I

(Legislatívne akty)

NARIADENIA

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2554

zo 14. decembra 2022

o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011

(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 ([1]),

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru ([2]),

konajúc v súlade s riadnym legislatívnym postupom ([3]),

keďže:

(1) V digitálnom veku informačné a komunikačné technológie (ďalej len „IKT“) podporujú zložité systémy používané pri každodenných činnostiach. Udržiavajú chod našich hospodárstiev v kľúčových odvetviach vrátane finančného sektora a zlepšujú fungovanie vnútorného trhu. Zvýšená digitalizácia a vzájomná prepojenosť zároveň zvyšujú IKT riziko a spoločnosť ako celok, a najmä finančný systém, sú zraniteľnejšie 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 činností finančných subjektov Únie, ich digitálna odolnosť sa ešte len musí začať lepšie upravovať a integrovať do ich širších operatívnych rámcov.

(2) Využívanie IKT začalo v posledných desaťročiach plniť v oblasti poskytovania finančných služieb kľúčovú úlohu, pričom dosiahlo bod, v ktorom v súčasnosti nadobudlo zásadný význam pre vykonávanie typických každodenných funkcií všetkých finančných subjektov. Digitalizácia sa dnes týka napríklad platieb, ktoré čoraz viac prechádzajú od hotovostných a papierových metód k používaniu digitálnych riešení, ako aj zúčtovania a vyrovnania transakcií s cennými papiermi, elektronického a algoritmického obchodovania, operácií požičiavania a financovania, partnerského financovania, úverových ratingov, správy nárokov a operácií back-office. Sektor poisťovníctva sa tiež

([1]) Ú. v. EÚ C 343, 26.8.2021, s. 1.
([2]) Ú. v. EÚ C 155, 30.4.2021, s. 38.
([3]) Pozícia Európskeho parlamentu z 10. novembra 2022 (zatiaľ neuverejnená v úradnom vestníku) a rozhodnutie Rady z 28. novembra 2022.

transformoval vďaka využívaniu IKT, od vzniku sprostredkovateľov poistenia ponúkajúcich svoje služby online využívajúc nástroje InsurTech až po digitálne upisovanie poistenia. 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.

(3) Európsky výbor pre systémové riziká (ďalej len „ESRB“) v správe z roku 2020, ktorá sa zaoberá systémovým kybernetickým rizikom, opätovne potvrdil, že súčasná vysoká úroveň prepojenosti medzi finančnými subjektmi, finančnými trhmi a infraštruktúrami finančného trhu, a najmä vzájomná závislosť ich IKT systémov, by mohli predstavovať systémovú zraniteľnosť, pretože lokalizované kybernetické incidenty by sa mohli rýchlo rozšíriť z ktoréhokoľvek z približne 22 000 finančných subjektov Únie do celého finančného systému, a to bez ohľadu na geografické hranice. Závažné narušenia v oblasti IKT, ku ktorým dochádza vo finančnom sektore, nemajú vplyv len na finančné subjekty samotné. Zároveň uľahčujú aj cestu pre šírenie lokalizovaných zraniteľných miest naprieč finančnými prenosovými kanálmi a potenciálne vedú k nepriaznivým dôsledkom pre stabilitu finančného systému Únie, ako je hromadné vyberanie peňazí a celková strata dôvery vo finančné trhy.

(4) V posledných rokoch sa na IKT riziko sústredila pozornosť medzinárodných, únijných a vnútroštátnych tvorcov politík, regulačných orgánov a orgánov stanovujúcich normy, ktorých snahou je zvýšiť digitálnu 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 G7 a G20 stanovili za cieľ poskytnúť príslušným orgánom a organizátorom trhu v rôznych jurisdikciách nástroje na posilnenie odolnosti ich finančných systémov. Táto práca bola motivovaná aj potrebou náležite zohľadniť IKT riziko v kontexte vysoko prepojeného globálneho finančného systému a usilovať sa o väčšiu konzistentnosť príslušných najlepších postupov.

(5) Napriek cieleným únijným a vnútroštátnym politickým a legislatívnym iniciatívam IKT riziko naďalej predstavuje výzvu pre prevádzkovú odolnosť, výkonnosť a stabilitu finančného systému Únie. Reformy, ktorá nasledovali po finančnej kríze v roku 2008, v prvom rade posilnili finančnú odolnosť finančného sektora Únie a boli zamerané na ochranu konkurencieschopnosti a stability Únie z hospodárskej, prudenciálnej perspektívy a perspektívy trhového správania. Hoci sú bezpečnosť IKT a digitálna odolnosť súčasťou prevádzkového rizika, v regulačnom programe nasledujúcom po finančnej kríze 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) Vo svojom oznámení z 8. marca 2018 s názvom Akčný plán pre finančné technológie: Za konkurencieschopnejší a inovatívnejší európsky finančný sektor Komisia zdôraznila, že je mimoriadne dôležité zvýšiť odolnosť finančného sektora Únie, a to 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 efektívne a plynule poskytovať finančné služby v celej Únii, a to aj v stresových situáciách, a zároveň zachovať dôveru spotrebiteľov a trhu.

(7) V apríli 2019 Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) (ďalej len „EBA“) zriadený nariadením Európskeho parlamentu a Rady (EÚ) č. 1093/2010 ([4]), Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov) (ďalej len „EIOPA“) zriadený nariadením Európskeho parlamentu a Rady (EÚ) č. 1094/2010 ([5]) a Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) (ďalej len „ESMA“) zriadený

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1093/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre bankovníctvo) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/78/ES (Ú. v. EÚ L 331, 15.12.2010, s. 12).

([5]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48).

nariadením Európskeho parlamentu a Rady (EÚ) č. 1095/2010 ([6]) (spoločne ďalej len „európske orgány dohľadu“) spolu vydali technické odporúčania, v ktorých vyzvali na jednotný prístup k IKT riziku v oblasti financií a odporučili primeraným spôsobom posilniť digitálnu prevádzkovú odolnosť odvetvia finančných služieb prostredníctvom iniciatívy Únie špecifickej pre toto odvetvie.

(8) Finančný sektor Únie je regulovaný 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 digitálnu prevádzkovú odolnosť, a to posilnením mandátov príslušných orgánov s cieľom umožniť im vykonávať dohľad nad riadením IKT rizika vo finančnom sektore v záujme ochrany integrity a efektívnosti vnútorného trhu a uľahčenia jeho riadneho fungovania.

(9) Legislatívne rozdiely a nerovnaké vnútroštátne regulačné prístupy alebo prístupy, pokiaľ ide o dohľad nad IKT rizikom, vytvárajú prekážky fungovania vnútorného trhu s finančnými službami, čo finančným subjektom vykonávajúcim činnosť na cezhraničnom základe bráni v bezproblémovom uplatňovaní slobody usadiť sa a poskytovať služby. Narušiť by sa mohla byť aj hospodárska súťaž medzi rovnakým typom finančných subjektov pôsobiacich v rôznych členských štátoch. Týka sa to najmä oblastí, v ktorých bola harmonizácia Únie veľmi obmedzená, ako je testovanie digitálnej prevádzkovej odolnosti, alebo v ktorých chýba, ako je monitorovanie externého IKT rizika. Rozdiely vyplývajúce z predpokladaného vývoja na vnútroštátnej úrovni by mohli vytvoriť ďalšie prekážky fungovania vnútorného trhu na úkor účastníkov trhu a finančnej stability.

(10) V súčasnosti v dôsledku skutočnosti, že ustanovenia týkajúce sa IKT rizika boli len čiastočne riešené na úrovni Únie, existujú nedostatky alebo navzájom sa prekrývajúce miesta v dôležitých oblastiach, ako je nahlasovanie incidentov súvisiacich s IKT a testovanie digitálnej prevádzkovej odolnosti, a nezrovnalosti vyplývajúce z nových rozdielnych vnútroštátnych pravidiel alebo nákladovo neúčinného uplatňovania prekrývajúcich sa pravidiel. Je to obzvlášť škodlivé pre používateľa intenzívne využívajúceho IKT, ako je napríklad finančný sektor, keďže technologické riziká nepoznajú hranice a finančný sektor poskytuje 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 každú licenciu mohol vydať iný príslušný orgán v jednom alebo viacerých členských štátoch) čelia pri riešení IKT rizika a zmierňovaní nepriaznivých vplyvov IKT incidentov prevádzkovým výzvam samostatne a koherentným, nákladovo efektívnym spôsobom.

(11) Keďže jednotný súbor pravidiel nesprevádza komplexný rámec pre IKT riziko alebo prevádzkové riziká, je potrebná ďalšia harmonizácia kľúčových požiadaviek na digitálnu prevádzkovú odolnosť všetkých finančných subjektov. Rozvoj spôsobilostí v oblasti IKT a celková odolnosť finančných subjektov na základe uvedených 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 vnútorného trhu, malo by vychádzať z ustanovení článku 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“), ako sa vykladá v súlade s príslušnou judikatúrou Súdneho dvora Európskej únie (ďalej len „Súdny dvor“).

(12) Cieľom tohto nariadenia je konsolidovať a vylepšiť požiadavky na IKT riziko ako súčasť požiadaviek na prevádzkové riziko, ktoré sa doteraz riešili samostatne v rôznych právnych aktoch Únie. Uvedenými aktmi boli síce pokryté hlavné kategórie finančného rizika (napr. kreditné riziko, trhové riziko, kreditné riziko protistrany a riziko likvidity a riziko trhového správania), no v čase ich prijatia neriešili komplexne všetky zložky prevádzkovej odolnosti. Keď sa pravidlá týkajúce sa prevádzkového rizika ďalej rozpracovávali v týchto právnych aktoch Únie, často uprednostňovali skôr tradičný kvantitatívny prístup k riešeniu rizika (a to stanovenie kapitálovej požiadavky na pokrytie IKT rizika) než cielené kvalitatívne požiadavky na ochranu, odhaľovanie, obmedzovanie, obnovu a nápravu spôsobilostí v súvislosti s incidentmi týkajúcimi sa IKT, alebo na stanovovanie spôsobilosti v oblasti

([6]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES (Ú. v. EÚ L 331, 15.12.2010, s. 84).

nahlasovania a digitálneho testovania. Uvedené akty mali v prvom rade upravovať a aktualizovať základné pravidlá prudenciálneho dohľadu, integrity trhu alebo trhového správania. Konsolidáciou a vylepšením rôznych pravidiel týkajúcich sa IKT rizika by sa všetky ustanovenia týkajúce sa digitálneho rizika vo finančnom sektore mali po prvýkrát konzistentným spôsobom spojiť do jedného legislatívneho aktu. Toto nariadenie preto vypĺňa medzery alebo odstraňuje nezrovnalosti v niektorých predchádzajúcich právnych aktoch, a to aj v súvislosti s terminológiou, ktorá sa v nich používa, a výslovne odkazuje na IKT riziko prostredníctvom cielených pravidiel týkajúcich sa spôsobilostí v oblasti riadenia IKT rizika, nahlasovania incidentov, testovania prevádzkovej odolnosti a monitorovania externého IKT rizika. Týmto nariadením by sa zároveň mala zvýšiť informovanosť o IKT riziku a malo by sa v ňom uznať, že incidenty v oblasti IKT a nedostatočná prevádzková odolnosť môžu ohroziť spoľahlivosť finančných subjektov.

(13) Finančné subjekty by sa mali pri riešení IKT rizika riadiť rovnakým prístupom a rovnakými pravidlami založenými na zásadách, pričom by mali zohľadniť svoju veľkosť a celkový rizikový profil, ako aj povahu, rozsah a zložitosť svojich služieb, činností a operácií. Konzistentnosť prispieva k posilneniu dôvery vo finančný systém a k zachovaniu jeho stability, a to najmä v časoch vysokej miery spoliehania sa na IKT systémy, platformy a infraštruktúry, čo so sebou prináša zvýšené digitálne riziko. Dodržiavanie základnej kybernetickej hygieny by malo tiež predísť vzniku vysokých nákladov pre hospodárstvo, a to tak, že sa minimalizuje vplyv a náklady narušení v oblasti IKT.

(14) Nariadením sa pomôže znížiť regulačná zložitosť, podporí sa konvergencia dohľadu a zvýši sa právna istota a zároveň sa prispeje 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 je preto najvhodnejší spôsob, ako zaručiť homogénne a ucelené uplatňovanie všetkých zložiek riadenia IKT rizika finančným sektorom Únie.

(15) Smernica Európskeho parlamentu a Rady (EÚ) 2016/114830 ([7]) bola prvým horizontálnym rámcom pre kybernetickú bezpečnosť na úrovni Únie, ktorý sa vzťahoval aj na tri typy finančných subjektov, a to úverové inštitúcie, obchodné miesta a centrálne protistrany. Keďže sa však v smernici (EÚ) 2016/1148 stanovil mechanizmus identifikácie prevádzkovateľov základných služieb na vnútroštátnej úrovni, členské štáty určili len niektoré úverové inštitúcie, obchodné miesta a centrálne protistrany, ktoré sa tak v praxi dostali do rozsahu jej pôsobnosti, a teda podliehali požiadavkám na bezpečnosť IKT a oznamovanie incidentov, ktoré sú v nej stanovené. V smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 ([8]) sa stanovuje jednotné kritérium na určenie subjektov, ktoré patria do rozsahu jej pôsobnosti (pravidlo veľkostnej hranice), pričom sa v rozsahu jej pôsobnosti ponechávajú aj tri typy finančných subjektov.

(16) Keďže sa však týmto nariadením zvyšuje úroveň harmonizácie rôznych zložiek digitálnej odolnosti zavedením požiadaviek na riadenie IKT rizika a nahlasovanie incidentov súvisiacich s IKT, ktoré sú prísnejšie v porovnaní s požiadavkami stanovenými v súčasnom práve Únie v oblasti finančných služieb, táto vyššia úroveň predstavuje zvýšenú harmonizáciu aj v porovnaní s požiadavkami stanovenými v smernici (EÚ) 2022/2555. Toto nariadenie preto predstavuje *lex specialis* vo vzťahu k smernici (EÚ) 2022/2555. Zároveň je nevyhnutné zachovať silný vzťah finančného sektoru s horizontálnym rámcom Únie v oblasti kybernetickej bezpečnosti, ako sa v súčasnosti stanovuje v smernici (EÚ) 2022/2555, s cieľom zabezpečiť súlad so stratégiami kybernetickej bezpečnosti, ktoré prijali členské štáty, a orgánom dohľadu nad finančnými subjektmi umožniť, aby boli informované o kybernetických incidentoch týkajúcich sa iných sektorov, na ktoré sa uvedená smernica vzťahuje.

([7]) 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).

([8]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, o zmene nariadenia (EÚ) č. 910/2014 a smernice (EÚ) 2018/1972 a o zrušení smernice (EÚ) 2016/1148 (smernica NIS 2) (pozri stranu 80 tohto úradného vestníka).

(17) V súlade s článkom 4 ods. 2 Zmluvy o Európskej únii a bez toho, aby bolo dotknuté súdne preskúmanie Súdnym dvorom, by toto nariadenie nemalo mať vplyv na zodpovednosť členských štátov, pokiaľ ide o základné funkcie štátu týkajúce sa verejnej bezpečnosti, obrany a ochrany národnej bezpečnosti, napríklad pokiaľ ide o poskytovanie informácií, ktoré by boli v rozpore so zaistením národnej bezpečnosti.

(18) S cieľom umožniť medziodvetvové vzdelávanie a účinne využívať skúsenosti z iných sektorov pri riešení kybernetických hrozieb by finančné subjekty uvedené v smernici (EÚ) 2022/2555+ mali zostať súčasťou „ekosystému“ uvedenej smernice (napríklad skupina pre spoluprácu a jednotky pre riešenie počítačových bezpečnostných incidentov [ďalej len „CSIRT“)]. Európske orgány dohľadu a vnútroštátne príslušné orgány by mali mať možnosť zúčastňovať sa na diskusiách o strategickej politike a na technických činnostiach skupiny pre spoluprácu podľa uvedenej smernice a vymieňať si informácie a ďalej spolupracovať s jednotnými kontaktnými miestami určenými alebo zriadenými v súlade s uvedenou smernicou. Príslušné orgány podľa tohto nariadenia by mali tiež konzultovať a spolupracovať s jednotkami CSIRT. Príslušné orgány by zároveň mali mať možnosť žiadať o technické poradenstvo príslušné orgány určené alebo zriadené v súlade so smernicou (EÚ) 2022/2555+ a uzatvárať dojednania v oblasti spolupráce, ktorých cieľom je zabezpečiť účinné a rýchlo reagujúce koordinačné mechanizmy.

(19) Vzhľadom na silné prepojenia medzi digitálnou odolnosťou a fyzickou odolnosťou finančných subjektov je v tomto nariadení a smernici Európskeho parlamentu a Rady (EÚ) 2022/2557+ ([9]) potrebný koherentný prístup, pokiaľ ide o odolnosť kritických subjektov. Vzhľadom na to, že fyzická odolnosť finančných subjektov sa komplexne rieši prostredníctvom povinností v oblasti riadenia IKT rizika a nahlasovania, na ktoré sa vzťahuje toto nariadenie, povinnosti stanovené v kapitolách III a IV smernice (EÚ) 2022/2557+ by sa nemali vzťahovať na finančné subjekty, ktoré patria do rozsahu pôsobnosti uvedenej smernice.

(20) Poskytovatelia služieb cloud computingu sú jednou z kategórií digitálnej infraštruktúry, na ktoré sa vzťahuje smernica (EÚ) 2022/2555+. Rámec dozoru zo strany Únie (ďalej len „rámec dozoru“) stanovený týmto nariadením sa vzťahuje na všetkých kritických externých poskytovateľov IKT služieb vrátane poskytovateľov služieb cloud computingu poskytujúcich IKT služby finančným subjektom a mal by sa považovať za doplnkový k dohľadu na základe smernice (EÚ) 2022/2555+. Rámec dozoru zriadený týmto nariadením by sa navyše mal vzťahovať na poskytovateľov služieb cloud computingu, keďže neexistuje horizontálny rámec Únie, ktorým by sa zriaďoval orgán pre digitálny dozor.

(21) S cieľom zachovať plnú kontrolu nad IKT rizikom musia mať finančné subjekty komplexné spôsobilosti umožňujúce silné a účinné riadenie IKT rizika, ako aj osobitné mechanizmy a politiky na zvládanie všetkých incidentov súvisiacich s IKT a nahlasovanie závažných incidentov súvisiacich s IKT. Podobne by finančné subjekty mali mať zavedené politiky na testovanie IKT systémov, kontrol a procesov, ako aj na riadenie externého IKT rizika. Mala by sa zvýšiť základná úroveň digitálnej prevádzkovej odolnosti finančných subjektov, pričom by sa malo zároveň umožniť primerané uplatňovanie požiadaviek na určité finančné subjekty, najmä mikropodniky, ako aj finančné subjekty, na ktoré sa vzťahuje zjednodušený rámec riadenia IKT rizika. S cieľom uľahčiť účinný dohľad nad inštitúciami zamestnaneckého dôchodkového zabezpečenia, ktorý je primeraný a rieši potrebu znížiť administratívne zaťaženie príslušných orgánov, by relevantné vnútroštátne mechanizmy dohľadu nad takýmito finančnými subjektmi mali zohľadňovať ich veľkosť a celkový rizikový profil, ako aj povahu, rozsah a zložitosť ich služieb, činností a operácií, a to aj v prípade prekročenia príslušných prahových hodnôt stanovených v článku 5 smernice Európskeho parlamentu a Rady (EÚ) 2016/2341 ([10]). Činnosti dohľadu by sa mali osobitne zameriavať predovšetkým na potrebu riešiť závažné riziká spojené s riadením IKT rizika konkrétneho subjektu.

([9]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557+ zo 14. decembra 2022 164 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES (pozri stranu ... tohto úradného vestníka).

([10]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/2341 zo 14. decembra 2016 o činnostiach inštitúcií zamestnaneckého dôchodkového zabezpečenia (IZDZ) a o dohľade nad nimi (Ú. v. EÚ L 354, 23.12.2016, s. 37).

Príslušné orgány by mali tiež zachovávať obozretný, ale primeraný prístup v súvislosti s dohľadom nad inštitúciami zamestnaneckého dôchodkového zabezpečenia, ktoré v súlade s článkom 31 smernice (EÚ) 2016/2341 zadávajú významnú časť svojej hlavnej činnosti, ako je správa aktív, poistno-matematické výpočty, účtovníctvo a správa údajov, poskytovateľom služieb formou outsourcingu.

(22) 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 (ďalej len „ENISA“) zriadenej nariadením Európskeho parlamentu a Rady (EÚ) 2019/881 ([11]) a skupiny pre spoluprácu podľa smernice (EÚ) 2022/2555+, stále existujú alebo sa môžu objaviť rozdielne prístupy k prahovým hodnotám a používaniu taxonómií pre ostatné finančné subjekty. V dôsledku uvedených rozdielov existujú viaceré požiadavky, ktoré musia finančné subjekty dodržiavať, najmä ak pôsobia v niekoľkých členských štátoch a sú súčasťou finančnej skupiny. Takéto rozdiely majú okrem toho potenciál brániť vytvoreniu ďalších jednotných alebo centralizovaných mechanizmov Únie, ktoré urýchľujú proces nahlasovania a podporujú rýchlu a plynulú výmenu informácií medzi príslušnými orgánmi, ktorá je kľúčová pre riešenie IKT rizika v prípade rozsiahlych útokov s potenciálne systémovými následkami.

