaných od príslušných externých poskytovateľov kritických IKT služieb.

2.2.2. Informácie o zistených rizikách a systémoch vnútornej kontroly zavedených na ich zmierňovanie

V súvislosti so zákonným, hospodárnym, účinným a efektívnym používaním pridelených rozpočtových prostriedkov vyplývajúcim z návrhu sa predpokladá, že návrh neprinesie významné nové riziká, na ktoré by sa nevzťahoval existujúci rámec vnútornej kontroly. Nová výzva sa však môže týkať zabezpečenia včasného výberu poplatkov od príslušných externých poskytovateľov kritických IKT služieb.

2.2.3. Odhad a opodstatnenie nákladovej účinnosti kontrol (pomer medzi nákladmi na kontroly a hodnotou súvisiacich riadených finančných prostriedkov) a posúdenie očakávaných úrovní rizika chyby (pri platbe a uzavretí)

Systémy riadenia a kontroly stanovené v nariadeniach o európskych orgánoch dohľadu sa už vykonávajú. Európske orgány dohľadu úzko spolupracujú s Útvarom Komisie pre vnútorný audit s cieľom zabezpečiť, aby sa príslušné normy dodržiavali vo všetkých oblastiach rámca vnútornej kontroly. Tieto opatrenia sa budú uplatňovať aj so zreteľom na úlohu európskych orgánov dohľadu podľa tohto návrhu. Európsky parlament okrem toho každý rozpočtový rok na základe odporúčania Rady udelí každému európskemu orgánu dohľadu absolutórium za plnenie jeho rozpočtu.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce a plánované preventívne a ochranné opatrenia, napr. zo stratégie na boj proti podvodom.

Na účel boja proti podvodom, korupcii a inej nezákonnej činnosti sa na európske orgány dohľadu bez obmedzenia uplatňujú ustanovenia nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 z 11. septembra 2013, pokiaľ ide o vyšetrovania vykonávané Európskym orgánom pre boj proti podvodom (OLAF).

Európske orgány dohľadu majú osobitnú stratégiu na boj proti podvodom a nadväzujúci akčný plán. Posilnené činnosti európskych orgánov dohľadu v oblasti boja proti podvodom budú v súlade s pravidlami a usmerneniami stanovenými v nariadení o rozpočtových pravidlách (opatrenia zamerané na boj proti podvodom ako súčasť správneho finančného riadenia), s politikami OLAF-u v oblasti predchádzania podvodom, s ustanoveniami zahrnutými v stratégii Komisie pre boj proti podvodom [KOM(2011) 376], ako aj v rámci spoločného prístupu k decentralizovaným agentúram EÚ (júl 2012) a v súvisiacom pláne.

V nariadeniach, ktorými sa zriaďujú európske orgány dohľadu, ako aj v nariadeniach o rozpočtových pravidlách európskych orgánov dohľadu sú navyše uvedené ustanovenia o plnení a kontrole rozpočtu európskych orgánov dohľadu a uplatniteľných rozpočtových pravidlách vrátane pravidiel zameraných na predchádzanie podvodom a nezrovnalostiam.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

Existujúce rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP[52]	krajín EZVO[53]	kandidátskych krajín[54]	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách

Požadované nové rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky.

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP	krajín EZVO	kandidátskych krajín	tretích krajín	v zmysle článku 21 ods. 2 písm. b) nariadenia o rozpočtových pravidlách

[52] DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.

[53] EZVO: Európske združenie voľného obchodu.

[54] Kandidátske krajiny a prípadne potenciálne kandidátske krajiny zo západného Balkánu.

3.2. Odhadovaný vplyv na výdavky

3.3. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	Číslo	Okruh

GR: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**SPOLU**
	Záväzky	(1)									
	Platby	(2)									
Rozpočtové prostriedky za GR SPOLU <>	Záväzky										
	Platby										

Okruh viacročného finančného rámca		

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2022	2023	2024	2025	2026	2027	**SPOLU**
Generálne riaditeľstvá:								
• Ľudské zdroje								
• Ostatné administratívne výdavky <>								
GR SPOLU	Rozpočtové prostriedky							

Rozpočtové prostriedky OKRUHU viacročného finančného rámca **SPOLU**	(Záväzky spolu = Platby spolu)							

v mil. EUR v stálych cenách (zaokrúhlené na 3 desatinné miesta)

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**SPOLU**
Rozpočtové prostriedky OKRUHU 1 viacročného finančného rámca **SPOLU**	Záväzky							
	Platby							