(23) S cieľom znížiť administratívne zaťaženie a potenciálne duplicitné nahlasovacie povinnosti pre určité finančné subjekty by sa požiadavky na nahlasovanie incidentov podľa smernice Európskeho parlamentu a Rady (EÚ) 2015/2366 ([12]) mali prestať uplatňovať na poskytovateľov platobných služieb, ktorí patria do rozsahu pôsobnosti tohto nariadenia. Úverové inštitúcie, inštitúcie elektronických peňazí, platobné inštitúcie a poskytovatelia služieb informovania o účte, ako sa uvádza v článku 33 ods. 1 uvedenej smernice, by preto mali od dátumu začatia uplatňovania tohto nariadenia podľa tohto nariadenia oznamovať všetky prevádzkové alebo bezpečnostné incidenty súvisiace s platbami, ktoré boli predtým nahlásené podľa uvedenej smernice, bez ohľadu na to, či takéto incidenty súvisia s IKT.

(24) 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 relevantnými verejnými orgánmi vrátane orgánov presadzovania práva a orgánov pre riešenie krízových situácií by sa v tomto nariadení mal stanoviť spoľahlivý režim nahlasovania incidentov súvisiacich s IKT, na základe ktorého sa relevantné požiadavky zamerajú na súčasné nedostatky v práve v oblasti finančných služieb a odstránia sa existujúce prekrývania a duplicity s cieľom zmierniť náklady. Je nevyhnutné harmonizovať režim nahlasovania incidentov súvisiacich s IKT tak, že sa od všetkých finančných subjektov bude vyžadovať, aby nahlasovali svojim príslušným orgánom prostredníctvom jednotného zjednodušeného rámca stanoveného v tomto nariadení. Európske orgány dohľadu by okrem toho mali byť splnomocnené upresniť relevantné prvky rámca nahlasovania incidentov súvisiacich s IKT, ako je taxonómia, časové rámce, dátové súbory, vzory a príslušné prahové hodnoty. S cieľom zabezpečiť úplný súlad so smernicou (EÚ) 2022/2555+ by finančné subjekty mali mať možnosť dobrovoľne oznamovať závažné kybernetické hrozby relevantnému príslušnému orgánu, ak sa domnievajú, že kybernetická hrozba je relevantná pre finančný systém, používateľov služieb alebo klientov.

(25) V určitých finančných podsektoroch sa vypracovali požiadavky na testovanie digitálnej prevádzkovej odolnosti, ktorými sa stanovili rámce, ktoré nie sú vždy plne zosúladené. To vedie k potenciálnej duplicite nákladov pre cezhraničné finančné subjekty a spôsobuje zložitosť vzájomného uznávania výsledkov testovania digitálnej prevádzkovej odolnosti, čo následne môže viesť k fragmentácii vnútorného trhu.

([11]) 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).

([12]) Smernica Európskeho parlamentu a Rady (EÚ) 2015/2366 z 25. novembra 2015 o platobných službách na vnútornom trhu, ktorou sa menia smernice 2002/65/ES, 2009/110/ES a 2013/36/EÚ a nariadenie (EÚ) č. 1093/2010, a ktorou sa zrušuje smernica 2007/64/ES (Ú. v. EÚ L 337, 23.12.2015, s. 35).

(26) Okrem toho, ak sa testovanie IKT nevyžaduje, zraniteľné miesta zostávajú neodhalené a spôsobujú vystavenie finančného subjektu IKT riziku a v konečnom dôsledku vytvárajú vyššie riziko pre stabilitu a integritu finančného sektora. Bez zásahu Únie by testovanie digitálnej prevádzkovej odolnosti bolo naďalej nekonzistentné a chýbal by mu systém vzájomného uznávania výsledkov testovania IKT medzi jednotlivým jurisdikciami. Keďže je tiež nepravdepodobné, že by iné finančné podsektory prijali schémy testovania v zmysluplnom rozsahu, chýbali by im potenciálne prínosy rámca pre testovanie, pokiaľ ide o odhaľovanie IKT zraniteľných miest a rizík a testovanie spôsobilostí obrany a kontinuity činností, čo prispieva k zvýšeniu dôvery zákazníkov, dodávateľov a obchodných partnerov. S cieľom napraviť uvedené prekrývanie, rozdiely a nedostatky je potrebné stanoviť pravidlá zamerané na režim koordinovaného testovania, čím sa uľahčí vzájomné uznávanie pokročilého testovania finančných subjektov spĺňajúcich kritériá stanovené v tomto nariadení.

(27) Závislosť finančných subjektov od využívania 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 uplynulých 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.

(28) Rozsiahle využívanie IKT služieb je preukázané 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 pri presadzovaní osobitných práv, ako sú práva na prístup alebo audit, dokonca aj keď sú tieto práva zakotvené v ich zmluvných dojednaniach. Mnohé uvedené zmluvné dojednania okrem toho neposkytujú dostatočné záruky umožňujúce plnohodnotne monitorovať subdodávateľské procesy, čím finančný subjekt stráca schopnosť posúdiť súvisiace riziká. Keďže okrem toho externí poskytovatelia IKT služieb často poskytujú štandardizované služby rôznym typom klientov, v takýchto zmluvných dojednaniach sa nemusia vždy primerane zohľadňovať individuálne alebo osobitné potreby subjektov finančného sektora.

(29) Aj keď právo Únie v oblasti finančných služieb obsahuje určité *všeobecné pravidlá týkajúce sa outsourcingu*, monitorovanie zmluvného rozmeru nie je plne zakotvené v práve 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 je potrebné stanoviť určité kľúčové zásady na usmernenie riadenia externého IKT rizika finančnými subjektmi, ktoré majú osobitný význam, keď finančné subjekty využívajú externých poskytovateľov IKT služieb na podporu svojich kritických alebo dôležitých funkcií. Uvedené zásady by mal sprevádzať súbor základných zmluvných práv vo vzťahu k niekoľkým prvkom pri plnení a ukončení zmluvných dojednaní s cieľom poskytnúť určité minimálne záruky, s cieľom posilniť schopnosť finančných subjektov účinne monitorovať každé IKT riziko vznikajúce na úrovni externých poskytovateľov služieb. Uvedenými zásadami sa dopĺňa odvetvové právo uplatniteľné na outsourcing.

(30) V súčasnosti je zjavný určitý nedostatok homogenity a konvergencie, pokiaľ ide o monitorovanie externého IKT rizika a externej závislosti v oblasti IKT. Napriek úsiliu o riešenie outsourcingu, ako sú napríklad usmernenia EBA k outsourcingu z roku 2019 a usmernenia ESMA o outsourcingu zo strany poskytovateľov cloudových služieb z roku 2021, sa širšia problematika opatrení proti systémovému riziku, ktoré môže byť vyvolané vystavením finančného sektora obmedzenému počtu kritických externých poskytovateľov IKT služieb, v práve Únie nerieši dostatočne. Chýbajúce pravidlá na úrovni Únie ešte zhoršuje neexistencia vnútroštátnych pravidiel týkajúcich sa mandátov a nástrojov, ktoré by orgánom dohľadu nad finančnými subjektmi umožňovali náležite pochopiť externú závislosť v oblasti IKT a primerane monitorovať riziká vyplývajúce z koncentrácie externej závislosti v oblasti IKT.

(31) Vzhľadom na potenciálne systémové riziko súvisiace so zvýšenou mierou outsourcingu a koncentráciou externých poskytovateľov IKT a so zreteľom na nedostatočnosť vnútroštátnych mechanizmov pri poskytovaní primeraných nástrojov orgánom dohľadu nad finančnými subjektmi na kvantifikovanie, kvalifikovanie a riešenie dôsledkov IKT rizika, ktoré vzniká u kritických externých poskytovateľov IKT služieb, je potrebné vytvoriť vhodný rámec dozoru, ktorý umožní nepretržité monitorovanie činností externých poskytovateľov IKT služieb, ktorí sú pre finančné subjekty kritickými poskytovateľmi, pričom sa zabezpečí zachovanie dôveryhodnosti a bezpečnosti iných zákazníkov, než sú finančné subjekty. Hoci poskytovanie IKT služieb v rámci skupiny so sebou prináša osobitné riziká a prínosy, nemalo by sa automaticky považovať za menej rizikové ako poskytovanie IKT služieb poskytovateľmi mimo finančnej skupiny, a preto by malo podliehať rovnakému regulačnému rámcu. Ak sa však IKT služby poskytujú z tej istej finančnej skupiny, finančné subjekty môžu mať vyššiu úroveň kontroly nad poskytovateľmi v rámci skupiny, čo by sa malo zohľadniť pri celkovom posúdení rizika.

(32) Keďže IKT riziko je stále zložitejšie a sofistikovanejšie, dobré opatrenia na odhaľovanie a prevenciu IKT rizika vo veľkej miere závisia od pravidelnej výmeny spravodajských informácií o hrozbách a zraniteľnosti medzi finančnými subjektmi. Výmena informácií prispieva k zvýšenej informovanosti o kybernetických hrozbách. To zase zvyšuje schopnosť finančných subjektov predchádzať tomu, aby sa kybernetické hrozby prerástli do skutočných incidentov súvisiacich s IKT, a finančným subjektom umožňuje účinnejšie obmedziť vplyv incidentov súvisiacich s IKT a rýchlejšie 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.

(33) Pochybnosti, 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), navyše vedú k tom, že sa užitočné informácie neposkytnú. Rozsah a kvalita výmeny informácií ostávajú preto v súčasnosti 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 systému. Preto je dôležité posilniť uvedené komunikačné kanály.

(34) Finančné subjekty by sa mali nabádať, aby si vzájomne vymieňali informácie a spravodajské informácie o kybernetických hrozbách, ako aj kolektívne využívali svoje individuálne znalosti a praktické skúsenosti na strategickej, taktickej a operatívnej úrovni s cieľom zlepšiť svoje spôsobilosti primerane posudzovať kybernetické hrozby, monitorovať ich, brániť sa proti nim a reagovať na ne, a to na základe účasti na dojednaniach v oblasti výmeny informácií. Na úrovni Únie je preto potrebné umožniť vytvorenie mechanizmov pre dojednania v oblasti dobrovoľnej výmeny informácií, ktoré by v prípade, že sa vykonávajú v dôveryhodnom prostredí, pomohli komunite finančného odvetvia predchádzať kybernetickým hrozbám a kolektívne na ne reagovať tak, aby sa rýchlo obmedzilo šírenie IKT rizika a aby sa zabránilo potenciálnej nákaze cez finančné kanály. Uvedené mechanizmy by mali byť v súlade s platnými pravidlami práva Únie v oblasti hospodárskej súťaže stanovenými v oznámení Komisie zo 14. januára 2011 s názvom Usmernenia o uplatňovaní článku 101 Zmluvy o fungovaní Európskej únie na dohody o horizontálnej spolupráci, ako aj s pravidlami Únie v oblasti ochrany údajov, najmä s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 ([13]). Mali by fungovať na základe použitia jedného alebo viacerých právnych základov, ktoré sú stanovené v článku 6 uvedeného nariadenia, napríklad v súvislosti so spracúvaním osobných údajov, ktoré je nevyhnutné na účely oprávneného záujmu, ktorý sleduje prevádzkovateľ alebo tretia strana, ako sa uvádza v článku 6 ods. 1 písm. f) uvedeného nariadenia, ako aj v kontexte spracúvania osobných údajov potrebného na splnenie zákonnej povinnosti, ktorej prevádzkovateľ podlieha, potrebného na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, ako sa uvádza v článku 6 ods. 1 písm. c) a e) uvedeného nariadenia.

([13]) 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).

(35) S cieľom zachovať vysokú úroveň digitálnej prevádzkovej odolnosti celého finančného sektora a zároveň držať krok s technologickým vývojom by sa v tomto nariadení malo riešiť riziko vyplývajúce zo všetkých druhov IKT služieb. Na tento účel by sa vymedzenie pojmu IKT služby v kontexte tohto nariadenia malo chápať široko a malo by zahŕňať digitálne a dátové služby poskytované prostredníctvom IKT systémov jednému alebo viacerým interným alebo externým používateľom na priebežnom základe. Uvedené vymedzenie by malo zahŕňať napríklad tzv. služby „over the top“, ktoré patria do kategórie elektronických komunikačných služieb. Mala by sa z neho vylúčiť len obmedzená kategória tradičných analógových telefónnych služieb, ktoré sa kvalifikujú ako služby verejnej prepínacej telefónnej siete (PSTN), služby pevnej linky, tradičný analógový telefónny systém (POTS) alebo telefónne služby pevnej linky.

(36) 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 ich veľkosť a celkový rizikový profil. Vo všeobecnosti platí, že pri smerovaní 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 celkovým rizikovým profilom, ako aj povahou, rozsahom a zložitosťou svojich služieb, činností a operácií, pričom príslušné orgány by mali naďalej posudzovať a preskúmavať prístup týkajúci sa takéhoto smerovania.

(37) Poskytovatelia služieb informovania o účte uvedení v článku 33 ods. 1 smernice (EÚ) 2015/2366 sú výslovne zahrnutí do rozsahu pôsobnosti tohto nariadenia, pričom sa zohľadňuje osobitná povaha ich činností a z toho vyplývajúce riziká. Okrem toho inštitúcie elektronických peňazí a platobné inštitúcie vyňaté podľa článku 9 ods. 1 smernice Európskeho parlamentu a Rady 2009/110/ES ([14]) a článku 32 ods. 1 smernice (EÚ) 2015/2366 sú zahrnuté do rozsahu pôsobnosti tohto nariadenia, aj keď im v súlade so smernicou 2009/110/ES nebolo udelené povolenie na vydávanie elektronických peňazí, alebo ak im nebolo udelené povolenie v súlade so smernicou (EÚ) 2015/2366 na poskytovanie a vykonávanie platobných služieb. Poštové žírové inštitúcie uvedené v článku 2 ods. 5 bode 3 smernice Európskeho parlamentu a Rady 2013/36/EÚ ([15]) sú však vylúčené z rozsahu pôsobnosti tohto nariadenia. Príslušným orgánom pre platobné inštitúcie vyňaté podľa smernice (EÚ) 2015/2366, inštitúcie elektronického peňažníctva vyňaté podľa smernice 2009/110/ES a poskytovateľov služieb informovania o účte uvedených v článku 33 ods. 1 smernice (EÚ) 2015/2366, by mal byť príslušný orgán určený v súlade s článkom 22 smernice (EÚ) 2015/2366.

(38) Keďže väčšie finančné subjekty môžu mať väčšie zdroje a môžu 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 dojednaniami s externými poskytovateľmi IKT služieb alebo na zvládanie krízového riadenia, na organizáciu svojho riadenia IKT rizika na základe modelu „troch línií obrany“ alebo na zavedenie modelu vnútorného riadenia rizika a kontroly a na predkladanie svojho rámca na riadenie IKT rizika vnútornému auditu.

(39) Niektoré finančné subjekty využívajú výnimky alebo podliehajú veľmi miernemu regulačnému rámcu podľa príslušného odvetvového práva Únie. Takéto finančné subjekty zahŕňajú správcov alternatívnych investičných fondov uvedených v článku 3 ods. 2 smernice Európskeho parlamentu a Rady 2011/61/EÚ ([16]), poisťovne a zaisťovne uvedené v článku 4 smernice Európskeho parlamentu a Rady 2009/138/ES ([17]) a inštitúcie zamestnaneckého dôchodkového zabezpečenia, ktoré prevádzkujú dôchodkové plány, ktoré spolu nemajú viac ako 15 členov. Vzhľadom na uvedené výnimky by nebolo primerané zahrnúť takéto finančné subjekty do rozsahu

([14]) 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).

([15]) Smernica Európskeho parlamentu a Rady 2013/36/EÚ z 26. júna 2013 o prístupe k činnosti úverových inštitúcií a prudenciálnom dohľade nad úverovými inštitúciami, o zmene smernice 2002/87/ES a o zrušení smerníc 2006/48/ES a 2006/49/ES (Ú. v. EÚ L 176, 27.6.2013, s. 338).

([16]) Smernica Európskeho parlamentu a Rady 2011/61/EÚ z 8. júna 2011 o správcoch alternatívnych investičných fondov a o zmene a doplnení smerníc 2003/41/ES a 2009/65/ES a nariadení (ES) č. 1060/2009 a (EÚ) č. 1095/2010 (Ú. v. EÚ L 174, 1.7.2011, s. 1).

([17]) Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1).

pôsobnosti tohto nariadenia. Okrem toho sa v tomto nariadení uznávajú osobitosti štruktúry trhu so sprostredkovaním poistenia, takže sprostredkovatelia poistenia, sprostredkovatelia zaistenia a sprostredkovatelia doplnkového poistenia, ktorí sa kvalifikujú ako mikropodniky alebo ako malé alebo stredné podniky, by nemali podliehať tomuto nariadeniu.

(40) Keďže subjekty uvedené v článku 2 ods. 5 bodoch 4 až 23 smernice 2013/36/EÚ sú vylúčené z rozsahu pôsobnosti uvedenej smernice, členské štáty by preto mali mať možnosť rozhodnúť sa vyňať z uplatňovania tohto nariadenia takéto subjekty nachádzajúce sa na ich príslušných územiach.

(41) Podobne s cieľom zosúladiť toto nariadenie s rozsahom pôsobnosti smernice Európskeho parlamentu a Rady 2014/65/EÚ ([18]) je takisto vhodné vylúčiť z rozsahu pôsobnosti tohto nariadenia fyzické a právnické osoby uvedené v článkoch 2 a 3 uvedenej smernice, ktorým je povolené poskytovať investičné služby bez toho, aby museli získať povolenie podľa smernice 2014/65/EÚ. V článku 2 smernice 2014/65/EÚ sa však z rozsahu pôsobnosti uvedenej smernice vylučujú aj subjekty, ktoré sa na účely tohto nariadenia kvalifikujú ako finančné subjekty, ako sú centrálne depozitáre cenných papierov, podniky kolektívneho investovania alebo poisťovne a zaisťovne. Vylúčenie z rozsahu pôsobnosti tohto nariadenia pre osoby a subjekty uvedené v článkoch 2 a 3 uvedenej smernice by sa nemalo vzťahovať na uvedené centrálne depozitáre cenných papierov, podniky kolektívneho investovania alebo poisťovne a zaisťovne.

(42) Podľa odvetvového práva Únie podliehajú niektoré finančné subjekty miernejším požiadavkám alebo výnimkám z dôvodov súvisiacich s ich veľkosťou alebo službami, ktoré poskytujú. Uvedená kategória finančných subjektov zahŕňa malé a neprepojené investičné spoločnosti, malé inštitúcie zamestnaneckého dôchodkového zabezpečenia, ktoré môžu byť vylúčené z rozsahu pôsobnosti smernice (EÚ) 2016/2341 za podmienok stanovených v článku 5 uvedenej smernice dotknutým členským štátom, a prevádzkujú dôchodkové plány, ktoré spolu nemajú celkovo viac ako 100 členov, ako aj inštitúcie vyňaté podľa smernice 2013/36/EÚ. Preto je v súlade so zásadou proporcionality a s cieľom zachovať ducha odvetvového práva Únie takisto vhodné, aby sa na tieto finančné subjekty vzťahoval zjednodušený rámec riadenia IKT rizika podľa tohto nariadenia. Primeraný charakter rámca riadenia IKT rizika vzťahujúceho sa na tieto finančné subjekty by sa nemal meniť regulačnými technickými predpismi, ktoré majú vypracovať európske orgány dohľadu. Okrem toho je v súlade so zásadou proporcionality vhodné podrobiť platobné inštitúcie, ktoré sú uvedené v článku 32 ods. 1 smernice (EÚ) 2015/2366, a inštitúcie elektronického peňažníctva, ktoré sú uvedené v článku 9 smernice 2009/110/ES, vyňaté v súlade s vnútroštátnym právom, ktorým sa transponujú tieto právne akty Únie, zjednodušenému rámcu riadenia IKT rizika podľa tohto nariadenia, zatiaľ čo platobné inštitúcie a inštitúcie elektronického peňažníctva, ktoré neboli vyňaté v súlade s ich príslušným právom, ktorým sa transponuje odvetvové právo Únie, by mali dodržiavať všeobecný rámec stanovený v tomto nariadení.

(43) Podobne by sa od finančných subjektov, ktoré sa kvalifikujú ako mikropodniky alebo podliehajú zjednodušenému rámcu riadenia IKT rizika podľa tohto nariadenia, nemalo vyžadovať, aby ustanovili funkciu monitorovania svojich dojednaní o využívaní IKT služieb uzavretých s externými poskytovateľmi IKT služieb; alebo aby určili člena vrcholového manažmentu, ktorý má byť zodpovedný za dohľad nad súvisiacou rizikovou expozíciou a za príslušnú dokumentáciu; priradili zodpovednosť za riadenie IKT rizika a dohľad nad ním osobe vykonávajúcej kontrolnú funkciu a zabezpečili primeranú úroveň nezávislosti takejto osoby vykonávajúcej kontrolnú funkciu s cieľom zabrániť konfliktom záujmu; zdokumentovali a preskúmali aspoň raz za rok rámec riadenia IKT rizika; pravidelne vykonávali vnútorný audit rámca riadenia IKT rizika; vykonávali hĺbkové posúdenia po rozsiahlych zmenách svojich infraštruktúr a procesov sietí a informačných systémov; pravidelne vykonávali analýzy rizík v súvislosti s pôvodnými IKT systémami; zabezpečovali nezávislé vnútorné audítorské preskúmania vykonávania plánov reakcie a obnovy v oblasti IKT; mali vytvorenú funkciu krízového riadenia, rozšírili testovanie kontinuity činnosti a plánov reakcie a obnovy tak, aby sa v nich zachytili scenáre prechodu medzi primárnou infraštruktúrou IKT a redundantnými zariadeniami; oznamovali príslušným orgánom na ich žiadosť odhad súhrnných ročných nákladov a strát spôsobených závažnými incidentmi súvisiacimi s IKT, udržiavali redundantné IKT kapacity; informovali vnútroštátne príslušné orgány o zmenách vykonaných na základe preskúmaní realizovaných po

([18]) Smernica Európskeho parlamentu a Rady 2014/65/EÚ z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorou sa mení smernica 2002/92/ES a smernica 2011/61/EÚ (Ú. v. EÚ L 173, 12.6.2014, s. 349).

incidentoch súvisiacich s IKT; nepretržite monitorovali relevantný technologický vývoj, vytvorili komplexný program testovania digitálnej prevádzkovej odolnosti ako neoddeliteľnú súčasť rámca riadenia IKT rizika stanoveného v tomto nariadení, alebo prijali a pravidelne preskúmavali stratégiu týkajúcu sa externého IKT rizika. Okrem toho by sa od mikropodnikov malo len vyžadovať, aby posudzovali potrebu udržiavať takéto redundantné IKT kapacity na základe svojho rizikového profilu. Mikropodniky by mali využívať flexibilnejší režim, pokiaľ ide o programy testovania digitálnej prevádzkovej odolnosti. Pri posudzovaní typu a frekvencie testovania, ktoré sa má vykonať, by mali náležite vyvážiť cieľ zachovania vysokej digitálnej prevádzkovej odolnosti, dostupné zdroje a svoj celkový rizikový profil. Mikropodniky a finančné subjekty, na ktoré sa vzťahuje zjednodušený rámec riadenia IKT rizika podľa tohto nariadenia, by mali byť oslobodené od požiadavky vykonávať pokročilé testovanie nástrojov, systémov a procesov IKT v zmysle penetračného testovania na základe konkrétnej hrozby (ďalej len „TLPT“), keďže takéto testovanie by sa malo vyžadovať len od finančných subjektov spĺňajúcich kritériá stanovené v tomto nariadení. Mikropodniky by vzhľadom na svoje obmedzené spôsobilosti mali mať možnosť dohodnúť sa s externým poskytovateľom IKT služieb na delegovaní práv finančného subjektu na prístup, inšpekciu a audit na nezávislú tretiu stranu, ktorú vymenuje externý poskytovateľ IKT služieb, za predpokladu, že finančný subjekt môže kedykoľvek požiadať príslušnú nezávislú tretiu stranu o všetky relevantné informácie a uistenie o výkonnosti externého poskytovateľa IKT služieb.

(44) Keďže len uvedené finančné subjekty identifikované 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 malo znášať malé percento finančných subjektov.

(45) 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 riadiacich orgánov finančných subjektov malo vyžadovať, aby si zachovali kľúčovú a aktívnu úlohu pri riadení a prispôsobovaní rámca riadenia IKT rizika a celkovej stratégie digitálnej prevádzkovej odolnosti. Prístup, ktorý majú riadiace orgány 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 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.

(46) Zásada úplnej a konečnej zodpovednosti riadiaceho orgánu za riadenie IKT rizika finančného subjektu navyše ide ruka v ruke s potrebou zabezpečiť určitú úroveň investícií súvisiacich s IKT a celkový rozpočet pre daný finančný subjekt, ktorý by finančnému subjektu umožnil dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti.

(47) Toto nariadenie, inšpirované najlepšími príslušnými medzinárodnými, vnútroštátnymi a odvetvovými postupmi, usmerneniami, odporúčaniami a prístupmi v oblasti riadenia kybernetického rizika, presadzuje súbor zásad, ktoré uľahčujú celkové štruktúrovanie riadenia IKT rizika. V dôsledku toho, pokiaľ hlavné spôsobilosti, ktoré finančné subjekty zaviedli s cieľom zabezpečiť rôzne funkcie v oblasti riadenia IKT rizika (identifikácia, ochrana a prevencia, odhaľovanie, reakcia a obnova, učenie a vývoj a komunikácia) stanovené v tomto nariadení, mali by naďalej voľne používať modely riadenia IKT rizika, ktoré sú rôzne vymedzené alebo kategorizované.

(48) V snahe držať krok s vývojom v oblasti kybernetických hrozieb by finančné subjekty mali udržiavať aktualizované IKT systémy, ktoré sú spoľahlivé a schopné nielen zaručiť spracúvanie údajov potrebných pre ich služby, ale aj zabezpečiť dostatočnú technologickú odolnosť, ktorá im umožní primerane riešiť dodatočné potreby v oblasti spracúvania, ktoré môžu vzniknúť v dôsledku stresových trhových podmienok alebo iných nepriaznivých situácií.

(49) Na to, aby finančné subjekty mohli promptne a rýchlo riešiť incidenty súvisiace s IKT, a najmä kybernetické útoky, sú potrebné efektívne plány kontinuity činnosti a plány obnovy, aby sa obmedzili škody a uprednostnilo obnovenie činností a opatrenia zamerané na obnovu v súlade s ich záložnými postupmi. Takéto obnovenie by však v žiadnom prípade nemalo ohroziť integritu a bezpečnosť sietí a informačných systémov ani dostupnosť, pravosť, integritu alebo dôvernosť údajov.

(50) Hoci toto nariadenie umožňuje finančným subjektom pružne určovať ich časové ciele obnovy a ciele bodov obnovy, a teda stanoviť takéto ciele tak, aby sa v plnej miere zohľadnila povaha a kritickosť príslušných funkcií a akékoľvek osobitné obchodné potreby, malo by sa v ňom napriek tomu od nich vyžadovať, aby pri určovaní takýchto cieľov vykonávali aj posúdenie potenciálneho celkového vplyvu na efektívnosť trhu.

(51) Šíritelia kybernetických útokov majú tendenciu usilovať sa o finančné zisky priamo pri zdroji, čím finančné subjekty vystavujú významným dôsledkom. S cieľom zabrániť tomu, aby IKT systémy stratili integritu alebo sa stali nedostupnými, a tým zabrániť narušeniu ochrany údajov a poškodeniu fyzickej infraštruktúry IKT, by sa malo výrazne zlepšiť a zefektívniť nahlasovanie závažných incidentov súvisiacich s IKT finančnými subjektmi. Nahlasovanie incidentov súvisiacich s IKT by sa malo harmonizovať prostredníctvom zavedenia požiadavky pre všetky finančné subjekty nahlasovať priamo ich relevantným príslušným orgánom. Ak finančný subjekt podlieha dohľadu viac ako jedného príslušného vnútroštátneho orgánu, členské štáty by mali určiť jediný príslušný orgán ako adresáta takéhoto nahlasovania. Úverové inštitúcie klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia Rady (EÚ) č. 1024/2013 ([19]) by mali takéto nahlasovanie predkladať vnútroštátnym príslušným orgánom, ktoré by následne mali správu zaslať Európskej centrálnej banke (ďalej len „ECB“).

(52) Priame nahlasovanie by malo orgánom dohľadu nad finančnými subjektmi umožniť okamžitý prístup k informáciám o závažných incidentoch súvisiacich s IKT. Orgány dohľadu nad finančnými subjektmi by mali zároveň podrobnosti o závažných incidentoch súvisiacich s IKT postúpiť verejným nefinančným orgánom (ako sú príslušné orgány a jednotné kontaktné miesta podľa smernice (EÚ) 2022/2555+, vnútroštátne orgány na ochranu údajov a v prípade závažných incidentov trestnej povahy súvisiacich s IKT orgány presadzovania práva), aby sa zvýšila informovanosť týchto orgánov o takýchto incidentoch a aby sa v prípade jednotiek CSIRT uľahčila promptná pomoc, ktorú možno poskytnúť finančným subjektom. Členské štáty by okrem toho mali mať možnosť určiť, že samotné finančné subjekty by mali poskytovať takéto informácie verejným orgánom mimo oblasti finančných služieb. Uvedené informačné toky by mali finančným subjektom umožniť rýchlo využívať všetky relevantné technické vstupy, poradenstvo o nápravných opatreniach a následné opatrenia zo strany takýchto orgánov. Informácie o závažných incidentoch súvisiacich s IKT by sa mali poskytovať spoločne: orgány dohľadu nad finančnými subjektmi by mali finančnému subjektu poskytnúť všetku potrebnú spätnú väzbu alebo usmernenia, zatiaľ čo európske orgány dohľadu by mali zdieľať anonymizované údaje o kybernetických hrozbách a zraniteľných miestach súvisiacich s incidentom s cieľom napomôcť širšej kolektívnej obrane.

(53) Aj keď by sa malo od všetkých finančných subjektov vyžadovať, aby vykonávali nahlasovanie incidentov, neočakáva sa, že táto požiadavka ich všetkých ovplyvní rovnakým spôsobom. Relevantné prahové hodnoty významnosti, ako aj lehoty pre nahlasovanie, by mali byť náležite upravené, a to v kontexte delegovaných aktov založených na regulačných technických predpisoch, ktoré majú vypracovať európske orgány dohľadu, aby zahŕňali len závažné incidenty súvisiace s IKT. Okrem toho by sa pri stanovovaní lehôt pre nahlasovacie povinnosti mali zohľadniť špecifiká finančných subjektov.

(54) V tomto nariadení by sa od úverových inštitúcií, platobných inštitúcií, poskytovateľov služieb informovania o účte a inštitúcií elektronického peňažníctva malo vyžadovať, aby oznamovali všetky prevádzkové alebo bezpečnostné incidenty súvisiace s platbami – predtým nahlasované podľa smernice (EÚ) 2015/2366 – bez ohľadu na IKT povahu incidentu.

([19]) 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).

(55) Európske orgány dohľadu by mali byť poverené posudzovaním uskutočniteľnosti a podmienok možnej centralizácie správ o incidentoch súvisiacich s IKT na úrovni Únie. Takáto centralizácia by mohla pozostávať z jednotného centra EÚ pre nahlasovanie závažných incidentov súvisiacich s IKT, ktoré by priamo dostávalo príslušné hlásenia a automaticky informovalo vnútroštátne príslušné orgány, alebo by len centralizovalo relevantné hlásenia postúpené vnútroštátnymi príslušnými orgánmi a tak plnilo koordinačnú úlohu. Európske orgány dohľadu by mali byť poverené úlohou, aby po konzultácii s ECB a agentúrou ENISA vypracovali spoločnú správu, v ktorej preskúmajú uskutočniteľnosť zriadenia jednotného centra EÚ.

(56) V snahe dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti a v súlade s relevantnými medzinárodnými normami (napr. základnými prvkami G7 pre penetračné testovanie na základe konkrétnej hrozby) a rámcami uplatňovanými v Únii, ako ja TIBER-EÚ, by finančné subjekty mali pravidelne testovať svoje IKT systémy a personál zodpovedný za IKT, 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 zohľadniť rozdiely, ktoré existujú medzi rôznymi finančnými podsektormi a v rámci nich, pokiaľ ide o úroveň pripravenosti 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 (analýzy open-source riešení), 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 (end-to-end testovanie)) až po pokročilejšie testovanie prostredníctvom TLPT. Takéto pokročilé testovanie by sa malo vyžadovať len od finančných subjektov, ktoré sú dostatočne vyspelé z hľadiska IKT na to, aby ho mohli primerane vykonať. Testovanie digitálnej prevádzkovej odolnosti vyžadované týmto nariadením by preto malo byť náročnejšie pre tie finančné subjekty, ktoré spĺňajú kritériá stanovené v tomto nariadení (napr. veľké systémové úverové inštitúcie, ktoré sú vyspelé z hľadiska IKT, burzy cenných papierov, centrálne depozitáre cenných papierov a centrálne protistrany) než pre iné finančné subjekty. Testovanie digitálnej prevádzkovej odolnosti prostredníctvom TLPT by malo byť relevantnejšie pre finančné subjekty, ktoré vykonávajú činnosť v podsektoroch hlavných finančných služieb a zohrávajú systémovú úlohu (napr. platby, bankovníctvo a zúčtovanie a vyrovnanie), a menej relevantné pre iné subsektory (napr. správcovia aktív a ratingové agentúry).

(57) Finančné subjekty, ktoré vykonávajú cezhraničné činnosti a uplatňujú si 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, ktorý by mal zahŕňať infraštruktúry IKT vo všetkých jurisdikciách, v ktorých cezhraničná finančná skupina pôsobí v rámci Únie, čím by takýmto cezhraničným finančným skupinám umožnil, aby im náklady na testovanie súvisiace s IKT vznikali len v jednej jurisdikcii.

(58) S cieľom využiť odborné znalosti, ktoré už získali určité príslušné orgány, najmä pokiaľ ide o vykonávanie rámca TIBER – EÚ, by toto nariadenie malo členským štátom umožniť, aby určili jeden verejný orgán zodpovedný za finančný sektor na vnútroštátnej úrovni za všetky záležitosti TLPT, alebo príslušným orgánom, aby v prípade, že takéto určenie neexistuje, delegovali výkon úloh súvisiacich s TLPT na iný vnútroštátny finančný príslušný orgán.

(59) Keďže sa v tomto nariadení nevyžaduje, aby finančné subjekty pokrývali všetky kritické alebo dôležité funkcie v rámci jediného penetračného testu na základe konkrétnej hrozby, finančné subjekty by mali mať možnosť určiť, ktoré a koľko kritických alebo dôležitých funkcií by sa malo zahrnúť do rozsahu takéhoto testu.

(60) Združené testovanie v zmysle tohto nariadenia – zahŕňajúce účasť viacerých finančných subjektov na TLPT a v prípade ktorého môže externý poskytovateľ IKT služieb priamo vstupovať do zmluvných dojednaní s externým testujúcim subjektom – by sa malo umožniť len vtedy, keď sa odôvodnene predpokladá, že kvalita alebo bezpečnosť služieb, ktoré poskytuje externý poskytovateľ IKT služieb zákazníkom, ktorí sú subjektmi, na ktoré sa toto nariadenie nevzťahuje, alebo dôvernosť údajov súvisiacich s takýmito službami, by boli nepriaznivo ovplyvnené. Združené testovanie by tiež malo podliehať zárukám (riadenie jedným určeným finančným subjektom, kalibrácia viacerých zúčastňujúcich sa finančných subjektov) s cieľom zabezpečiť prísny výkon testovania zúčastnených finančných subjektov, ktoré spĺňa ciele TLPT podľa tohto nariadenia.

(61) S cieľom využiť interné zdroje dostupné na podnikovej úrovni by sa týmto nariadením malo umožniť využívanie interných testovacích subjektov na účely vykonávania TLPT za predpokladu, že existuje súhlas orgánov dohľadu, nie sú žiadne konflikty záujmov a vykonáva sa pravidelné striedanie využívania interných a externých testovacích subjektov (každé tri testy), pričom sa vyžaduje, aby poskytovateľ spravodajských informácií o hrozbe v TLPT bol vo vzťahu k finančnému subjektu vždy externý. Zodpovednosť za vykonávanie TLPT by mal v plnej miere niesť finančný subjekt. Potvrdenia, ktoré poskytujú orgány, by mali byť výlučne na účely vzájomného uznávania a nemali by brániť žiadnym následným opatreniam potrebným na riešenie IKT rizika, ktorému je finančný subjekt vystavený, ani by sa nemali považovať za schválenie schopností, ktoré má finančný subjekt v oblasti riadenia a zmierňovania IKT rizika, v rámci dohľadu.

(62) Na zabezpečenie riadneho monitorovania externého IKT rizika vo finančnom sektore je potrebné stanoviť súbor pravidiel založených na zásadách s cieľom usmerňovať finančné subjekty pri monitorovaní rizika, ktoré vzniká v súvislosti s funkciami, ktoré sú zabezpečované na základe outsourcingu externými poskytovateľmi IKT služieb, najmä v prípade IKT služieb podporujúcich kritické alebo dôležité funkcie, ako aj všeobecnejšie v súvislosti so všetkými externými závislosťami v oblasti IKT.

(63) S cieľom riešiť zložitosť rôznych zdrojov IKT rizika a zároveň zohľadniť množstvo a rozmanitosť poskytovateľov technologických riešení, ktoré umožňujú bezproblémové poskytovanie finančných služieb, by sa toto nariadenie malo vzťahovať na širokú škálu externých poskytovateľov IKT služieb vrátane poskytovateľov služieb cloud computingu, softvéru, služieb analýzy údajov a poskytovateľov služieb dátových centier. Podobne, keďže finančné subjekty by mali účinne a koherentne identifikovať a riadiť všetky druhy rizík, a to aj v kontexte IKT služieb obstarávaných v rámci finančnej skupiny, malo by sa objasniť, že podniky, ktoré sú súčasťou finančnej skupiny a poskytujú IKT služby prevažne svojmu materskému podniku alebo dcérskym podnikom či pobočkám svojho materského podniku, ako aj finančné subjekty, ktoré poskytujú IKT služby iným finančným subjektom, by sa mali tiež považovať za externých poskytovateľov IKT služieb podľa tohto nariadenia. Napokon, vzhľadom na to, že vyvíjajúci sa trh s platobnými službami sa čoraz viac stáva závislým od zložitých technických riešení, a vzhľadom na nové druhy platobných služieb a riešenia súvisiace s platbami by sa účastníci ekosystému platobných služieb, ktorí poskytujú činnosti spracovania platieb alebo prevádzkujú platobné infraštruktúry, mali tiež považovať za externých poskytovateľov IKT služieb podľa tohto nariadenia s výnimkou centrálnych bánk, keď prevádzkujú platobné systémy alebo systémy vyrovnania transakcií s cennými papiermi, a verejných orgánov pri poskytovaní služieb súvisiacich s IKT v kontexte plnenia funkcií štátu.

(64) Za dodržiavanie svojich povinností podľa tohto nariadenia by mal neustále naďalej niesť plnú zodpovednosť finančný subjekt. Finančné subjekty by mali uplatňovať primeraný prístup k monitorovaniu rizík, ktoré vznikajú na úrovni externých poskytovateľov IKT služieb, a to náležitým zohľadnením povahy, rozsahu, zložitosti a významu ich závislostí súvisiacich s IKT, kritickosti alebo dôležitosti 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.

(65) Vykonávanie takéhoto monitorovania by sa malo riadiť strategickým prístupom k externému IKT riziku, ktoré by bolo formalizované tak, že riadiaci orgán finančného subjektu prijme špecializovanú stratégiu zameranú na externé IKT riziko, ktorá bude vychádzať z nepretržitého preverovania všetkých externých závislostí v oblasti IKT. S cieľom zvýšiť informovanosť orgánov dohľadu o externých závislostiach v oblasti IKT a s cieľom ďalej podporovať prácu v kontexte rámca dozoru zriadeného týmto nariadením by sa od všetkých finančných subjektov malo vyžadovať, aby viedli register informácií so všetkými zmluvnými dojednaniami o využívaní IKT služieb poskytovaných externými poskytovateľmi IKT služieb. Orgány dohľadu nad finančnými subjektmi by mali mať možnosť požiadať o úplný register alebo požiadať o jeho konkrétne časti, a tak získať dôležité informácie na širšie pochopenie závislostí finančných subjektov v oblasti IKT.

(66) Dôkladnou analýzou pred uzavretím zmluvy by sa malo podporiť formálne uzavretie zmluvných dojednaní, a to najmä zameraním sa na prvky, ako je kritickosť alebo dôležitosť služieb podporovaných plánovanou zmluvou v oblasti IKT, potrebné schválenia orgánmi dohľadu alebo iné podmienky, možné súvisiace riziko koncentrácie, ako aj uplatňovaním náležitej starostlivosti v procese výberu a posudzovania externých poskytovateľov IKT služieb a posúdením potenciálnych konfliktov záujmov. V prípade zmluvných dojednaní týkajúcich sa kritických alebo dôležitých funkcií by finančné subjekty mali zohľadňovať, ako externí poskytovatelia IKT služieb využívajú najaktuálnejšie a najprísnejšie normy informačnej bezpečnosti. Ukončenie zmluvných dojednaní by mohlo byť motivované aspoň sériou okolností, ktoré preukazujú nedostatky na úrovni externého poskytovateľa IKT služieb, najmä významné porušenia právnych predpisov alebo zmluvných podmienok, okolnosti odhaľujúce možnú zmenu

v plnení funkcií poskytovaných na základe zmluvných dojednaní, dôkazy o slabých stránkach externého poskytovateľa IKT služieb v jeho celkovom riadení IKT rizika alebo okolnosti naznačujúce neschopnosť relevantného príslušného orgánu vykonávať účinný dohľad nad finančným subjektom.

(67) S cieľom riešiť systémový vplyv rizika koncentrácie externých poskytovateľov IKT sa týmto nariadením podporuje vyvážené riešenie prostredníctvom uplatnenia flexibilného a postupného prístupu k takémuto riziku koncentrácie, keďže stanovenie akýchkoľvek pevných horných hraníc alebo prísnych obmedzení by mohlo brániť vykonávaniu obchodnej činnosti a obmedzovať zmluvnú slobodu. Finančné subjekty by mali dôkladne posúdiť svoje zamýšľané 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 zaručiť finančnú stabilitu sa nepovažuje za vhodné stanoviť prísne horné hranice a obmedzenia expozícií voči externým stranám v oblasti IKT. V súvislosti s rámcom dozoru by mal hlavný orgán dozoru vymenovaný podľa tohto nariadenia, a to vo vzťahu ku kritickým externým poskytovateľom IKT služieb, venovať osobitnú pozornosť plnému využitiu celého rozsahu vzájomných závislostí, odhaľovať konkrétne prípady, keď vysoký stupeň koncentrácie kritických externých poskytovateľov IKT služieb v Únii pravdepodobne zaťaží stabilitu a integritu finančného systému Únie, a udržiavať dialóg s kritickými externými poskytovateľmi IKT služieb, ak dôjde k identifikácii konkrétneho rizika.