3.3.1. Odhadovaný vplyv na rozpočtové prostriedky

☑ Návrh/iniciatíva si nevyžaduje použitie operačných rozpočtových prostriedkov

☐ Návrh/iniciatíva si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

Viazané rozpočtové prostriedky v mil. EUR v stálych cenách (zaokrúhlené na 3 desatinné miesta)

Uveďte ciele a výstupy ⇩			2022		2023		2024		2025		2026		2027		**SPOLU**	
	VÝSTUPY															
	Druh[55]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[56]…																
– Výstup																
Špecifický cieľ č. 1 medzisúčet																
ŠPECIFICKÝ CIEĽ č. 2…																
– Výstup																
Špecifický cieľ č. 2 medzisúčet																
NÁKLADY SPOLU																

[55] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[56] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

3.3.2. Odhadovaný vplyv na ľudské zdroje

3.3.2.1. Zhrnutie

☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov

☑ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR v stálych cenách (zaokrúhlené na 3 desatinné miesta)

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**SPOLU**
Dočasní zamestnanci (funkčná skupina AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Dočasní zamestnanci (funkčná skupina AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Zmluvní zamestnanci							
Vyslaní národní experti							
SPOLU	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Požiadavky na pracovníkov (ekvivalent plného pracovného času):

EBA, EIOPA, ESMA a EEA	2022	2023	2024	2025	2026	2027	**SPOLU**
Dočasní zamestnanci (funkčná skupina AD) EBA=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Dočasní zamestnanci (funkčná skupina AST) EBA=1, EIOPA=1, EEA=1	3	3	3	3	3	3	3
Zmluvní zamestnanci							
Vyslaní národní experti							

SPOLU	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Odhadované potreby ľudských zdrojov pre (zodpovedné) GR

☑ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

☐ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa zaokrúhľujú na celé čísla (alebo najviac na jedno desatinné miesto)

		2022	2023	2024	2025	2026	2027
• **Plán pracovných miest (úradníci a dočasní zamestnanci)**							
• **Externí zamestnanci (ekvivalent plného pracovného času EPPČ)**[57]							
XX 01 02 01 (ZZ, VNE, DAZ z celkového finančného krytia)							
XX 01 02 02 (ZZ, MZ, VNE, DAZ, PED v delegáciách)							
XX 01 04 ***yy***[58]	– ústredie[59]						
	– delegácie						
XX 01 05 02 (ZZ, VNE, DAZ – nepriamy výskum)							
10 01 05 02 (ZZ, VNE, DAZ – priamy výskum)							
Iné rozpočtové riadky (uveďte)							
SPOLU							

XX predstavuje príslušnú oblasť politiky alebo rozpočtovú hlavu.

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	
Externí zamestnanci	

Opis výpočtu nákladov na ekvivalent plného pracovného času by mal byť uvedený v oddiele 3 prílohy V.

[57] ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

[58] Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

[59] Najmä pre štrukturálne fondy, Európsky poľnohospodársky fond pre rozvoj vidieka (EPFRV) a Európsky fond pre rybné hospodárstvo.

3.3.3. Súlad s platným viacročným finančným rámcom

☑ Návrh/iniciatíva je v súlade s platným viacročným finančným rámcom.

☐ Návrh/iniciatíva si vyžaduje zmenu v plánovaní príslušného okruhu vo viacročnom finančnom rámci.

☐ Návrh/iniciatíva si vyžaduje, aby sa použil nástroj flexibility alebo aby sa uskutočnila revízia viacročného finančného rámca[60].

Vysvetlite potrebu a uveďte príslušné okruhy, rozpočtové riadky a zodpovedajúce sumy. […]

3.3.4. Príspevky od tretích strán

☐ Návrh/iniciatíva nezahŕňa spolufinancovanie tretími stranami.

☑ Návrh/iniciatíva zahŕňa spolufinancovanie tretími stranami, ako je odhadnuté v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

EBA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dohľad[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Prostriedky zo spolufinancovania SPOLU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dohľad[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Prostriedky zo spolufinancovania SPOLU	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Pozri články 11 a 17 nariadenia Rady (EÚ, Euratom) č. 1311/2013, ktorým sa stanovuje viacročný finančný rámec na roky 2014 – 2020.

61 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

62 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

ESMA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dohľad[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Prostriedky zo spolufinancovania SPOLU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Odhadovaný vplyv na príjmy

☑ Návrh/iniciatíva nemá finančný vplyv na príjmy.

☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:

☐ vplyv na vlastné zdroje

☐ vplyv na iné príjmy

☐ uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Rozpočtové prostriedky k dispozícii v bežnom rozpočtovom roku	Vplyv návrhu/iniciatívy[64]						
		Rok **N**	Rok **N + 1**	Rok **N + 2**	Rok **N + +3**	Uveďte všetky roky, počas ktorých vplyv trvá (pozri bod 1.6)		
Článok …….								