(68) S cieľom pravidelne hodnotiť a monitorovať schopnosť externého poskytovateľa IKT služieb bezpečne poskytovať služby finančnému subjektu bez nepriaznivých účinkov na digitálnu prevádzkovú odolnosť finančného subjektu, by sa malo harmonizovať niekoľko kľúčových zmluvných prvkov s externými poskytovateľmi IKT služieb. Takáto harmonizácia by mala zahŕňať aspoň oblasti, ktoré sú kľúčové na to, aby finančnému subjektu umožnili úplné monitorovanie rizík, ktoré by mohol spôsobiť externý poskytovateľ IKT služieb, a to z hľadiska potreby finančného subjektu zabezpečiť svoju digitálnu odolnosť, keďže výrazne závisí od stability, funkčnosti, dostupnosti a bezpečnosti IKT služieb, ktoré sú mu poskytované.

(69) Pri opätovnom prerokovaní zmluvných dojednaní s cieľom dosiahnuť súlad s požiadavkami tohto nariadenia by finančné subjekty a externí poskytovatelia IKT služieb mali zabezpečiť pokrytie kľúčových zmluvných ustanovení, ako sa stanovuje v tomto nariadení.

(70) Vymedzenie pojmu „kritická alebo dôležitá funkcia“ stanovené v tomto nariadení zahŕňa vymedzenie pojmu „zásadné funkcie“ stanovené v článku 2 ods. 1 bode 35 smernice Európskeho parlamentu a Rady 2014/59/EÚ ([20]). Funkcie považované za zásadné podľa smernice 2014/59/EÚ sú preto zahrnuté do vymedzenia kritických funkcií v zmysle tohto nariadenia.

(71) Bez ohľadu na kritickosť alebo dôležitosť funkcie podporovanej IKT službami by zmluvné dojednania mali obsahovať najmä uvedenie úplných opisov funkcií a služieb, miest, kde sa takéto funkcie poskytujú a kde sa údaje majú spracúvať, ako aj uvedenie opisov úrovne služieb. Iné nevyhnutné prvky na to, aby finančný subjekt mohol monitorovať externé IKT riziko sú: zmluvné ustanovenia, v ktorých sa stanovuje, ako externý poskytovateľ IKT služieb zabezpečuje prístupnosť, dostupnosť, integritu, bezpečnosť a ochranu osobných údajov, ustanovenia, v ktorých sa stanovujú relevantné záruky umožňujúce prístup k údajom, ich obnovu a vrátenie v prípade platobnej neschopnosti, riešenia krízových situácií alebo ukončenia obchodných činností externého poskytovateľa IKT služieb, ako aj ustanovenia vyžadujúce, aby externý poskytovateľ IKT služieb poskytol pomoc v prípade incidentov týkajúcich sa IKT v súvislosti s poskytovanými službami, a to bez dodatočných nákladov alebo s nákladmi určenými ex-ante; ustanovenia o povinnosti externého poskytovateľa IKT služieb plne spolupracovať s príslušnými orgánmi a orgánmi pre riešenie krízových situácií finančného subjektu; a ustanovenia o práve ukončiť zmluvný vzťah

([20]) Smernica Európskeho parlamentu a Rady 2014/59/EÚ z 15. mája 2014, ktorou sa stanovuje rámec pre ozdravenie a riešenie krízových situácií úverových inštitúcií a investičných spoločností a ktorou sa mení smernica Rady 82/891/EHS a smernice Európskeho parlamentu a Rady 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EÚ, 2012/30/EÚ a 2013/36/EÚ a nariadenia Európskeho parlamentu a Rady (EÚ) č. 1093/2010 a (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 190).

a súvisiacich minimálnych výpovedných lehôt na ukončenie zmluvných dojednaní v súlade s očakávaniami príslušných orgánov a orgánov pre riešenie krízových situácií.

(72) Okrem takýchto zmluvných ustanovení a s cieľom zabezpečiť, aby si finančné subjekty zachovali plnú kontrolu nad všetkými možnosťami vývoja na úrovni externého subjektu, ktorý môže narušiť ich bezpečnosť IKT, by zmluvy o poskytovaní IKT služieb podporujúcich kritické alebo dôležité funkcie mali tiež obsahovať: uvedenie úplného opisu úrovne poskytovaných služieb vrátane presných kvantitatívnych a kvalitatívnych výkonnostných cieľov, s cieľom umožniť bezodkladné prijatie vhodných nápravných opatrení, ak sa dohodnutá úroveň poskytovaných služieb nedosahuje; príslušné výpovedné lehoty a nahlasovacie povinnosti externého poskytovateľa IKT služieb v prípade vývoja, ktorý môže mať potenciálne významný vplyv na schopnosť externého poskytovateľa IKT služieb účinne poskytovať svoje príslušné IKT služby; požiadavku, aby externý poskytovateľ IKT služieb vykonával a testoval pohotovostné plány obchodnej činnosti a aby mal k dispozícii bezpečnostné opatrenia, nástroje a politiky v oblasti IKT, ktoré umožňujú bezpečné poskytovanie služieb, a aby sa zúčastňoval a plne spolupracoval na TLPT, ktorý vykonáva finančný subjekt.

(73) Zmluvy o poskytovaní IKT služieb podporujúcich kritické alebo dôležité funkcie by mali obsahovať aj ustanovenia poskytujúce finančnému subjektu alebo určenému externému subjektu práva na prístup, inšpekciu a audit, ako aj právo vyhotovovať kópie, ako kľúčové nástroje pri priebežnom monitorovaní výkonnosti externého poskytovateľa IKT služieb zo strany finančného subjektu, spolu s úplnou spoluprácou poskytovateľa služieb počas inšpekcií. Podobne by sa príslušnému orgánu finančného subjektu malo na základe oznámení udeliť právo na inšpekciu a audit externého poskytovateľa IKT služieb, a to pod podmienkou ochrany dôverných informácií.

(74) V takýchto zmluvných dojednaniach by sa mali stanoviť aj osobitné stratégie ukončenia angažovanosti umožňujúce najmä povinné prechodné obdobia, počas ktorých by externí poskytovatelia IKT služieb mali naďalej poskytovať príslušné služby s cieľom znížiť riziko narušení na úrovni finančného subjektu alebo umožniť tomuto subjektu účinne prejsť k využívaniu iných externých poskytovateľov IKT služieb, alebo alternatívne začať využívať vlastné riešenia v závislosti od zložitosti poskytovanej IKT služby. Okrem toho by finančné subjekty patriace do rozsahu pôsobnosti smernice 2014/59/EÚ mali zabezpečiť, aby príslušné zmluvy o IKT službách boli spoľahlivé a plne vynútiteľné v prípade riešenia krízových situácií týchto finančných subjektov. V súlade s očakávaniami orgánov pre riešenie krízových situácií by tieto finančné subjekty mali zabezpečiť, aby príslušné zmluvy o IKT službách boli odolné voči krízovým situáciám. Pokiaľ tieto finančné subjekty naďalej plnia svoje platobné záväzky, mali by okrem iných požiadaviek zabezpečiť, aby príslušné zmluvy o IKT službách obsahovali doložky o nevypovedaní, nepozastavení a nezmenení z dôvodu reštrukturalizácie alebo riešenia krízových situácií.

(75) Dobrovoľné používanie štandardných zmluvných doložiek vypracovaných verejnými orgánmi alebo inštitúciami Únie, najmä používanie zmluvných doložiek vypracovaných Komisiou pre služby cloud computingu by mohlo navyše finančné subjekty a externých poskytovateľov IKT služieb ešte viac odbremeniť, a to zvýšením ich úrovne právnej istoty, pokiaľ ide o využívanie služieb cloud computingu vo finančnom sektore, v plnom súlade s požiadavkami a očakávaniami stanovenými v práve Únie v oblasti finančných služieb. Vypracovanie štandardných zmluvných doložiek 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 služieb cloud computingu formou outsourcingu finančnými subjektmi, a to na základe medziodvetvového úsilia zainteresovaných strán v oblasti služieb cloud computingu, ktoré Komisia uľahčila zapojením finančného sektora.

(76) S cieľom podporiť konvergenciu a efektívnosť, pokiaľ ide o prístupy dohľadu pri riešení externého IKT rizika vo finančnom sektore, ako aj posilniť digitálnu prevádzkovú odolnosť finančných subjektov, ktoré sa v súvislosti s poskytovaním IKT služieb podporujúcimi poskytovanie finančných služieb spoliehajú na kritických externých poskytovateľov IKT služieb, a tým prispieť k zachovaniu stability finančného systému Únie a integrity vnútorného trhu s finančnými službami, by sa na kritických externých poskytovateľov IKT služieb mal vzťahovať rámec dozoru

Únie. Hoci je vytvorenie rámca dozoru odôvodnené pridanou hodnotou prijatia opatrení na úrovni Únie a prirodzenou úlohou a osobitosťami využívania IKT služieb pri poskytovaní finančných služieb, zároveň by sa malo pripomenúť, že toto riešenie sa zdá vhodné len v kontexte tohto nariadenia, ktoré sa špecificky zaoberá digitálnou prevádzkovou odolnosťou finančného sektora. Takýto rámec dozoru by sa však nemal považovať za nový model dohľadu Únie v iných oblastiach finančných služieb a činností.

(77) Rámec dozoru by sa mal uplatňovať len na kritických externých poskytovateľov IKT služieb. Mal by preto existovať mechanizmus určenia, ktorý zohľadní rozmer a povahu spoliehania sa finančného sektora na takýchto externých poskytovateľov IKT služieb. Uvedený mechanizmus by mal zahŕňať súbor kvantitatívnych a kvalitatívnych kritérií na stanovenie parametrov kritickosti ako základu pre začlenenie do rámca dozoru. S cieľom zabezpečiť presnosť tohto posúdenia a bez ohľadu na podnikovú štruktúru externého poskytovateľa IKT služieb by takéto kritériá v prípade externého poskytovateľa IKT služieb, ktorý je súčasťou širšej skupiny, mali zohľadňovať celú skupinovú štruktúru externého poskytovateľa IKT služieb. Na jednej strane kritickí externí poskytovatelia IKT služieb, ktorí nie sú automaticky označení na základe uplatňovania uvedených kritérií, by mali mať možnosť zapojiť sa na dobrovoľnom základe **do** rámca dozoru, na strane druhej tí externí poskytovatelia IKT služieb, na ktorých sa už vzťahujú rámce mechanizmov dozoru podporujúce plnenie úloh Európskeho systému centrálnych bánk, ako sa uvádza v článku 127 ods. 2 ZFEÚ, by sa mali z rámca vyňať.

(78) Podobne by sa z rámca dozoru mali vyňať aj finančné subjekty, ktoré poskytujú IKT služby iným finančným subjektom, hoci patria do kategórie externých poskytovateľov IKT služieb podľa tohto nariadenia, keďže už podliehajú mechanizmom dohľadu stanoveným v príslušnom práve Únie v oblasti finančných služieb. V príslušných prípadoch by príslušné orgány mali v kontexte svojich činností dohľadu zohľadniť IKT riziko, ktoré pre finančné subjekty predstavujú finančné subjekty poskytujúce IKT služby. Podobne by sa vzhľadom na existujúce mechanizmy monitorovania rizík na úrovni skupiny mala zaviesť rovnaká výnimka pre externých poskytovateľov IKT služieb, ktorí poskytujú služby prevažne subjektom svojej vlastnej skupiny. Externí poskytovatelia IKT služieb, ktorí poskytujú IKT služby výlučne v jednom členskom štáte finančným subjektom, ktoré pôsobia len v tomto členskom štáte, by mali byť takisto vyňatí z mechanizmu určenia z dôvodu ich obmedzených činností a nedostatočného cezhraničného vplyvu.

(79) Digitálna transformácia v oblasti finančných služieb priniesla bezprecedentnú úroveň využívania IKT služieb a spoliehania sa na ne. Keďže poskytovanie finančných služieb bez využívania služieb cloud computingu, softvérových riešení a služieb súvisiacich s údajmi sa stalo nemysliteľným, finančný ekosystém Únie sa stal vo svojej podstate spoluzávislým od určitých IKT služieb poskytovaných poskytovateľmi IKT služieb. Niektorí z týchto dodávateľov, inovátorov pri vývoji a uplatňovaní technológií založených na IKT, zohrávajú významnú úlohu pri poskytovaní finančných služieb alebo sa stali súčasťou hodnotového reťazca finančných služieb. Nadobudli tak kritické postavenie z hľadiska stability a integrity finančného systému Únie. Toto rozsiahle spoliehanie sa na služby poskytované kritickými externými poskytovateľmi IKT služieb v kombinácii so vzájomnou závislosťou informačných systémov rôznych organizátorov trhu vytvára priame a potenciálne závažné riziko pre systém finančných služieb Únie a pre kontinuitu poskytovania finančných služieb, ak by kritickí externí poskytovatelia IKT služieb boli ovplyvnení prevádzkovými narušeniami alebo závažnými kybernetickými incidentmi. Kybernetické incidenty majú jedinečnú schopnosť znásobiť a šíriť sa v celom finančnom systéme výrazne rýchlejším tempom než iné druhy rizík monitorované vo finančnom sektore a môžu sa rozšíriť naprieč sektormi a za geografickými hranicami. Majú potenciál vyvinúť sa v systémovú krízu, v ktorej sa narušila dôvera vo finančný systém v dôsledku narušenia funkcií podporujúcich reálnu ekonomiku alebo značných finančných strát, ktoré dosahujú úroveň, ktorú finančný systém nie je schopný zvládnuť, alebo ktorá si vyžaduje zavedenie rozsiahlych opatrení na absorpciu otrasov. S cieľom zabrániť vzniku týchto scenárov, a tým ohroziť finančnú stabilitu a integritu Únie, je nevyhnutné zabezpečiť konvergenciu postupov dohľadu týkajúcich sa externého IKT rizika v oblasti financií, a to najmä prostredníctvom nových pravidiel umožňujúcich dohľad Únie nad kritickými externými poskytovateľmi IKT služieb.

(80) Rámec dozoru vo veľkej miere závisí od stupňa spolupráce medzi hlavným orgánom dozoru a kritickým externým poskytovateľom IKT služieb, ktorý finančným subjektom poskytuje služby ovplyvňujúce poskytovanie finančných služieb. Úspešný dozor je okrem iného založený na schopnosti hlavného orgánu dozoru účinne vykonávať monitorovacie misie a inšpekcie s cieľom posúdiť pravidlá, kontroly a procesy, ktoré používajú kritickí externí poskytovatelia IKT služieb, ako aj posúdiť potenciálny kumulatívny vplyv ich činností na finančnú stabilitu a integritu finančného systému. Zároveň je veľmi dôležité, aby kritickí externí poskytovatelia IKT služieb dodržiavali odporúčania hlavného orgánu dozoru a riešili jeho obavy. Keďže nedostatočná spolupráca zo strany kritického externého poskytovateľa IKT služieb, ktorý poskytuje služby, ktoré majú vplyv na poskytovanie finančných služieb, ako je odmietnutie udeliť prístup do jeho priestorov alebo predložiť informácie, by v konečnom dôsledku zbavila hlavného orgánu dozoru jeho základných nástrojov na hodnotenie externého IKT rizika a mohla by mať nepriaznivý vplyv na finančnú stabilitu a integritu finančného systému, je potrebné stanoviť aj primeraný sankčný režim.

(81) V tejto súvislosti by nemala byť ohrozená potreba hlavného orgánu dozoru ukladať sankcie s cieľom prinútiť kritických externých poskytovateľov IKT služieb, aby dodržiavali povinnosti týkajúce sa transparentnosti a prístupu stanovené v tomto nariadení, a to ťažkosťami vyvolanými vymáhaním uvedených sankcií v súvislosti s kritickými externými poskytovateľmi IKT služieb usadenými v tretích krajinách. S cieľom zabezpečiť vykonateľnosť takýchto sankcií a umožniť rýchle uplatnenie postupov na dodržiavanie práva kritických externých poskytovateľov IKT služieb na obhajobu v kontexte mechanizmu určenia a vydávania odporúčaní by sa od uvedených kritických externých poskytovateľov IKT služieb, ktorí poskytujú finančným subjektom služby ovplyvňujúce poskytovanie finančných služieb, malo vyžadovať, aby si zachovali primeranú obchodnú prítomnosť v Únii. Vzhľadom na povahu dozoru a neexistenciu porovnateľných dojednaní v iných jurisdikciách neexistujú žiadne vhodné alternatívne mechanizmy na zabezpečenie tohto cieľa prostredníctvom účinnej spolupráce s orgánmi dohľadu nad finančnými subjektmi v tretích krajinách v súvislosti s monitorovaním vplyvu digitálnych prevádzkových rizík, ktoré predstavujú externí systémoví poskytovatelia IKT služieb, ktorí sa kvalifikujú ako kritickí externí poskytovatelia IKT služieb usadení v tretích krajinách. S cieľom naďalej poskytovať svoje IKT služby finančným subjektom v Únii by preto externý poskytovateľ IKT služieb usadený v tretej krajine, ktorý bol určený ako kritický v súlade s týmto nariadením, mal do 12 mesiacov od takéhoto určenia prijať všetky potrebné opatrenia s cieľom zabezpečiť svoju registráciu v Únii prostredníctvom založenia dcérskeho podniku, ako sa vymedzuje v *acquis* Únie, konkrétne v smernici Európskeho parlamentu a Rady 2013/34/EÚ ([21]).

(82) Požiadavka založiť dcérsky podnik v Únii by nemala brániť kritickému externému poskytovateľovi IKT služieb v poskytovaní IKT služieb a súvisiacej technickej podpory zo zariadení a infraštruktúry, ktoré sa nachádzajú mimo Únie. Týmto nariadením sa neukladá povinnosť lokalizácie údajov, keďže sa v ňom nevyžaduje, aby sa údaje uchovávali alebo spracúvali v Únii.

(83) Kritickí externí poskytovatelia IKT služieb by mali byť schopní poskytovať IKT služby z akéhokoľvek miesta na svete, nie nevyhnutne alebo nielen z priestorov nachádzajúcich sa v Únii. Činnosti dozoru by sa mali najprv vykonávať v priestoroch nachádzajúcich sa v Únii a prostredníctvom interakcie so subjektmi nachádzajúcimi sa v Únii vrátane dcérskych podnikov založených kritickými externými poskytovateľmi IKT služieb podľa tohto nariadenia. Takéto opatrenia v rámci Únie by však nemuseli byť dostatočné na to, aby hlavnému orgánu dozoru umožnili v plnej miere a účinne vykonávať svoje povinnosti podľa tohto nariadenia. Hlavný orgán dozoru by preto mal mať možnosť vykonávať svoje príslušné právomoci dozoru aj v tretích krajinách. Vykonávanie uvedených právomocí v tretích krajinách by malo umožniť hlavnému orgánu dozoru preskúmať zariadenia, z ktorých IKT služby alebo služby technickej podpory skutočne poskytuje alebo riadi kritický externý poskytovateľ IKT služieb, a hlavnému orgánu dozoru by malo poskytnúť komplexné a operatívne pochopenie riadenia IKT rizika kritického externého poskytovateľa IKT služieb. Možnosť hlavného orgánu dozoru ako agentúry Únie vykonávať právomoci mimo územia Únie by mala byť riadne vymedzená príslušnými podmienkami, najmä súhlasom dotknutého kritického externého poskytovateľa IKT služieb. Podobne by mali byť relevantné orgány tretej krajiny informované o vykonávaní činností hlavného orgánu dozoru na svojom vlastnom území a nemali by proti nemu namietať.

([21]) Smernica Európskeho parlamentu a Rady 2013/34/EÚ z 26. júna 2013 o ročných účtovných závierkach, konsolidovaných účtovných závierkach a súvisiacich správach určitých druhov podnikov, ktorou sa mení smernica Európskeho parlamentu a Rady 2006/43/ES a zrušujú smernice Rady 78/660/EHS a 83/349/EHS (Ú. v. EÚ L 182, 29.6.2013, s. 19).

S cieľom zabezpečiť účinné vykonávanie a bez toho, aby boli dotknuté príslušné právomoci inštitúcií Únie a členských štátov, však takéto právomoci musia byť plne zakotvené aj v uzavretých dohodách o administratívnej spolupráci s relevantnými orgánmi dotknutej tretej krajiny. Toto nariadenie by preto malo európskym orgánom dohľadu umožniť uzatvárať dohody o administratívnej spolupráci s relevantnými orgánmi tretích krajín, ktoré by inak nemali vytvárať právne záväzky vo vzťahu k Únii a jej členským štátom.

(84) S cieľom uľahčiť komunikáciu s hlavným orgánom dozoru a zabezpečiť primerané zastúpenie by kritickí externí poskytovatelia IKT služieb, ktorí sú súčasťou skupiny, mali ako svoje koordinačné miesto určiť jednu právnickú osobu.

(85) Rámcom dozoru by nemala byť dotknutá právomoc členských štátov vykonávať vlastné dozorné alebo monitorovacie úlohy v súvislosti s externými poskytovateľmi IKT služieb, ktorí nie sú určení ako kritickí podľa tohto nariadenia, ale ktorí by sa mohli považovať za dôležitých na vnútroštátnej úrovni.

(86) V snahe využiť 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. Mal by ho podporovať nový podvýbor (ďalej len „fórum pre dozor“), ktorý bude vykonávať prípravné práce pre jednotlivé rozhodnutia určené kritickým externým poskytovateľom IKT služieb, ako aj pre vydávanie kolektívnych odporúčaní, najmä v súvislosti s referenčným porovnávaním programov dozoru pre kritických externých poskytovateľov IKT služieb, a identifikovať najlepšie postupy na riešenie rizika koncentrácie IKT.

(87) S cieľom zabezpečiť, aby kritickí externí poskytovatelia IKT služieb podliehali náležitému a účinnému dozoru na úrovni Únie sa v tomto nariadení stanovuje, že ktorýkoľvek z troch európskych orgánov dohľadu by sa mohol určiť ako hlavný orgán dozoru. Individuálne pridelenie kritického externého poskytovateľa IKT služieb jednému z troch európskych orgánov dohľadu by malo vyplývať z posúdenia prevahy finančných subjektov pôsobiacich vo finančných sektoroch, za ktoré má daný európsky orgán dohľadu zodpovednosť. Tento prístup by mal viesť k vyváženému rozdeleniu úloh a zodpovedností medzi tri európske orgány dohľadu v kontexte vykonávania funkcií dozoru a mal by čo najlepšie využívať ľudské zdroje a technické odborné znalosti dostupné v každom z troch európskych orgánov dohľadu.

(88) Hlavným orgánom dozoru by sa mali udeliť právomoci nevyhnutné na vykonávanie vyšetrovaní, inšpekcií na mieste i na diaľku v priestoroch a lokalitách kritických externých poskytovateľov IKT služieb a na získavanie úplných a aktualizovaných informácií. Uvedené právomoci by mali umožniť hlavnému orgánu dozoru získať skutočný prehľad o druhu, rozmere a vplyve externého IKT rizika pre finančné subjekty a v konečnom dôsledku pre finančný systém Únie. Poverenie európskych orgánov dohľadu úlohou hlavného orgánu dozoru je predpokladom na pochopenie a riešenie systémového rozmeru IKT rizika v oblasti financií. Vplyv kritických externých poskytovateľov IKT služieb na finančný sektor Únie a potenciálne problémy spôsobené súvisiacim rizikom koncentrácie IKT si vyžadujú prijatie kolektívneho prístupu na úrovni Únie. Súbežné vykonávanie viacerých auditov a prístupových práv realizované zo strany viacerých samostatných príslušných orgánov pri malej alebo žiadnej vzájomnej koordinácii by orgánom dohľadu nad finančnými subjektmi bránilo získať úplný a komplexný prehľad o externom IKT riziku v Únii, a zároveň by sa vytvorila redundancia, zaťaženie a zložitosť pre kritických externých poskytovateľov IKT služieb, ak by boli vystavení početným žiadostiam o monitorovanie a inšpekciu.

(89) Vzhľadom na významné dôsledky určenia kritickosti by sa týmto nariadením malo zabezpečiť, aby sa práva kritických externých poskytovateľov IKT služieb dodržiavali počas celého vykonávania rámca dozoru. Pred určením kritickosti by takíto poskytovatelia mali napríklad mať právo predložiť hlavnému orgánu dozoru odôvodnené vyhlásenie obsahujúce všetky relevantné informácie na účely posúdenia týkajúceho sa ich určenia. Keďže hlavný orgán dozoru by mal byť oprávnený predkladať odporúčania týkajúce sa problematiky IKT rizika a vhodných s tým súvisiacich nápravných opatrení vrátane právomoci namietať proti určitým zmluvným dojednaniam, ktoré v konečnom dôsledku ovplyvňujú stabilitu finančného subjektu alebo finančného systému, kritickí externí poskytovatelia IKT služieb by tiež mali dostať možnosť poskytnúť pred finalizáciou uvedených odporúčaní vysvetlenia týkajúce sa očakávaného vplyvu riešení, ktoré sú plánované v odporúčaniach, na zákazníkov, ktorí sú

subjektmi mimo rozsahu pôsobnosti tohto nariadenia, a sformulovať riešenia na zmiernenie rizík. Kritickí externí poskytovatelia IKT služieb, ktorí nesúhlasia s odporúčaniami, by mali predložiť odôvodnené vysvetlenie svojho zámeru nepodporiť odporúčanie. Ak takéto odôvodnené vysvetlenie nie je predložené alebo sa považuje za nedostatočné, hlavný orgán dozoru by mal vydať verejné oznámenie, v ktorom stručne opíše záležitosť nesúladu.

(90) Príslušné orgány by mali do svojich funkcií v súvislosti s prudenciálnym dohľadom nad finančnými subjektmi náležite zahrnúť úlohu overovania vecného dodržiavania odporúčaní vydaných hlavným orgánom dozoru. Príslušné orgány by mali mať možnosť požadovať od finančných subjektov, aby prijali dodatočné opatrenia na riešenie rizík identifikovaných v odporúčaniach hlavného orgánu dozoru, a vo vhodnom čase by na tento účel mali vydávať oznámenia. Ak hlavný orgán dozoru adresuje odporúčania kritickým externým poskytovateľom IKT služieb, nad ktorými sa vykonáva dohľad podľa smernice (EÚ) 2022/2555+, príslušné orgány by mali mať možnosť na dobrovoľnom základe a pred prijatím dodatočných opatrení konzultovať s príslušnými orgánmi podľa uvedenej smernice s cieľom podporiť koordinovaný prístup vo vzťahu k dotknutým kritickým externým poskytovateľom IKT služieb.

(91) Vykonávanie dozoru by sa malo riadiť tromi operatívnymi zásadami, ktorých cieľom je zabezpečiť: a) úzku koordináciu medzi európskymi orgánmi dohľadu v ich úlohách hlavných orgánov dozoru prostredníctvom spoločnej siete dozoru, b) súlad s rámcom stanoveným smernicou (EÚ) 2022/2555+ (prostredníctvom dobrovoľnej konzultácie s orgánmi podľa uvedenej smernice s cieľom zabrániť duplicite opatrení zameraných na kritických externých poskytovateľov IKT služieb) a c) uplatňovanie náležitej starostlivosti s cieľom minimalizovať potenciálne riziko narušenia služieb, ktoré poskytujú kritickí externí poskytovatelia IKT služieb zákazníkom, ktorí sú subjektmi mimo rozsahu pôsobnosti tohto nariadenia.

(92) Rámec dozoru by nemal nahrádzať ani žiadnym spôsobom a ani čiastočne suplovať požiadavku na finančné subjekty, aby sami riadili riziká súvisiace s využívaním externých poskytovateľov IKT služieb vrátane ich povinnosti zachovávať priebežné monitorovanie zmluvných dojednaní uzavretých s kritickými externými poskytovateľmi IKT služieb. Podobne by rámec dozoru nemal mať vplyv na plnú zodpovednosť finančných subjektov za dodržiavanie a plnenie všetkých právnych povinností stanovených v tomto nariadení a v príslušnom práve v oblasti finančných služieb.

(93) Aby sa predišlo duplicite a prekrývaniu, príslušné orgány by sa mali zdržať individuálneho prijímania akýchkoľvek opatrení zameraných na monitorovanie rizík súvisiacich s kritickými externými poskytovateľmi IKT služieb a v tejto súvislosti by sa mali spoliehať na posúdenie hlavného dozorného orgánu. Akékoľvek opatrenia by sa mali *v* každom prípade koordinovať a dohodnúť vopred *s* hlavným dozorným orgánom v kontexte výkonu úloh v rámci dozoru.

(94) V snahe podporiť na medzinárodnej úrovni zbližovanie, pokiaľ ide o používanie najlepších postupov pri preskúmavaní a monitorovaní 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 relevantnými orgánmi dohľadu a regulačnými orgánmi tretích krajín.

(95) S cieľom využiť osobitné kompetencie, technické zručnosti a odborné znalosti pracovníkov špecializujúcich sa na prevádzkové riziká a IKT riziko v rámci príslušných orgánov, troch európskych orgánov dohľadu, a na dobrovoľnom základe príslušných orgánov podľa smernice (EÚ) 2022/2555+, hlavný orgán dozoru by mal vychádzať zo spôsobilostí a znalostí vnútroštátneho dohľadu a mal by vytvoriť špecializované prieskumné tímy pre každého kritického externého poskytovateľa IKT služieb, v ktorých by sa združili multidisciplinárne tímy na podporu prípravy a vykonávania činností dozoru vrátane všeobecných vyšetrovaní a inšpekcií na mieste u kritických externých poskytovateľov IKT služieb, ako aj akýchkoľvek potrebných následných opatrení.

(96) Zatiaľ čo náklady vyplývajúce z úloh dozoru by sa v plnej miere financovali z poplatkov vyberaných od kritických externých poskytovateľov IKT služieb, európskym orgánom dohľadu pred začatím fungovania rámca dozoru pravdepodobne vzniknú náklady na zavedenie špecializovaných IKT systémov podporujúcich nadchádzajúci dozor, keďže špecializované IKT systémy by sa museli vyvinúť a zaviesť vopred. V tomto nariadení sa preto stanovuje hybridný model financovania, na základe ktorého by bol rámec dozoru ako taký plne financovaný z poplatkov, zatiaľ čo vývoj systémov IKT európskych orgánov dohľadu by sa financoval z príspevkov Únie a príslušných vnútroštátnych orgánov.

(97) Príslušné orgány by mali mať všetky potrebné právomoci v oblasti dohľadu, vyšetrovania a ukladania sankcií na zabezpečenie riadneho výkonu ich funkcií podľa tohto nariadenia. Mali by v zásade uverejňovať informácie o administratívnych sankciách, ktoré uložili. Keďže finančné subjekty a externí poskytovatelia IKT služieb môžu byť usadení v rôznych členských štátoch a môžu podliehať dohľadu rôznych príslušných orgánov, uplatňovanie tohto nariadenia by mala uľahčovať na jednej strane 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. 1024/201339, a na strane druhej konzultácia s európskymi orgánmi dohľadu prostredníctvom vzájomnej výmeny informácií a poskytovania pomoci v kontexte relevantných činností dohľadu.

(98) S cieľom bližšie kvantifikovať a kvalifikovať kritériá určovania externých poskytovateľov IKT služieb ako kritických a harmonizovať poplatky za dozor by sa mala na Komisiu delegovať právomoc prijímať akty v súlade s článkom 290 ZFEÚ s cieľom doplniť toto nariadenie tým, že sa bližšie určí systémový vplyv, ktorý by zlyhanie alebo výpadok prevádzky externého poskytovateľa IKT služieb mohol mať na finančné subjekty, ktorým poskytuje IKT služby, 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 danom trhu, náklady na prenos údajov a pracovnej záťaže v oblasti IKT na iných externých poskytovateľov 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 ([22]). Predovšetkým v záujme rovnakého zastúpenia pri príprave delegovaných aktov by sa všetky dokumenty mali Európskemu parlamentu a Rade doručovať v rovnakom čase ako expertom z členských štátov, a experti Európskeho parlamentu a Rady by mali mať systematicky prístup na zasadnutia skupín expertov Komisie, ktoré sa zaoberajú prípravou delegovaných aktov.

(99) Konzistentná harmonizácia požiadaviek stanovených v tomto nariadení by mala byť zabezpečená regulačnými technickými predpismi. Európske orgány dohľadu by v úlohe orgánov disponujúcich vysoko špecializovanými odbornými znalosťami mali vypracovať 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, nahlasovania závažných incidentov súvisiacich s IKT, testovania, ako aj vo vzťahu ku kľúčovým požiadavkám na riadne monitorovanie externého IKT rizika. Komisia a európske orgány dohľadu by mali zabezpečiť, aby uvedené predpisy a požiadavky mohli všetky finančné subjekty uplatňovať spôsobom, ktorý je primeraný ich veľkosti a celkovému rizikovému profilu, ako aj povahe, rozsahu a zložitosti ich služieb, činností a operácií. Komisia by mala byť splnomocnená prijať uvedené regulačné technické predpisy prostredníctvom delegovaných aktov podľa článku 290 ZFEÚ a v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

(100) S cieľom uľahčiť porovnateľnosť hlásení o závažných incidentoch súvisiacich s IKT a závažných prevádzkových alebo bezpečnostných incidentoch súvisiacich s platbami, ako aj zabezpečiť transparentnosť zmluvných dojednaní o využívaní IKT služieb poskytovaných externými poskytovateľmi IKT služieb by európske orgány dohľadu mali vypracovať návrh vykonávacích technických predpisov, ktorými sa stanovia štandardizované vzory, formuláre a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a závažných prevádzkových alebo bezpečnostných incidentoch súvisiacich s platbami, ako aj štandardizované vzory registra informácií. Pri vypracúvaní uvedených predpisov by európske orgány dohľadu mali zohľadniť veľkosť a celkový rizikový profil finančného subjektu, ako aj povahu, rozsah a zložitosť ich služieb, činností a operácií. 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.

([22]) Ú. v. EÚ L 123, 12.5.2016, s. 1.

(101) Keďže bližšie požiadavky už boli stanovené prostredníctvom delegovaných a vykonávacích aktov založených na regulačných technických a vykonávacích technických predpisoch v nariadeniach Európskeho parlamentu a Rady (ES) č. 1060/2009 ([23]), (EÚ) č. 648/2012 ([24]), (EÚ) č. 600/2014 ([25]) a (EÚ) č. 909/2014 ([26]), 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.

(102) Keďže toto nariadenie spolu so smernicou Európskeho parlamentu a Rady (EÚ) 2022/2556+ ([27]) zahŕňa konsolidáciu ustanovení o riadení IKT rizika naprieč viacerými nariadeniami a smernicami *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 a nariadení (EÚ) 2016/1011 ([28]), s cieľom zabezpečiť úplný súlad by sa uvedené nariadenia mali zmeniť tak, aby sa v nich objasnilo, že príslušné ustanovenia týkajúce sa IKT rizika sú stanovené v tomto nariadení.

(103) Rozsah pôsobnosti relevantných článkov súvisiacich s prevádzkovým rizikom, na základe ktorých splnomocnenia v nariadeniach (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 viedli k prijatiu delegovaných a vykonávacích aktov, by sa mal preto zúžiť s cieľom preniesť do tohto nariadenia všetky ustanovenia týkajúce sa aspektov digitálnej prevádzkovej odolnosti, ktoré sú dnes súčasťou uvedených nariadení.

(104) Potenciálne systémové kybernetické riziko spojené s využívaním infraštruktúr IKT, ktoré umožňujú prevádzku platobných systémov a poskytovanie činností spracovania platieb, by sa malo náležite riešiť na úrovni Únie prostredníctvom harmonizovaných pravidiel digitálnej odolnosti. Na tento účel by Komisia mala urýchlene posúdiť potrebu preskúmania rozsahu pôsobnosti tohto nariadenia a zároveň zosúladiť takéto preskúmanie s výsledkom komplexného preskúmania stanoveného v smernici (EÚ) 2015/2366. Početné rozsiahle útoky za posledné desaťročie ukazujú, ako sa platobné systémy stali vystavené kybernetickým hrozbám. Postavenie v centre reťazca platobných služieb a preukázanie silných prepojení s celkovým finančným systémom, platobnými systémami a činnosťami spracovania platieb nadobudli rozhodujúci význam pre fungovanie finančných trhov Únie. Kybernetické útoky na takéto systémy môžu spôsobiť vážne narušenia prevádzky s priamymi dôsledkami pre kľúčové hospodárske funkcie, ako je uľahčovanie platieb, a nepriame účinky na súvisiace hospodárske procesy. Kým sa na úrovni Únie nezavedie harmonizovaný režim a dohľad nad prevádzkovateľmi platobných systémov a spracovateľskými subjektmi, členské štáty sa môžu pri uplatňovaní pravidiel na prevádzkovateľov platobných systémov a spracovateľské subjekty, nad ktorými vykonávajú dohľad v rámci svojej vlastnej jurisdikcie, inšpirovať požiadavkami na digitálnu prevádzkovú odolnosť stanovenými v tomto nariadení s cieľom uplatňovať podobné trhové postupy.

([23]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1060/2009 zo 16. septembra 2009 o ratingových agentúrach (Ú. v. EÚ L 302, 17.11.2009, s. 1).

([24]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 zo 4. júla 2012 o mimoburzových derivátoch, centrálnych protistranách a archívoch obchodných údajov (Ú. v. EÚ L 201, 27.7.2012, s. 1).

([25]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 600/2014 z 15. mája 2014 o trhoch s finančnými nástrojmi, ktorým sa mení nariadenie (EÚ) č. 648/2012 (Ú. v. EÚ L 173, 12.6.2014, s. 84).

([26]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 909/2014 z 23. júla 2014 o zlepšení vyrovnania transakcií s cennými papiermi v Európskej únii, centrálnych depozitároch cenných papierov a o zmene smerníc 98/26/ES a 2014/65/EÚ a nariadenia (EÚ) č. 236/2012 (Ú. v. EÚ L 257, 28.8.2014, s. 1).

([27]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2556+ zo 14. decembra 2022, ktorou sa menia smernice 2009/65/ES, 2009/138/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/59/EÚ, 2014/65/EÚ, (EÚ) 2015/2366 a (EÚ) 2016/2341, pokiaľ ide o digitálnu prevádzkovú odolnosť finančného sektora (pozri stranu 153 tohto úradného vestníka).

([28]) 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).

(105) Keďže cieľ tohto nariadenia, a to dosiahnutie vysokej úrovne digitálnej prevádzkovej odolnosti pre regulované finančné subjekty, nie je možné uspokojivo dosiahnuť na úrovni členských štátov, pretože si vyžaduje harmonizáciu rôznych predpisov v rámci práva Únie alebo vnútroštátneho práva, ale ho možno z dôvodu jeho 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.

(106) V súlade s článkom 42 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2018/1725 ([29]) sa konzultovalo s európskym dozorným úradníkom pre ochranu údajov, ktorý vydal svoje stanovisko 10. mája 2021 ([30]),

PRIJALI TOTO NARIADENIE:

KAPITOLA I

Všeobecné ustanovenia

Článok 1

Predmet úpravy

1. S cieľom dosiahnuť vysokú spoločnú úroveň digitálnej prevádzkovej odolnosti sa v tomto nariadení stanovujú tieto jednotné požiadavky týkajúce sa bezpečnosti sietí a informačných systémov podporujúcich obchodné procesy finančných subjektov:

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

   i) riadenie rizika v oblasti informačných a komunikačných technológií (ďalej len „IKT“);

   ii) nahlasovanie závažných incidentov súvisiacich s IKT a dobrovoľné oznamovanie významných kybernetických hrozieb príslušným orgánom;

   iii) nahlasovanie závažných prevádzkových incidentov alebo bezpečnostných incidentov súvisiacich s platbami príslušným orgánom zo strany finančných subjektov uvedených v článku 2 ods. 1 písm. a) až d);

   iv) testovanie digitálnej prevádzkovej odolnosti;

   v) výmena informácií a spravodajských informácií v súvislosti s kybernetickými hrozbami a zraniteľnými miestami;

   vi) opatrenia na správne riadenie externého IKT rizika;

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

c) pravidlá zriadenia a vykonávania rámca dozoru nad kritickými externými poskytovateľmi IKT služieb, keď tieto služby poskytujú finančným subjektom;

d) pravidlá spolupráce medzi príslušnými orgánmi a pravidlá dohľadu a presadzovania príslušnými orgánmi v súvislosti so všetkými záležitosťami, na ktoré sa vzťahuje toto nariadenie.

2. V súvislosti s finančnými subjektmi identifikovanými ako kľúčové alebo dôležité subjekty podľa vnútroštátnych predpisov, ktorými sa transponuje článok 3 smernice (EÚ) 2022/2555 sa toto nariadenie považuje za právny akt Únie špecifický pre určité odvetvie na účely článku 4 uvedenej smernice.

3. Týmto nariadením nie je dotknutá zodpovednosť členských štátov, pokiaľ ide o základné funkcie štátu týkajúce sa verejnej bezpečnosti, obrany a národnej bezpečnosti v súlade s právom Únie.

([29]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39).

([30]) Ú. v. EÚ C 229, 15.6.2021, s. 16.

Článok 2

Rozsah pôsobnosti

1. Bez toho, aby boli dotknuté odseky 3 a 4, sa toto nariadenie vzťahuje na tieto subjekty:

a) úverové inštitúcie;

b) platobné inštitúcie vrátane platobných inštitúcií vyňatých podľa smernice (EÚ) 2015/2366;

c) poskytovatelia služieb informovania o účte;

d) inštitúcie elektronického peňažníctva vrátane inštitúcií elektronického peňažníctva vyňatých podľa smernice 2009/110/ES;

e) investičné spoločnosti;

f) poskytovatelia služieb kryptoaktív, ktorým bolo udelené povolenie podľa nariadenia Európskeho parlamentu a Rady o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937 (ďalej len „nariadenie o trhoch s kryptoaktívami“) a emitenti tokenov krytých aktívami;

g) centrálne depozitáre cenných papierov;

h) centrálne protistrany;

i) obchodné miesta;

j) archívy obchodných údajov;

k) správcovia alternatívnych investičných fondov;

l) správcovské spoločnosti;

m) poskytovatelia služieb vykazovania údajov;

n) poisťovne a zaisťovne;

o) sprostredkovatelia poistenia, sprostredkovatelia zaistenia a sprostredkovatelia doplnkového poistenia;

p) inštitúcie zamestnaneckého dôchodkového zabezpečenia;

q) ratingové agentúry;

r) správcovia kritických referenčných hodnôt;

s) poskytovatelia služieb hromadného financovania;

t) archívy sekuritizačných údajov;

u) externí poskytovatelia IKT služieb.