V prípade rôznych pripísaných príjmov uveďte príslušné rozpočtové riadky výdavkov.

[…]

Uveďte spôsob výpočtu vplyvu na príjmy.

[…]

63 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

64 Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.

PRÍLOHA

Všeobecné predpoklady

Hlava I – Výdavky na zamestnancov

Vo výpočte výdavkov na zamestnancov sa uplatnili nasledujúce osobitné predpoklady na základe ďalej vysvetlených identifikovaných personálnych potrieb:

- Náklady za ďalších zamestnancov prijatých do zamestnania v roku 2022 sú stanovené za 6 mesiacov vzhľadom na predpokladaný čas potrebný na prijatie ďalších zamestnancov do zamestnania.
- Priemerné ročné náklady na dočasného zamestnanca sú 150 000 EUR, v čom sú zahrnuté tzv. prípravné náklady vo výške 25 000 EUR (budovy, IT atď.)
- Opravné koeficienty vzťahujúce sa na mzdy zamestnancov predstavujú v Paríži 117,7 (EBA a ESMA) a vo Frankfurte (EIOPA) 99,4.
- Príspevky zamestnávateľa do systému dôchodkového zabezpečenia za dočasných zamestnancov boli založené na štandardných základných platoch zahrnutých v štandardných priemerných ročných nákladoch, t. j. 95 660 EUR.
- Dodatoční dočasní zamestnanci sú v triedach AD5 a AST.

Hlava II – Infraštruktúra a prevádzkové výdavky

Náklady sú založené na vynásobení počtu zamestnancov podielom roka a štandardnými nákladmi na tzv. prípravu, t. j. 25 000 EUR.

Title III – Operačné výdavky

Odhady nákladov sú založené na týchto predpokladoch:

- Náklady na preklad sú stanovené na 350 000 EUR ročne za každý európsky orgán dohľadu.
- Očakáva sa realizácia nákladov vo výške 500 000 EUR za každý európsky orgán dohľadu počas dvoch rokov 2022 a 2023 na základe rozdelenia 50 % – 50 %. Ročné náklady na údržbu podľa odhadov od roka 2024 dosiahnu 50 000 EUR za každý európsky orgán dohľadu.
- Ročné náklady na dohľad na mieste sú odhadnuté na 200 000 EUR za každý európsky orgán dohľadu.

Výsledkom uvedených odhadov sú nasledujúce náklady ročne:

Okruh viacročného finančného rámca	Číslo	

Stále ceny

EBA:			2022	2023	2024	2025	2026	2027	**SPOLU**
Hlava 1:	Záväzky	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Platby	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Hlava 2:	Záväzky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Záväzky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Rozpočtové prostriedky pre orgán EBA SPOLU	Záväzky	= 1 + 1a + 3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Platby	= 2 + 2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**SPOLU**
Hlava 1:	Záväzky	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Platby	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Hlava 2:	Záväzky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Záväzky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Rozpočtové prostriedky	Záväzky	= 1 + 1a + 3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

pre orgán EIOPA SPOLU	Platby	= 2 + 2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**SPOLU**
Hlava 1:	Záväzky	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Platby	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Hlava 2:	Záväzky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Záväzky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Rozpočtové prostriedky pre orgán ESMA SPOLU	Záväzky	= 1 + 1a + 3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Platby	= 2 + 2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Návrh si vyžaduje použitie operačných rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

Viazané rozpočtové prostriedky v mil. EUR v stálych cenách (zaokrúhlené na 3 desatinné miesta)

EBA

Uveďte ciele a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[65]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[66] Priamy dozor nad externými poskytovateľmi kritických IKT služieb																
– Výstup				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Špecifický cieľ č. 1 medzisúčet																
ŠPECIFICKÝ CIEĽ č. 2…																
– Výstup																
Špecifický cieľ č. 2 medzisúčet																
NÁKLADY SPOLU				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Uveďte ciele a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[67]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[68] Priamy dozor nad externými poskytovateľmi kritických IKT služieb																
– Výstup				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[66] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

[67] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[68] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

Špecifický cieľ č. 1 medzisúčet															
ŠPECIFICKÝ CIEĽ č. 2…															
– Výstup															
Špecifický cieľ č. 2 medzisúčet															
NÁKLADY SPOLU			**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Uveďte ciele a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[69]	Priemerné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet spolu	Náklady spolu
ŠPECIFICKÝ CIEĽ č. 1[70] Priamy dozor nad externými poskytovateľmi kritických IKT služieb																
– Výstup				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Špecifický cieľ č. 1 medzisúčet																
ŠPECIFICKÝ CIEĽ č. 2…																
– Výstup																
Špecifický cieľ č. 2 medzisúčet																
NÁKLADY SPOLU				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Výstupy sú produkty, ktoré sa majú dodať, a služby, ktoré sa majú poskytnúť (napr.: počet financovaných výmen študentov, vybudované cesty v km atď.).