2. Na účely tohto nariadenia sa subjekty uvedené v odseku 1 písm. a) až t) spoločne označujú ako „finančné subjekty“.

3. Toto nariadenie sa neuplatňuje na:

a) správcov alternatívnych investičných fondov, ako sa uvádza v článku 3 ods. 2 smernice 2011/61/EÚ;

b) poisťovne a zaisťovne, ako sa uvádza v článku 4 smernice 2009/138/ES;

c) inštitúcie zamestnaneckého dôchodkového zabezpečenia, ktoré prevádzkujú dôchodkové plány, ktoré spolu nemajú viac ako 15 členov;

d) fyzické alebo právnické osoby oslobodené podľa článkov 2 a 3 smernice 2014/65/EÚ;

e) sprostredkovateľov poistenia, sprostredkovateľov zaistenia a sprostredkovateľov doplnkového poistenia, ktorými sú mikropodniky alebo malé alebo stredné podniky;

f) poštové sporožírové inštitúcie ako sa uvádza v článku 2 ods. 5 bode 3 smernice 2013/36/EÚ.

4. Členské štáty môžu z rozsahu pôsobnosti tohto nariadenia vylúčiť subjekty uvedené v článku 2 ods. 5 bodoch 4 až 23 smernice 2013/36/EÚ, ktoré sa nachádzajú na ich príslušných územiach. Ak členský štát využije takúto možnosť, informuje o tom, ako aj o všetkých jej následných zmenách Komisiu. Komisia tieto informácie zverejní na svojom webovom sídle alebo inými ľahko dostupnými prostriedkami.

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 a spoľahlivosť tak, že priamo alebo nepriamo prostredníctvom využívania služieb poskytovaných externými poskytovateľmi IKT služieb 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, a to aj počas narušení;

2. „sieť a informačný systém“ je sieť a informačný systém v zmysle vymedzenia v článku 6 bodu 1 smernice (EÚ) 2022/2555+;

3. „pôvodný IKT systém“ je IKT systém, ktorý dosiahol koniec svojho životného cyklu (koniec životnosti), ktorý nie je vhodný na vylepšenia alebo opravy z technologických alebo obchodných dôvodov alebo ho už jeho dodávateľ alebo externý poskytovateľ IKT služieb nepodporuje, ale ktorý sa stále používa a podporuje funkcie finančného subjektu;

4. „bezpečnosť sietí a informačných systémov“ je bezpečnosť sietí a informačných systémov v zmysle vymedzenia v článku 6 bode 2 smernice (EÚ) 2022/2555+;

5. „IKT riziko“ je každá primerane identifikovateľná okolnosť v súvislosti s používaním sietí a informačných systémov, ktorá, ak k nej dôjde, môže ohroziť bezpečnosť sietí a informačných systémov, akéhokoľvek nástroja alebo procesu závislého od technológií, ako aj bezpečnosť operácií a procesov alebo poskytovania služieb vytvorením nepriaznivých účinkov v digitálnom alebo fyzickom prostredí;

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

7. „IKT aktívum“ je softvérové alebo hardvérové aktívum v sieťach a informačných systémoch, ktoré používa finančný subjekt;

8. „incident súvisiaci s IKT“ je jedna udalosť alebo séria prepojených udalostí, ktoré finančný subjekt neplánoval a ktoré narúšajú bezpečnosť sietí a informačných systémov a majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov alebo na služby, ktoré poskytuje finančný subjekt;

9. „prevádzkový alebo bezpečnostný incident súvisiaci s platbami“ je jedna udalosť alebo séria prepojených udalostí, ktoré finančné subjekty uvedené v článku 2 ods. 1 písm. a) až d) neplánovali, bez ohľadu na to, či súvisia s IKT alebo nie, a ktoré majú nepriaznivý vplyv na dostupnosť, pravosť, integritu alebo dôvernosť údajov súvisiacich s platbami, alebo na služby súvisiace s platbami, ktoré poskytuje finančný subjekt;

10. „závažný incident súvisiaci s IKT“ je incident súvisiaci s IKT, ktorý má veľký nepriaznivý vplyv na siete a informačné systémy, ktoré podporujú kritické alebo dôležité funkcie finančného subjektu;

11. „závažný prevádzkový alebo bezpečnostný incident súvisiaci s platbami“ je prevádzkový alebo bezpečnostný incident súvisiaci s platbami, ktorý má veľký nepriaznivý vplyv na poskytované služby súvisiace s platbami;

12. „kybernetická hrozba“ je kybernetická hrozba v zmysle vymedzenia v článku 2 bode 8 nariadenia (EÚ) 2019/881;

13. „významná kybernetická hrozba“ je kybernetická hrozba, ktorej technické charakteristiky naznačujú, že by mohla mať potenciál viesť k závažnému incidentu súvisiacemu s IKT alebo závažnému prevádzkovému alebo bezpečnostnému incidentu súvisiacemu s platbami;

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

15. „spravodajské informácie o hrozbách“ sú informácie, ktoré boli agregované, transformované, analyzované, interpretované alebo obohatené tak, aby poskytli potrebný kontext pre rozhodovanie a umožnili relevantné a dostatočné pochopenie s cieľom zmierniť vplyv incidentu súvisiaceho s IKT alebo kybernetickej hrozby vrátane technických podrobností kybernetického útoku, subjektov zodpovedných za útok a ich modu operandi a motivácie;

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

17. „penetračné testovanie na základe konkrétnej hrozby“ alebo „TLPT“)“ 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 finančného subjektu založený na spravodajských informáciách (červený tím);

18. „externé IKT riziko“ je IKT riziko, ktoré môže finančnému subjektu vzniknúť v súvislosti s jeho využívaním IKT služieb, ktoré poskytujú externí poskytovatelia IKT služieb alebo ich subdodávatelia, a to aj prostredníctvom dohôd o outsourcingu;

19. „externý poskytovateľ IKT služieb“ je podnik poskytujúci IKT služby;

20. „vnútroskupinový poskytovateľ IKT služieb“ je podnik, ktorý je súčasťou finančnej skupiny a ktorý poskytuje prevažne IKT služby finančným subjektom v rámci rovnakej skupiny alebo finančným subjektom patriacim do rovnakej schémy inštitucionálneho zabezpečenia vrátane ich materských podnikov, dcérskych podnikov, pobočiek alebo iných subjektov, ktoré sú v spoločnom vlastníctve alebo pod spoločnou kontrolou;

21. „IKT služby“ sú digitálne a dátové služby poskytované prostredníctvom IKT systémov jednému alebo viacerým interným alebo externým používateľom priebežne vrátane hardvéru ako služby a hardvérových služieb, ktoré zahŕňajú poskytovanie technickej podpory prostredníctvom aktualizácií softvéru alebo firmvéru poskytovateľom hardvéru s výnimkou tradičných analógových telefónnych služieb;

22. „kritická alebo dôležitá funkcia“ je funkcia, ktorej narušenie by v podstatnej miere negatívne ovplyvnilo finančnú výkonnosť finančného subjektu či správnosť alebo kontinuitu jeho služieb a činností, alebo funkcia, ktorej ukončenie, chybné plnenie alebo neplnenie by v podstatnej miere negatívne ovplyvnilo nepretržité dodržiavanie podmienok a povinností finančného subjektu vyplývajúcich z jeho povolenia alebo jeho iných povinností podľa uplatniteľného práva v oblasti finančných služieb;

23. „kritický externý poskytovateľ IKT služieb“ je externý poskytovateľ IKT služieb určený ako kritický v súlade s článkom 31;

24. „externý poskytovateľ IKT služieb usadený v tretej krajine“ je externý poskytovateľ IKT služieb, ktorý je právnickou osobou usadenou v tretej krajine a ktorý má s finančným subjektom uzavreté zmluvné dojednanie o poskytovaní IKT služieb;

25. „dcérsky podnik“ je dcérsky podnik v zmysle článku 2 bodu 10 a článku 22 smernice 2013/34/EÚ;

26. „skupina“ je skupina v zmysle článku 2 bodu 11 smernice 2013/34/EÚ;

27. „materský podnik“ je materský podnik v zmysle článku 2 bodu 9 a článku 22 smernice 2013/34/EÚ;

28. „subdodávateľ IKT usadený v tretej krajine“ je subdodávateľ IKT, ktorý je právnickou osobou usadenou v tretej krajine a ktorý má uzavreté zmluvné dojednanie buď s externým poskytovateľom IKT služieb alebo s externým poskytovateľom IKT služieb usadeným v tretej krajine;

29. „riziko koncentrácie IKT“ je expozícia voči jednotlivému kritickému externému poskytovateľovi IKT služieb alebo viacerým súvisiacim kritickým externým poskytovateľom IKT služieb, v dôsledku ktorej vzniká určitá závislosť od takýchto poskytovateľov, takže nedostupnosť, zlyhanie alebo iný druh nedostatku na strane takéhoto poskytovateľa môže potenciálne ohroziť schopnosť finančného subjektu plniť kritické alebo dôležité funkcie alebo spôsobiť mu iný druh nepriaznivých účinkov vrátane veľkých strát, alebo ohroziť finančnú stabilitu Únie ako celku;

30. „riadiaci orgán“ je riadiaci orgán v zmysle vymedzenia v článku 4 ods. 1 bode 36 smernice Európskeho parlamentu a Rady 2014/65/EÚ, v článku 3 ods. 1 bode 7 smernice Európskeho parlamentu a Rady 2013/36/EÚ, v článku 2 ods. 1 písm. s) smernice Európskeho parlamentu a Rady 2009/65/ES ([31]), v článku 2 ods. 1 bode 45 nariadenia (EÚ) č. 909/2014, v článku 3 ods. 1 bode 20 nariadenia (EÚ) 2016/1011 a v príslušnom ustanovení nariadenia o trhoch s kryptoaktívami alebo rovnocenné osoby, ktoré daný subjekt skutočne riadia alebo vykonávajú kľúčové funkcie v súlade s príslušným právom Únie alebo vnútroštátnym právom;

31. „úverová inštitúcia“ je úverová inštitúcia v zmysle vymedzenia v článku 4 ods. 1 bode 1 nariadenia Európskeho parlamentu a Rady (EÚ) č. 575/2013 ([32]);

32. „inštitúcia vyňatá podľa smernice 2013/36/EÚ“ je subjekt uvedený v článku 2 ods. 5 bodoch 4 až 23 smernice 2013/36/EÚ;

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

34. „malá a neprepojená investičná spoločnosť“ je investičná spoločnosť, ktorá spĺňa podmienky stanovené v článku 12 ods. 1 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/2033 ([33]);

35. „platobná inštitúcia“ je platobná inštitúcia v zmysle vymedzenia v článku 4 bode 4 smernice (EÚ) 2015/2366;

36. „platobná inštitúcia vyňatá podľa smernice (EÚ) 2015/2366“ je platobná inštitúcia vyňatá podľa článku 32 ods. 1 smernice (EÚ) 2015/2366;

37. „poskytovateľ služieb informovania o účte“ je poskytovateľ služieb informovania o účte, ako sa uvádza v článku 33 ods. 1 smernice (EÚ) 2015/2366;

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

39. „inštitúcia elektronického peňažníctva vyňatá podľa smernice 2009/110/ES“ je inštitúcia elektronického peňažníctva, na ktorú sa vzťahuje výnimka uvedená v článku 9 ods. 1 smernice 2009/110/ES;

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

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

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

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

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

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

46. „poskytovateľ služieb vykazovania údajov“ je poskytovateľ služieb vykazovania údajov v zmysle nariadenia (EÚ) č. 600/2014, ako sa uvádza v jeho článku 2 ods. 1 bodoch 34 až 36;

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

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

([31]) Smernica Európskeho parlamentu a Rady 2009/65/ES z 13. júla 2009 o koordinácii zákonov, iných právnych predpisov a správnych opatrení týkajúcich sa podnikov kolektívneho investovania do prevoditeľných cenných papierov (PKIPCP) (Ú. v. EÚ L 302, 17.11.2009, s. 32).

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

([33]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/2033 z 27. novembra 2019 o prudenciálnych požiadavkách na investičné spoločnosti a o zmene nariadení (EÚ) č. 1093/2010, (EÚ) č. 575/2013, (EÚ) č. 600/2014 a (EÚ) č. 806/2014 (Ú. v. EÚ L 314, 5.12.2019, s. 1).

49. „sprostredkovateľ poistenia“ je sprostredkovateľ poistenia v zmysle vymedzenia v článku 2 ods. 1 bode 3 smernice Európskeho parlamentu a Rady (EÚ) 2016/97 ([34]);

50. „sprostredkovateľ doplnkového poistenia“ je sprostredkovateľ doplnkového poistenia v zmysle vymedzenia v článku 2 ods. 1 bode 4 smernice (EÚ) 2016/97;

51. „sprostredkovateľ zaistenia“ je sprostredkovateľ zaistenia v zmysle vymedzenia v článku 2 ods. 1 bode 5 smernice (EÚ) 2016/97;

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

53. „malá inštitúcia zamestnaneckého dôchodkového zabezpečenia“ je inštitúcia zamestnaneckého dôchodkového zabezpečenia, ktorá prevádzkuje dôchodkové plány, ktoré majú spolu celkovo menej ako 100 členov;

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

55. „poskytovateľ služieb kryptoaktív“ je poskytovateľ služieb kryptoaktív v zmysle vymedzenia v príslušnom ustanovení nariadenia o trhoch s kryptoaktívami;

56. „emitent tokenov krytých aktívami“ je emitent tokenov krytých aktívami v zmysle vymedzenia v príslušnom ustanovení nariadenia o trhoch s kryptoaktívami;

57. „správca kritických referenčných hodnôt“ je správca kritických referenčných hodnôt v zmysle vymedzenia v článku 3 ods. 1 bode 25 (EÚ) 2016/1011;

58. „poskytovateľ služieb hromadného financovania“ je poskytovateľ služieb hromadného financovania v zmysle vymedzenia v článku 2 ods. 1 písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2020/1503 ([35]);

59. „archív sekuritizačných údajov“ je archív sekuritizačných údajov v zmysle vymedzenia v článku 2 bode 23 nariadenia Európskeho parlamentu a Rady (EÚ) 2017/2402 ([36]);

60. „mikropodnik“ je finančný subjekt iný ako obchodné miesto, centrálna protistrana, archív obchodných údajov alebo centrálny depozitár cenných papierov, ktorý zamestnáva menej ako 10 osôb a ktorého ročný obrat a/alebo celková ročná súvaha nepresahuje 2 milióny EUR;

61. „hlavný orgán dozoru“ je európsky orgán dohľadu vymenovaný v súlade s článkom 31 ods. 1 písm. b) tohto nariadenia;

62. „spoločný výbor“ je výbor uvedený v článku 54 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010;

63. „malý podnik“ je finančný subjekt, ktorý zamestnáva 10 alebo viac osôb, ale menej ako 50 osôb a ktorého ročný obrat a/alebo ročná súvaha presahujú 2 milióny EUR, ale nepresahujú 10 miliónov EUR;

64. „stredný podnik“ je finančný subjekt, ktorý nie je malým podnikom, zamestnáva menej ako 250 osôb a jeho ročný obrat nepresahuje 50 miliónov EUR a/alebo ročná súvaha nepresahuje 43 miliónov EUR;

65. „orgán verejnej moci“ je akýkoľvek vládny alebo iný subjekt verejnej správy vrátane národných centrálnych bánk.

([34]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/97 z 20. januára 2016 o distribúcii poistenia (Ú. v. EÚ L 26, 2.2.2016, s. 19).

([35]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2020/1503 zo 7. októbra 2020 o európskych poskytovateľoch služieb hromadného financovania pre podnikanie a o zmene nariadenia (EÚ) 2017/1129 a smernice (EÚ) 2019/1937 (Ú. v. EÚ L 347, 20.10.2020, s. 1).

([36]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/2402 z 12. decembra 2017, ktorým sa stanovuje všeobecný rámec pre sekuritizáciu a vytvára sa osobitný rámec pre jednoduchú, transparentnú a štandardizovanú sekuritizáciu, a ktorým sa menia smernice 2009/65/ES, 2009/138/ES a 2011/61/EÚ a nariadenia (ES) č. 1060/2009 a (EÚ) č. 648/2012 (Ú. v. EÚ L 347, 28.12.2017, s. 35).

Článok 4

Zásada proporcionality

1. Finančné subjekty uplatňujú pravidlá stanovené v kapitole II v súlade so zásadou proporcionality, pričom zohľadňujú svoju veľkosť a celkový rizikový profil, ako aj povahu, rozsah a zložitosť svojich služieb, činností a operácií.

2. Okrem toho uplatňovanie oddielu I v kapitolách III, IV a V finančnými subjektmi musí byť primerané ich veľkosti a celkovému rizikovému profilu, ako aj povahe, rozsahu a zložitosti ich služieb, činností a operácií, ako sa konkrétne stanovuje v príslušných pravidlách uvedených kapitol.

3. Príslušné orgány zvážia uplatňovanie zásady proporcionality finančnými subjektmi pri skúmaní konzistentnosti rámca riadenia IKT rizika na základe správ predložených na žiadosť príslušných orgánov podľa článku 6 ods. 5 a článku 16 ods. 2

KAPITOLA II

Riadenie IKT rizika

Oddiel I

Článok 5

Správa a riadenie a organizácia

1. Finančné subjekty musia mať v súlade s článkom 6 ods. 4 zavedený rámec vnútornej správy a riadenia a kontroly, ktorým sa zabezpečí účinné a obozretné riadenie IKT rizika s cieľom dosiahnuť vysokú úroveň digitálnej prevádzkovej odolnosti.

2. Riadiaci orgán finančného subjektu vymedzuje a schvaľuje vykonávanie všetkých opatrení súvisiacich s rámcom riadenia IKT rizika uvedeným v článku 6 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) zavádza politiky zamerané na zabezpečenie zachovania vysokých noriem dostupnosti, pravosti, integrity a dôvernosti údajov;

c) stanovuje jasné úlohy a zodpovednosti pre všetky funkcie súvisiace s IKT a zavádza vhodné mechanizmy správy a riadenia s cieľom zabezpečiť účinnú a včasnú komunikáciu, spoluprácu a koordináciu medzi týmito funkciami;

d) nesie celkovú zodpovednosť za stanovenie a schválenie stratégie digitálnej prevádzkovej odolnosti, ako sa uvádza v článku 6 ods. 8, vrátane určenia primeranej úrovne tolerancie IKT rizika finančného subjektu, ako sa uvádza v článku 6 ods. 8 písm. b);

e) schvaľuje, vykonáva dozor a pravidelne preskúmava vykonávanie politiky kontinuity činností finančného subjektu v oblasti IKT a plánov reakcie a obnovy v oblasti IKT uvedených v článku 11 ods. 1 a 3, ktoré sa môžu prijať ako osobitná politika tvoriaca neoddeliteľnú súčasť celkovej politiky kontinuity činností finančného subjektu a plánu reakcie a obnovy finančného subjektu;

f) schvaľuje a pravidelne preskúmava plány vnútorných auditov IKT, ktoré vypracúva finančný subjekt, audity IKT a ich podstatné zmeny;

g) prideľuje a pravidelne preskúmava primeraný rozpočet na splnenie potrieb finančného subjektu v oblasti digitálnej prevádzkovej odolnosti, pokiaľ ide o všetky druhy zdrojov, vrátane relevantných programov zvyšovania informovanosti o bezpečnosti v oblasti IKT a školení o digitálnej prevádzkovej odolnosti uvedených v článku 13 ods. 6 a IKT zručností pre všetkých zamestnancov;

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

i) zavádza na podnikovej úrovni kanály nahlasovania, ktoré mu umožnia, aby bol riadne informovaný o:

i) dojednaniach o využívaní IKT služieb uzavretých s externými poskytovateľmi IKT služieb;

ii) akýchkoľvek relevantných plánovaných podstatných zmenách týkajúcich sa externých poskytovateľov IKT služieb;

iii) potenciálnom vplyve takýchto zmien na kritické alebo dôležité funkcie, ktoré podliehajú uvedeným dojednaniam, vrátane zhrnutia analýzy rizík na posúdenie vplyvu uvedených zmien, a aspoň o závažných incidentoch súvisiacich s IKT a ich vplyve, ako aj o opatreniach zameraných na reakciu, obnovu a nápravu.

3. Finančné subjekty iné než mikropodniky zriadia funkciu, 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 finančného subjektu si aktívne udržiavajú dostatočné znalosti a zručnosti potrebné na pochopenie a posúdenie IKT rizika a jeho vplyvu na operácie finančného subjektu, a to aj pravidelným absolvovaním osobitných školení zodpovedajúcich IKT riziku, ktoré je predmetom riadenia.

Oddiel II

Článok 6

Rámec riadenia IKT rizika

1. Finančné subjekty musia mať ako súčasť svojho celkového systému riadenia rizika 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.

2. Rámec riadenia IKT rizika zahŕňa aspoň stratégie, politiky, postupy, IKT protokoly a nástroje, ktoré sú potrebné na riadnu a primeranú ochranu všetkých informačných aktív a IKT aktív vrátane počítačového softvéru**,** hardvéru, serverov, ako aj ochranu všetkých relevantných fyzických zložiek a infraštruktúr, ako sú priestory, dátové centrá a citlivé určené oblasti s cieľom zabezpečiť, aby boli všetky informačné aktíva a IKT aktíva primerane chránené pred rizikami vrátane poškodenia a neoprávneného prístupu či používania.

3. Finančné subjekty v súlade so svojím rámcom riadenia IKT rizika minimalizujú vplyv IKT rizika zavedením vhodných stratégií, politík, postupov, IKT protokolov a nástrojov. Príslušným orgánom poskytujú na ich žiadosť úplné a aktualizované informácie o IKT riziku a o svojom rámci riadenia IKT rizika.

4. Finančné subjekty iné než mikropodniky priradia zodpovednosť za riadenie IKT rizika a dozor nad ním kontrolnej funkcii a zabezpečia primeranú úroveň nezávislosti tejto kontrolnej funkcie, aby sa zabránilo konfliktom záujmov. Finančné subjekty zabezpečia primeranú segregáciu a nezávislosť riadiacich funkcií v oblasti IKT rizika, kontrolných funkcií a funkcií vnútorného auditu, a to na základe modelu troch línií obrany alebo na základe interného modelu riadenia rizík a kontroly.

5. Rámec riadenia IKT rizika sa zdokumentuje a preskúma aspoň raz ročne, alebo pravidelne v prípade mikropodnikov, 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. Správa o preskúmaní rámca riadenia IKT rizika sa predkladá príslušnému orgánu na jeho žiadosť.

6. Rámec riadenia IKT rizika finančných subjektov iných ako mikropodnikov podlieha pravidelnému vnútornému auditu vykonávanému audítormi v súlade s plánom auditu finančných subjektov. Títo audítori musia mať dostatočné znalosti, zručnosti a odborné znalosti v oblasti IKT rizika, ako aj primeranú nezávislosť. Frekvencia a zameranie auditov IKT musia zodpovedať IKT riziku daného finančného subjektu.

7. Na základe záverov vnútorného audítorského preskúmania finančné subjekty zavedú formálny postup prijímania následných opatrení vrátane pravidiel včasného overovania a nápravy kritických zistení auditu IKT.

8. Rámec riadenia IKT rizika zahŕňa stratégiu digitálnej prevádzkovej odolnosti, v ktorej sa stanoví spôsob vykonávania rámca. Na tento účel stratégia digitálnej prevádzkovej odolnosti 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 riziko a analýza tolerancie vplyvu narušení v oblasti IKT;

c) stanovenie jasných cieľov informačnej bezpečnosti vrátane kľúčových ukazovateľov výkonnosti a kľúčových ukazovateľov rizika;

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

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

f) preukázanie súčasnej situácie v oblasti digitálnej prevádzkovej odolnosti na základe počtu nahlásených závažných incidentov súvisiacich s IKT a účinnosti preventívnych opatrení;

g) vykonávanie testovania digitálnej prevádzkovej odolnosti v súlade s kapitolou IV tohto nariadenia;

h) stanovenie komunikačnej stratégie v prípade incidentov súvisiacich s IKT, ktorých zverejnenie sa vyžaduje v súlade s článkom 14.

9. Finančné subjekty môžu v súvislosti so stratégiou digitálnej prevádzkovej odolnosti uvedenou v odseku 8 vymedziť holistickú stratégiu viacerých dodávateľov IKT, a to na úrovni skupiny alebo subjekt, ktorá preukazuje kľúčové závislosti od externých poskytovateľov IKT služieb a vysvetľuje dôvody, na ktorých je založený príslušný obstarávací mix externých poskytovateľov služieb.

10. Finančné subjekty môžu v súlade s právom Únie a vnútroštátnym odvetvovým právom zadať úlohy overovania súladu s požiadavkami na riadenie IKT rizika vnútroskupinovým alebo externým podnikom formou outsourcingu. V prípade takéhoto outsourcingu zostáva finančný subjekt plne zodpovedný za overovanie súladu s požiadavkami na riadenie IKT rizika.

Článok 7

Systémy, protokoly a nástroje IKT

S cieľom riešiť a riadiť IKT riziko finančné subjekty používajú a udržiavajú aktualizované systémy, protokoly a nástroje IKT, ktoré sú:

a) primerané rozsahu operácií, ktoré podporujú vykonávanie ich činností, v súlade so zásadou proporcionality uvedenou v článku 4;

b) spoľahlivé;

c) vybavené dostatočnou kapacitou na to, aby sa nimi presne spracúvali údaje potrebné na vykonávanie činností a včasné 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) dostatočne technologicky odolné na to, aby primerane zvládali dodatočné potreby v oblasti spracúvania informácií, ak si to vyžadujú stresové trhové podmienky alebo iné nepriaznivé situácie.

Článok 8

Identifikácia

1. Ako súčasť rámca riadenia IKT rizika uvedeného v článku 6 ods. 1 finančné subjekty identifikujú, klasifikujú a primerane dokumentujú všetky obchodné funkcie, úlohy a povinnosti podporované IKT, informačné aktíva a IKT aktíva podporujúce uvedené funkcie a ich úlohy a závislosti vo vzťahu k IKT riziku. Finančné subjekty podľa potreby, najmenej však raz ročne, preskúmavajú primeranosť tejto klasifikácie 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 podporovaných IKT, informačných aktív a IKT aktív. 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 významnej zmene infraštruktúry siete a informačných systémov, pokiaľ ide o procesy alebo postupy, ktoré majú vplyv na ich obchodné funkcie podporované IKT, informačné aktíva alebo IKT aktíva.

4. Finančné subjekty identifikujú všetky informačné aktíva a IKT aktíva vrátane aktív na vzdialených miestach, sieťové zdroje a hardvérové zariadenia a zmapujú tie, ktoré sa považujú za kritické. Zmapujú konfiguráciu informačných aktív a IKT aktív, ako aj prepojenia a vzájomné závislosti medzi jednotlivými informačnými aktívami a IKT aktívami.

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, ktorí poskytujú služby podporujúce kritické alebo dôležité funkcie.

6. Na účely odsekov 1, 4 a 5 finančné subjekty vedú relevantné inventáre a aktualizujú ich pravidelne a vždy, keď dôjde k akejkoľvek významnej zmene uvedenej v odseku 3.

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

Článok 9

Ochrana a prevencia

1. Na účely primeranej ochrany IKT systémov a s cieľom organizovať opatrenia v oblasti reakcie finančné subjekty nepretržite monitorujú a kontrolujú bezpečnosť a fungovanie IKT systémov a nástrojov a minimalizujú vplyv IKT rizika na IKT systémy 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 zabezpečiť odolnosť, kontinuitu a dostupnosť IKT systémov, najmä tých, ktoré podporujú kritické alebo dôležité funkcie, a zachovať vysoké štandardy dostupnosti, pravosti, integrity a dôvernosti údajov, či už v pokoji, pri používaní alebo pri prenose.

3. Na dosiahnutie cieľov uvedených v odseku 2 finančné subjekty používajú IKT riešenia a procesy, ktoré sú vhodné v súlade s článkom 4. Uvedené IKT riešenia a procesy:

a) zaručujú bezpečnosť prostriedkov prenosu údajov;

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

c) predchádzajú nedostatočnej dostupnosti, narušeniu pravosti a integrity, porušeniam dôvernosti a strate údajov;

d) zabezpečujú, že údaje sú chránené pred rizikami vyplývajúcimi z riadenia údajov vrátane nedostatočnej správy, rizikami súvisiacimi so spracúvaním a ľudskou chybou.

4. Ako súčasť rámca riadenia IKT rizika uvedeného v článku 6 ods. 1 finančné subjekty:

a) vypracúvajú a zdokumentujú politiku v oblasti informačnej bezpečnosti, v ktorej sa vymedzujú pravidlá na ochranu dostupnosti, pravosti, integrity a dôvernosti údajov, informačných aktív a IKT aktív vrátane prípadných údajov a aktív ich zákazníkov;

b) na základe prístupu založeného na riziku zavedú spoľahlivé riadenie siete a infraštruktúry pomocou vhodných techník, metód a protokolov, ktoré môžu zahŕňať zavedenie automatizovaných mechanizmov na izolovanie dotknutých informačných aktív v prípade kybernetických útokov;

c) vykonávajú politiky, ktoré obmedzujú fyzický alebo logický prístup k informačným aktívam a IKT aktívam 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 zabezpečujú ich riadnu správu;

d) vykonávajú politiky a protokoly pre silné mechanizmy autentifikácie založené na príslušných normách a špecializovaných kontrolných systémoch, ako aj ochranné opatrenia v podobe šifrovacích kľúčov, pričom údaje sú šifrované na základe výsledkov schválenej klasifikácie údajov a procesov posudzovania IKT rizika;

e) vykonávajú zdokumentované politiky, postupy a kontroly riadenia zmien IKT vrátane zmien komponentov softvéru, hardvéru, firmvéru, systémov alebo bezpečnostných parametrov, 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) majú vhodné a komplexné zdokumentované politiky týkajúce sa opráv a aktualizácií.

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

Proces riadenia zmien IKT na účely prvého pododseku písm. e) schvaľujú príslušné riadiace línie, ktoré majú zavedené osobitné protokoly.

Článok 10

Detekcia

1. Finančné subjekty musia mať zavedené mechanizmy na rýchle odhaľovanie anomálnych činností v súlade s článkom 17 vrátane problémov s výkonnosťou IKT siete a incidentov súvisiacich s IKT, ako aj na identifikáciu potenciálnych závažných jednotlivých miest zlyhania.

Všetky detekčné mechanizmy uvedené v prvom pododseku sa pravidelne testujú v súlade s článkom 25.

2. Detekčné mechanizmy uvedené v odseku 1 umožňujú viaceré úrovne kontroly, vymedzujú sa v nich varovné prahové hodnoty a kritériá na spustenie a iniciáciu procesov reakcie na incidenty súvisiace s IKT vrátane automatických mechanizmov varovania pre príslušných zamestnancov zodpovedných za reakciu na incidenty súvisiace s IKT.

3. Finančné subjekty venujú dostatočné zdroje a spôsobilosti na monitorovanie činnosti používateľov, výskytu anomálií IKT a incidentov súvisiacich s IKT, a to najmä kybernetických útokov.

4. Poskytovateľ služieb vykazovania údajov musí mať navyše zavedené systémy, ktoré dokážu účinne kontrolovať úplnosť správ o obchode, identifikovať opomenutia a zjavné chyby a požiadať o opätovné zaslanie všetkých týchto správ.

Článok 11

Reakcia a obnova

1. Finančné subjekty ako súčasť rámca riadenia IKT rizika uvedeného v článku 6 ods. 1 a na základe požiadaviek na identifikáciu stanovených v článku 8 zavedú komplexnú politiku kontinuity činností v oblasti IKT, ktorá môže byť prijatá ako osobitná, špecifická politika tvoriaca neoddeliteľnú súčasť celkovej politiky kontinuity činností finančného subjektu.

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

a) zabezpečenie kontinuity kritických alebo dôležitých funkcií finančného subjektu;

b) rýchlu, primeranú a účinnú reakciu na všetky incidenty súvisiace s IKT a ich riešenie,, a to spôsobom, ktorý obmedzuje škody a uprednostňuje obnovenie činností a opatrenia zamerané na obnovu;

c) 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 12;

d) odhad predbežných vplyvov, škôd a strát;

e) 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 14 a aby sa o nich podávali správy príslušným orgánom v súlade s článkom 19.

3. Finančné subjekty ako súčasť rámca riadenia IKT rizika uvedeného v článku 6 ods. 1 vykonávajú súvisiace plány reakcie a obnovy v oblasti IKT, ktoré v prípade finančných subjektov iných než mikropodnikov podliehajú nezávislému vnútornému audítorskému preskúmaniu.

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

5. V rámci celkovej politiky kontinuity činností finančné subjekty vykonávajú analýzu vplyvu na svoje činnosti (ďalej len „BIA“) zameranú na svoje expozície voči závažným narušeniam činnosti. V rámci BIA finančné subjekty posudzujú potenciálny vplyv závažných narušení činnosti prostredníctvom kvantitatívnych a kvalitatívnych kritérií, pričom náležite využívajú interné a externé údaje a analýzu scenárov. V BIA sa zohľadňuje kritickosť identifikovaných a zmapovaných obchodných funkcií, podporných procesov, závislostí od tretích strán a informačných aktív a ich vzájomná závislosť. Finančné subjekty zabezpečia, aby sa IKT aktíva a IKT služby koncipovali a používali v plnom súlade s BIA, najmä pokiaľ ide o primerané zabezpečenie redundancie všetkých kritických komponentov.

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

a) testujú plány kontinuity činností v oblasti IKT a plány reakcie a obnovy v oblasti IKT vo vzťahu k IKT systémom podporujúcim všetky funkcie aspoň raz ročne, ako aj v prípade akýchkoľvek podstatných zmien IKT systémov podporujúcich kritické alebo dôležité funkcie;

b) testujú plány krízovej komunikácie vypracované v súlade s článkom 14.

Na účely prvého pododseku písm. 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 12.

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

7. Finančné subjekty iné než mikropodniky musia mať funkciu krízového riadenia, ktorá v prípade aktivácie ich plánov kontinuity činností v oblasti IKT alebo plánov reakcie a obnovy v oblasti IKT stanoví okrem iného jasné postupy riadenia vnútornej a vonkajšej krízovej komunikácie v súlade s článkom 14.

8. Finančné subjekty vedú ľahko prístupné záznamy o činnostiach pred udalosťami narušenia a počas nich, keď sa aktivujú ich plány kontinuity činností v oblasti IKT alebo plány reakcie a obnovy v oblasti IKT.

9. Centrálni depozitári cenných papierov poskytnú príslušným orgánom kópie výsledkov testov kontinuity činností v oblasti IKT alebo podobných cvičení.

10. Finančné subjekty iné ako mikropodniky oznamujú príslušným orgánom na ich žiadosť odhad súhrnných ročných nákladov a strát spôsobených závažnými incidentmi súvisiacimi s IKT.

11. V súlade s článkom 16 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 európske orgány dohľadu prostredníctvom spoločného výboru do 17. júla 2024 vypracujú spoločné usmernenia o odhade súhrnných ročných nákladov a strát uvedených v odseku 10.

Článok 12

Politiky a postupy zálohovania, postupy a metódy reštaurovania a obnovy

1. Na účely zabezpečenia reštaurovania IKT systémov a údajov s minimálnym výpadkom, obmedzeným narušením a stratami finančné subjekty v rámci ich riadenia IKT rizika vypracujú a zdokumentujú:

a) politiky a postupy zálohovania, v ktorých sa špecifikuje rozsah údajov, ktoré sú predmetom zálohovania, a minimálna frekvencia zálohovania na základe kritickosti informácií alebo úrovne dôvernosti údajov;

b) postupy a metódy reštaurovania a obnovy.

2. Finančné subjekty zriadia záložné systémy, ktoré možno aktivovať v súlade s politikami a postupmi zálohovania, ako aj postupmi a metódami reštaurovania a obnovy. Aktivácia záložných systémov nesmie ohroziť bezpečnosť sietí a informačných systémov ani dostupnosť, pravosť, integritu alebo dôvernosť údajov. Pravidelne sa vykonáva testovanie postupov zálohovania a postupov a metód reštaurovania a obnovy.

3. Pri reštaurovaní záložných údajov pomocou vlastných systémov finančné subjekty používajú IKT systémy, ktoré sú fyzicky a logicky oddelené od zdrojového IKT systému. IKT systémy musia byť bezpečne chránené pred akýmkoľvek neoprávneným prístupom alebo poškodením IKT a podľa potreby umožňujú včasné reštaurovanie služieb využívajúcich údaje a zálohy systému.

V prípade centrálnych protistrán 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.

Poskytovatelia služieb vykazovania údajov okrem toho udržiavajú primerané zdroje a majú zavedené záložné zariadenia a zariadenia na reštaurovanie s cieľom neustále ponúkať a udržiavať svoje služby.

4. Finančné subjekty iné ako mikropodniky udržiavajú redundantné IKT kapacity vybavené zdrojmi, spôsobilosťami a funkciami, ktoré sú dostatočné na zabezpečenie obchodných potrieb. Mikropodniky posudzujú potrebu udržiavať takéto redundantné IKT kapacity na základe svojho rizikového profilu.

5. Centrálni depozitári cenných papierov udržiavajú aspoň jedno sekundárne miesto spracúvania vybavené dostatočnými zdrojmi, spôsobilosťami, funkciami a personálnym zabezpečením na zaistenie obchodných potrieb.

Sekundárne miesto spracúvania musí:

a) byť umiestnené v lokalite geograficky vzdialenej od primárneho miesta spracúvania 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 alebo dôležitých funkcií 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 alebo dôležitých funkcií v prípade, že sa primárne miesto spracúvania stalo nedostupným.

6. Pri určovaní časových bodov obnovy a cieľov bodov obnovy pre každú funkciu finančné subjekty zohľadňujú, či ide o kritickú alebo dôležitú funkciu a potenciálny celkový vplyv na efektívnosť trhu. Takéto časové ciele zabezpečia, aby sa v extrémnych scenároch dosiahli dohodnuté úrovne služieb.

7. Pri zotavovaní sa po incidente súvisiacom s IKT vykonávajú finančné subjekty potrebné kontroly vrátane akýchkoľvek viacnásobných kontrol a zosúhlasení s cieľom zabezpečiť zachovanie najvyššej úrovne integrity údajov. Tieto kontroly sa vykonávajú aj pri rekonštrukcii údajov od externých zainteresovaných strán s cieľom zabezpečiť konzistentnosť všetkých údajov medzi jednotlivými systémami.

Článok 13

Učenie sa a vývoj

1. Finančné subjekty musia mať k dispozícii spôsobilosti a personál na zhromažďovanie informácií o zraniteľných miestach a kybernetických hrozbách, incidentoch súvisiacich s IKT, najmä kybernetických útokoch, a analyzovanie vplyvu, ktorý pravdepodobne majú na ich digitálnu prevádzkovú odolnosť.

2. Finančné subjekty zavedú preskúmania realizované po incidentoch súvisiacich s IKT po tom, ako závažný incident súvisiaci s IKT narušil ich hlavné činnosti, pričom analyzujú príčiny narušenia a identifikujú požadované zlepšenia operácií IKT alebo zlepšenia v rámci politiky kontinuity činností v oblasti IKT uvedenej v článku 11.

Finančné subjekty iné ako mikropodniky na požiadanie oznámia príslušným orgánom zmeny, ktoré sa vykonali v nadväznosti na preskúmania realizované po incidentoch súvisiacich s IKT, ako sa uvádza v prvom pododseku.

V preskúmaniach realizovaných 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 závažnosť;

b) kvalitu a rýchlosť vykonania forenznej analýzy, ak sa to považuje za vhodné;

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 26 a 27, a z reálnych incidentov súvisiacich s IKT, najmä kybernetických útokov, spolu s výzvami, ktorým sa čelilo po aktivácii plánov kontinuity činností v oblasti IKT a plánov reakcie a obnovy v oblasti IKT spolu s príslušnými informáciami vymieňanými s protistranami a posudzovanými počas preskúmaní orgánmi dohľadu, sa náležite a nepretržite začleňujú do procesu posudzovania IKT rizika. Uvedené zistenia sa premietnu do vhodných preskúmaní príslušných zložiek rámca riadenia IKT rizika uvedeného v článku 6 ods. 1.

4. Finančné subjekty monitorujú účinnosť vykonávania svojej stratégie digitálnej prevádzkovej odolnosti stanovenej v článku 6 ods. 8 Mapujú vývoj v oblasti IKT rizika v priebehu času, analyzujú frekvenciu, druhy, rozsah a vývoj incidentov súvisiacich s IKT, najmä kybernetických útokov a ich spôsobov vedenia, s cieľom pochopiť úroveň vystavenia IKT riziku, najmä pokiaľ ide o kritické a dôležité funkcie, 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 školenia zamestnancov. Uvedené programy a školenia sa vzťahujú na všetkých zamestnancov a zamestnancov vrcholového manažmentu a majú takú úroveň zložitosti, ktorá zodpovedá rozsahu ich funkcií. Finančné subjekty v náležitých prípadoch zahrnú do svojich príslušných systémov školenia v súlade s článkom 30 ods. 2 písm. i) aj externých poskytovateľov IKT služieb.

7. Finančné subjekty iné ako mikropodniky 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 s cieľom účinne bojovať proti súčasným alebo novým formám kybernetických útokov.

Článok 14

Komunikácia

1. Finančné subjekty majú ako súčasť rámca riadenia IKT rizika uvedeného v článku 6 ods. 1 zavedené krízové komunikačné plány, ktoré umožňujú zodpovedné zverejňovanie aspoň závažných incidentov súvisiacich s IKT alebo zraniteľných miest pre klientov a protistrany, ako aj pre verejnosť, podľa konkrétneho prípadu.

2. Finančné subjekty vykonávajú ako súčasť rámca riadenia IKT rizika komunikačné politiky pre interných 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 zamestnancov zodpovedných za reakciu a obnovu, a zamestnancami, ktorí musia byť informovaní.

3. Aspoň jedna osoba vo finančnom subjekte musí byť poverená vykonávaním komunikačnej stratégie pre incidenty súvisiace s IKT a na tento účel plní funkciu styku s verejnosťou a médiami.