[70] Ako je uvedené v bode 1.4.2. „Špecifické ciele…“

Činnosti dozoru sú v celom rozsahu financované z poplatkov vybraných od subjektov, nad ktorými sa vykonáva dozor, takto:

EBA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dozor[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Prostriedky zo spolufinancovania SPOLU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dozor[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Prostriedky zo spolufinancovania SPOLU	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Spolu
Náklady budú na 100 % kryté poplatkami vybranými od subjektov, nad ktorými sa vykonáva dozor[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Prostriedky zo spolufinancovania SPOLU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

[72] 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

[73] 100 % celkových odhadovaných nákladov plus celé príspevky zamestnávateľa do systému dôchodkového zabezpečenia.

OSOBITNÉ INFORMÁCIE

Právomoci priameho dozoru

Na úvod treba pripomenúť, že subjekty podliehajúce priamemu dohľadu orgánu ESMA by mali orgánu ESMA platiť poplatky (jednorazové poplatky za registráciu a pravidelné poplatky za priebežný dohľad). Platí to pre ratingové agentúry [pozri delegované nariadenie Komisie (EÚ) č. 272/2012] a archívy obchodných údajov [delegované nariadenie Komisie (EÚ) č. 1003/2013].

Podľa tohto legislatívneho návrhu budú európske orgány dohľadu poverené novými úlohami zameranými na podporu konvergencie prístupov dohľadu nad IKT rizikom tretej strany vo finančnom sektore tak, že sa externí poskytovatelia kritických IKT služieb podrobia rámcu dozoru Únie.

Rámec dozoru plánovaný v tomto návrhu vychádza z existujúcej inštitucionálnej architektúry v oblasti finančných služieb, v ktorej spoločný výbor európskych orgánov dohľadu zabezpečuje medziodvetvovú koordináciu vo vzťahu ku všetkým záležitostiam týkajúcim sa IKT rizika, v súlade s jeho úlohami v oblasti kybernetickej bezpečnosti, podporovaný príslušným podvýborom (fórum pre dozor) vykonávajúcim prípravnú činnosť pre jednotlivé rozhodnutia a kolektívne odporúčania určené externým poskytovateľom kritických IKT služieb.

Prostredníctvom tohto rámca európske orgány dohľadu označené ako hlavné orgány dozoru pre každého externého poskytovateľa kritických IKT služieb získavajú právomoci na zabezpečenie toho, aby poskytovatelia technologických služieb, ktorí plnia kritickú úlohu pre fungovanie finančného sektora, boli primerane monitorovaní v celoeurópskom meradle. Povinnosti dozoru sú stanovené v návrhu a podrobnejšie objasnené v dôvodovej správe. Zahŕňajú práva požadovať všetky príslušné informácie a dokumentáciu na vykonanie všeobecných vyšetrovaní a kontrol, na adresovanie odporúčaní a následné predkladanie správ o prijatých opatreniach alebo vykonaných nápravných opatrení na riešenie uvedených odporúčaní.

S cieľom vykonávať nové úlohy predpokladané v tomto návrhu európske orgány dohľadu najmú ďalších zamestnancov špecializujúcich sa na IKT riziko a zameriavajúcich sa na posudzovanie externých závislostí.

Odhad potrieb ľudských zdrojov je na úrovni 6 ekvivalentov plného pracovného času pre každý orgán (5 AD a 1 AST na podporu AD). Európskym orgánom dohľadu takisto vzniknú ďalšie náklady na IT podľa odhadu na úrovni 500 000 EUR (jednorazové náklady), ako aj 50 000 EUR ročne v prípade každého z európskych orgánov dohľadu ako náklady na údržbu. Jedným dôležitým prvkom v plnení nových úloh sú misie na vykonávanie kontrol a auditov na mieste, ktoré je možné odhadnúť na úrovni 200 000 EUR ročne za každý európsky orgán dohľadu. Náklady na preklad rôznych dokumentov, ktoré by európske orgány dohľadu dostávali od externých poskytovateľov kritických IKT služieb, sú takisto zahrnuté do riadku operačných nákladov a ročne predstavujú 350 000 EUR.

Všetky uvedené administratívne náklady budú v celom rozsahu financované z ročných poplatkov vyberaných európskymi orgánmi dohľadu od externých poskytovateľov kritických IKT služieb, nad ktorými sa bude vykonávať dozor (bez vplyvu na rozpočet EÚ).