Článok 15

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

Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s Agentúrou Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) vypracujú spoločný návrh regulačných technických predpisov s cieľom:

a) bližšie špecifikovať ďalšie prvky, ktoré sa majú zahrnúť do bezpečnostných politík, postupov, protokolov a nástrojov v oblasti IKT uvedených v článku 9 ods. 2, aby sa zaistila bezpečnosť sietí, umožnili primerané záruky proti neoprávneným vniknutiam a zneužitiu údajov, zachovala dostupnosť, pravosť, integrita a dôvernosť údajov vrátane kryptografických techník, ako aj zaručil presný a rýchly prenos údajov bez závažných narušení a zbytočných omeškaní;

b) vypracovať ďalšie zložky kontrol práv na riadenie prístupu uvedené v článku 9 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 riziku prostredníctvom vhodných ukazovateľov, a to aj pokiaľ ide o modely využívania siete, hodiny, činnosť v oblasti IT a neznáme zariadenia;

c) ďalej rozvíjať mechanizmy uvedené v článku 10 ods. 1, ktoré umožňujú rýchle odhalenie anomálnych činností, a kritériá stanovené v článku 10 ods. 2, ktoré spúšťajú procesy zisťovania incidentov súvisiacich s IKT a reakcie na takéto incidenty;

d) bližšie špecifikovať zložky politiky kontinuity činností v oblasti IKT uvedenej v článku 11 ods. 1;

e) bližšie špecifikovať testovanie plánov kontinuity činností v oblasti IKT uvedené v článku 11 ods. 6 s cieľom zabezpečiť, aby takéto testovanie náležite zohľadnilo scenáre, v ktorých sa kvalita poskytovania kritickej alebo dôležitej funkcie zhoršuje na neprijateľnú úroveň alebo zlyháva, ako aj náležite zvážilo potenciálny vplyv platobnej neschopnosti alebo iných zlyhaní ktoréhokoľvek príslušného externého poskytovateľa IKT služieb a prípadne politické riziká v jurisdikciách príslušných poskytovateľov;

f) bližšie špecifikovať zložky plánov reakcie a obnovy v oblasti IKT uvedených v článku 11 ods. 3;

g) bližšie špecifikovať obsah a formát správy o preskúmaní rámca riadenia IKT rizika uvedenej v článku 6 ods. 5.

Pri vypracúvaní tohto návrhu regulačných technických predpisov európske orgány dohľadu zohľadňujú veľkosť a celkový rizikový profil finančného subjektu, ako aj povahu, rozsah a zložitosť jeho služieb, činností a operácií, pričom náležite zohľadňujú všetky osobitné vlastnosti vyplývajúce z odlišnej povahy činností v rôznych sektoroch finančných služieb.

Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. januára 2024.

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

Článok 16

Zjednodušený rámec riadenia IKT rizika

1. Články 5 až 15 tohto nariadenia sa neuplatňujú na malé a neprepojené investičné spoločnosti, platobné inštitúcie vyňaté podľa smernice (EÚ) 2015/2366; inštitúcie vyňaté podľa smernice 2013/36/EÚ, v súvislosti s ktorými sa členské štáty rozhodli neuplatňovať možnosť uvedenú v článku 2 ods. 4 tohto nariadenia, inštitúcie elektronického peňažníctva vyňaté podľa smernice 2009/110/ES; a malé inštitúcie zamestnaneckého dôchodkového zabezpečenia.

Bez toho, aby bol dotknutý prvý pododsek subjekty uvedené v prvom pododseku:

a) zavedú a udržiavajú spoľahlivý a zdokumentovaný rámec riadenia IKT rizika, v ktorom sa podrobne opisujú mechanizmy a opatrenia zamerané na rýchle, účinné a komplexné riadenie IKT rizika vrátane ochrany príslušných fyzických zložiek a infraštruktúr;

b) neustále monitorujú bezpečnosť a fungovanie všetkých IKT systémov;

c) minimalizujú vplyv IKT rizika využívaním spoľahlivých, odolných a aktualizovaných IKT systémov, protokolov a nástrojov, ktoré sú vhodné na podporu výkonu ich činností a poskytovania služieb a na primeranú ochranu dostupnosti, pravosti, integrity a dôvernosti údajov v sieťach a informačných systémoch;

d) umožňujú rýchlo identifikovať a odhaľovať zdroje IKT rizika a anomálií v sieťach a informačných systémoch a rýchlo riešiť incidenty súvisiace s IKT;

e) identifikujú kľúčové závislosti od externých poskytovateľov IKT služieb;

f) zabezpečujú kontinuitu kritických alebo dôležitých funkcií prostredníctvom plánov kontinuity činností a opatrení reakcie a obnovy, ktoré zahŕňajú aspoň záložné a reštaurovacie opatrenia;

g) pravidelne testujú plány a opatrenia uvedené v písmene f), ako aj účinnosť kontrol vykonaných v súlade s písmenami a) a c);

h) náležite vykonávajú príslušné operatívne závery, ktoré vyplývajú z testov uvedených v písmene g) a z analýzy po incidente, do procesu posudzovania IKT rizika a v súlade s potrebami a rizikovým profilom v oblasti IKT vypracúvajú programy zvyšovania informovanosti v oblasti bezpečnosti IKT a školenia digitálnej prevádzkovej odolnosti pre zamestnancov a manažment.

2. Rámec riadenia IKT rizika uvedený v odseku 1 druhom pododseku písm. a) sa pravidelne dokumentuje a preskúmava v prípade výskytu závažných incidentov súvisiacich s IKT v súlade s pokynmi orgánov dohľadu. Na základe skúseností získaných pri vykonávaní a monitorovaní sa rámec neustále vylepšuje. Správa o preskúmaní rámca riadenia IKT rizika sa predkladá príslušnému orgánu na jeho žiadosť.

3. Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s agentúrou ENISA vypracujú spoločný návrh regulačných technických predpisov s cieľom:

a) bližšie špecifikovať prvky, ktoré sa majú zahrnúť do rámca riadenia IKT rizika uvedeného v odseku 1 druhom pododseku písm. a);

b) bližšie špecifikovať prvky v súvislosti so systémami, protokolmi a nástrojmi na minimalizáciu vplyvu IKT rizika uvedeného v odseku 1 druhom pododseku písm. c) s cieľom zaistiť bezpečnosť sietí, umožniť primerané záruky proti vniknutiam a zneužitiu údajov a zachovať dostupnosť, pravosť integritu a dôvernosť údajov;

c) bližšie špecifikovať zložky plánov kontinuity činností v oblasti IKT uvedených v odseku 1 druhom pododseku písm. f);

d) bližšie špecifikovať pravidlá testovania plánov kontinuity činností a zabezpečiť účinnosť kontrol uvedených v odseku 1 druhom pododseku písm. g) a zabezpečiť, aby takéto testovanie náležite zohľadňovalo scenáre, v ktorých sa kvalita poskytovania kritickej alebo dôležitej funkcie zhoršuje na neprijateľnú úroveň alebo zlyháva;

e) bližšie špecifikovať obsah a formát správy o preskúmaní rámca riadenia IKT rizika uvedenej v odseku 2.

Pri vypracúvaní uvedeného návrhu regulačných technických predpisov by európske orgány dohľadu mali zohľadniť veľkosť a celkový rizikový profil finančného subjektu, ako aj povahu, rozsah a zložitosť jeho služieb, činností a operácií.

Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. januára 2024.

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. 1094/2010 a (EÚ) č. 1095/2010.

KAPITOLA III

Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT

Článok 17

Proces riadenia incidentov súvisiacich s IKT

1. Finančné subjekty vymedzia, zavedú a vykonávajú proces riadenia incidentov súvisiacich s IKT s cieľom odhaľovať, riadiť a oznamovať incidenty súvisiace s IKT.

2. Finančné subjekty zaznamenávajú všetky incidenty súvisiace s IKT a významné kybernetické hrozby. Finančné subjekty stanovia vhodné postupy a procesy na zaistenie konzistentného a integrovaného monitorovania, riešenia a následných opatrení v prípade incidentov súvisiacich s IKT s cieľom zabezpečiť, aby sa hlavné príčiny identifikovali, zdokumentovali a riešili s cieľom zabrániť výskytu takýchto incidentov.

3. V rámci procesu riadenia incidentov súvisiacich s IKT uvedeným v odseku 1 sa:

a) zavedú ukazovatele včasného varovania;

b) v súlade s kritériami stanovenými v článku 18 ods. 1 stanovia postupy na identifikáciu, sledovanie, zaznamenávanie, kategorizáciu a klasifikáciu incidentov súvisiacich s IKT podľa ich priority a závažnosti a podľa kritickosti zasiahnutých služieb;

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

d) stanovujú plány komunikácie so zamestnancami, externými zainteresovanými stranami a médiami v súlade s článkom 14 a plány oznamovania klientom, plány interných eskalačných postupov vrátane sťažností zákazníkov súvisiacich s IKT, ako aj plány poskytovania informácií finančným subjektom, ktoré konajú ako protistrany, vo vhodných prípadoch;

e) zabezpečujú, aby sa aspoň závažné incidenty súvisiace s IKT nahlasovali príslušnému vrcholovému manažmentu a informujú riadiaci orgán aspoň o závažných incidentoch súvisiacich s IKT, pričom vysvetlia vplyv, reakciu a dodatočné kontroly, ktoré sa majú zaviesť v dôsledku takýchto incidentov súvisiacich s IKT;

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

Článok 18

Klasifikácia incidentov súvisiacich s IKT a kybernetických hrozieb

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

a) počet a/alebo relevantnosť klientov alebo finančných protistrán a prípadne výška alebo počet transakcií, ktoré sú ovplyvnené 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, ktoré incident súvisiaci s IKT prináša v súvislosti s dostupnosťou, pravosťou, integritou alebo dôvernosťou údajov;

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

f) hospodársky vplyv, najmä priame a nepriame náklady a straty, incidentu súvisiaceho s IKT v absolútnom aj relatívnom vyjadrení.

2. Finančné subjekty klasifikujú kybernetické hrozby ako významné na základe kritickosti služieb vystavených riziku vrátane transakcií a operácií finančného subjektu, počtu a/alebo relevantnosti cieľových klientov alebo finančných protistrán a geografického rozloženia rizikových oblastí.

3. Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s ECB a agentúrou ENISA vypracuje spoločný návrh regulačných technických predpisov s cieľom bližšie špecifikovať:

a) kritériá stanovené v odseku 1 vrátane prahových hodnôt významnosti na určenie závažných incidentov súvisiacich s IKT alebo prípadne závažných prevádzkových alebo bezpečnostných incidentov súvisiacich s platbami, na ktoré sa vzťahuje nahlasovacia povinnosť stanovená v článku 19 ods. 1;

b) kritériá, ktoré majú príslušné orgány uplatňovať na účely posúdenia relevantnosti závažných incidentov súvisiacich s IKT alebo prípadne závažných prevádzkových alebo bezpečnostných incidentov súvisiacich s platbami na relevantné príslušné orgány v iných členských štátoch, ako aj podrobnosti hlásení o závažných incidentoch súvisiacich s IKT alebo prípadne závažných prevádzkových alebo bezpečnostných incidentov súvisiacich s platbami, ktoré sa majú poskytnúť iným príslušným orgánom podľa článku 19 ods. 6 a 7;

c) kritériá stanovené v odseku 2 tohto článku vrátane vysokých prahových hodnôt významnosti na určenie významných kybernetických hrozieb.

4. Pri vypracúvaní spoločného návrhu regulačných technických predpisov uvedeného v odseku 3 tohto článku európske orgány dohľadu zohľadňujú kritériá uvedené v článku 4 ods. 2, ako aj medzinárodné normy, usmernenia a špecifikácie vypracované a uverejnené agentúrou ENISA vrátane prípadných špecifikácií pre iné hospodárske odvetvia. Na účely uplatňovania kritérií stanovených v článku 4 ods. 2 európske orgány dohľadu náležite zvážia potrebu, aby mikropodniky a malé a stredné podniky mobilizovali dostatočné zdroje a kapacity na zabezpečenie rýchleho riadenia incidentov súvisiacich s IKT.

Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. januára 2024.

Na Komisiu sa deleguje právomoc doplniť toto nariadenie prijatím regulačných technických predpisov uvedených v odseku 3 v súlade s článkami 10 až 14 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010.

Článok 19

Nahlasovanie závažných incidentov súvisiacich s IKT a dobrovoľné oznamovanie významných kybernetických hrozieb

1. Finančné subjekty nahlasujú závažné incidenty súvisiace s IKT relevantnému príslušnému orgánu uvedenému v článku 46 v súlade s odsekom 4 tohto článku.

Ak finančný subjekt podlieha dohľadu viac ako jedného príslušného vnútroštátneho orgánu uvedeného v článku 46, členské štáty určia jediný príslušný orgán ako relevantný príslušný orgán zodpovedný za vykonávanie funkcií a povinností stanovených v tomto článku.

Úverové inštitúcie klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013 oznamujú závažné incidenty súvisiace s IKT relevantnému vnútroštátnemu príslušnému orgánu určenému v súlade s článkom 4 smernice 2013/36/EÚ, ktorý uvedenú správu bezodkladne zašle ECB.

Na účely prvého pododseku finančné subjekty vypracujú po získaní a analýze všetkých relevantných informácií počiatočné oznámenie a správy uvedené v odseku 4 tohto článku s použitím vzorov uvedených v článku 20 a predložia ich príslušnému orgánu. V prípade, že nie je technicky možné predložiť počiatočné oznámenia s použitím vzoru, finančné subjekty o tom informujú príslušný orgán alternatívnymi prostriedkami.

Počiatočné oznámenie a správy uvedené v odseku 4 obsahujú všetky informácie, ktoré príslušný orgán potrebuje na určenie významnosti závažného incidentu súvisiaceho s IKT a posúdenie možných cezhraničných vplyvov.

Bez toho, aby bolo dotknuté nahlasovanie podľa prvého pododseku zo strany finančného subjektu relevantnému príslušnému orgánu môžu členské štáty dodatočne stanoviť, aby niektoré alebo všetky finančné subjekty tiež poskytovali počiatočné oznámenie a každú správu uvedenú v odseku 4 tohto článku s použitím vzorov uvedených v článku 20 príslušným orgánom alebo jednotkami pre riešenie počítačových bezpečnostných incidentov (ďalej len „CSIRT“) určeným alebo zriadeným v súlade so smernicou (EÚ) 2022/2555.

2. Finančné subjekty môžu dobrovoľne oznamovať významné kybernetické hrozby relevantnému príslušnému orgánu, ak sa domnievajú, že hrozba je relevantná pre finančný systém, používateľov služieb alebo klientov. Relevantný príslušný orgán môže poskytnúť takéto informácie iným relevantným orgánom uvedeným v odseku 6.

Úverové inštitúcie klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013 môžu dobrovoľne oznamovať významné kybernetické hrozby relevantnému vnútroštátnemu príslušnému orgánu určenému v súlade s článkom 4 smernice 2013/36/EÚ, ktorý oznámenie bezodkladne zašle ECB.

Členské štáty môžu určiť, že tie finančné subjekty, ktoré dobrovoľne oznamujú v súlade s prvým pododsekom, môžu uvedené oznámenie zaslať aj jednotkám CSIRT určeným alebo zriadeným v súlade so smernicou (EÚ) 2022/2555.

3. Ak dôjde k závažnému incidentu súvisiacemu s IKT, ktorý má vplyv na finančné záujmy klientov, finančné subjekty bez zbytočného odkladu a čo najskôr po tom, ako o ňom nadobudli vedomosť, informujú svojich klientov o závažnom incidente súvisiacom s IKT a o opatreniach, ktoré boli prijaté na zmiernenie nepriaznivých účinkov takéhoto incidentu.

V prípade významnej kybernetickej hrozby finančné subjekty v náležitých prípadoch informujú svojich klientov, ktorí sú potenciálne dotknutí, o akýchkoľvek vhodných ochranných opatreniach, ktorých prijatie títo klienti môžu zvážiť.

4. Finančné subjekty v lehotách, ktoré sa stanovia v súlade s článkom 20 prvým odsekom písm. a) bodom ii), predložia relevantnému príslušnému orgánu:

a) počiatočné oznámenie;

b) priebežnú správu po počiatočnom oznámení uvedenom v písmene a), hneď ako sa výrazne zmení stav pôvodného incidentu alebo po zmene riešenia závažného incidentu súvisiaceho s IKT na základe nových dostupných informácií, po ktorej v náležitých prípadoch 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 vykonané zmierňujúce opatrenia, a keď sú k dispozícii skutočné údaje o vplyve, aby sa nahradili odhady.

5. Finančné subjekty môžu v súlade s odvetvovým právom Únie a vnútroštátnym odvetvovým právom zveriť nahlasovacie povinnosti podľa tohto článku externému poskytovateľovi služieb formou outsourcing. V prípade takéhoto outsourcingu je finančný subjekt naďalej plne zodpovedný za plnenie požiadaviek na nahlasovanie incidentov.

6. Po prijatí počiatočného oznámenia a každej správy uvedenej v odseku 4 príslušný orgán včas poskytne podrobné údaje o závažnom incidente súvisiacom s IKT týmto príjemcom, a to náležite na základe ich príslušných právomocí:

a) orgánom EBA, ESMA alebo EIOPA;

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

c) príslušným orgánom, jednotným kontaktným miestam alebo jednotkám CSIRT určeným alebo zriadeným v súlade so smernicou (EÚ) 2022/2555;

d) orgánom pre riešenie krízových situácií uvedeným v článku 3 smernice 2014/59/EÚ a Jednotnej rade pre riešenie krízových situácií (SRB), pokiaľ ide o subjekty uvedené v článku 7 ods. 2 nariadenia Európskeho parlamentu a Rady (EÚ) č. 806/2014 ([37]), a pokiaľ ide o subjekty a skupiny uvedené v článku 7 ods. 4 písm. b) a článku 7 ods. 5 nariadenia (EÚ) č. 806/2014, ak sa takéto údaje týkajú incidentov, ktoré predstavujú riziko pre zabezpečenie kritických funkcií v zmysle článku 2 ods. 1 bodu 35 smernice 2014/59/EÚ, a

e) iným príslušným verejným orgánom podľa vnútroštátneho práva.

7. Po prijatí informácií v súlade s odsekom 6 EBA, ESMA alebo EIOPA a ECB po konzultácii s agentúrou ENISA a v spolupráci s relevantným príslušným orgánom posúdia, či je závažný incident súvisiaci s IKT relevantný pre príslušné orgány v iných členských štátoch. Po tomto posúdení EBA, ESMA alebo EIOPA čo najskôr náležite informujú relevantné príslušné orgány v iných členských štátoch. 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.

([37]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 806/2014 z 15. júla 2014, ktorým sa stanovujú jednotné pravidlá a jednotný postup riešenia krízových situácií úverových inštitúcií a určitých investičných spoločností v rámci jednotného mechanizmu riešenia krízových situácií a jednotného fondu na riešenie krízových situácií a ktorým sa mení nariadenie (EÚ) č. 1093/2010 (Ú. v. EÚ L 225, 30.7.2014, s. 1).

8. Oznámením, ktoré má orgán ESMA vykonať podľa odseku 7 tohto článku, nie je dotknutá zodpovednosť príslušného orgánu bezodkladne zaslať podrobné údaje o závažnom incidente súvisiacom s IKT relevantnému orgánu v hostiteľskom členskom štáte, ak centrálny depozitár cenných papierov vykonáva významnú cezhraničnú činnosť v hostiteľskom členskom štáte, závažný incident súvisiaci s IKT bude mať pravdepodobne vážne dôsledky pre finančné trhy hostiteľského členského štátu a ak medzi príslušnými orgánmi existujú dohody o spolupráci týkajúce sa dohľadu nad finančnými subjektmi.

Článok 20

Harmonizácia obsahu a vzorov nahlasovania

Európske orgány dohľadu prostredníctvom spoločného výboru a po konzultácii s agentúrou ENISA a ECB vypracujú:

a) spoločný návrh regulačných technických predpisov s cieľom:

   i) stanoviť obsah správ závažných incidentov súvisiacich s IKT, aby sa zohľadnili kritériá stanovené v článku 18 ods. 1 a začlenili ďalšie prvky, ako napríklad podrobnosti na stanovenie relevantnosti nahlasovania pre iné členské štáty a toho, či predstavuje závažný prevádzkový alebo bezpečnostný incident súvisiaci s platbami alebo nie;

   ii) určiť lehoty pre počiatočné oznámenie a pre každú správu uvedenú v článku 19 ods. 4;

   iii) stanoviť obsah oznámenia o významných kybernetických hrozbách.

   Pri vypracúvaní tohto návrhu regulačných technických predpisov európske úrady dohľadu zohľadňujú veľkosť a celkový rizikový profil finančného subjektu a povahu, rozsah a zložitosť jeho služieb, činností a operácií, a najmä s cieľom zabezpečiť, aby na účely tohto odseku písm. a) bodu ii) mohli rôzne lehoty náležite odrážať osobitosti finančných sektorov bez toho, aby bolo dotknuté zachovanie konzistentného prístupu k nahlasovaniu incidentov súvisiacich s IKT podľa tohto nariadenia a smernice (EÚ) 2022/2555. Ak sa európske úrady dohľadu odchyľujú od prístupov prijatých v súvislosti s uvedenou smernicou, poskytnú odôvodnenie.

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

Európske úrady dohľadu predložia Komisii spoločný návrh regulačných technických predpisov uvedený v prvom odseku písm. a) a spoločný návrh vykonávacích technických predpisov uvedený v prvom odseku písm. b) do 17. júla 2024.

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

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

Článok 21

Centralizácia nahlasovania závažných incidentov súvisiacich s IKT

1. Európske úrady 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 spoločnej 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. Spoločná správa uvedená v odseku 1 obsahuje aspoň tieto prvky:

a) predpoklady na zriadenie jednotného centra EÚ;

b) prínosy, obmedzenia a riziká vrátane rizík spojených s vysokou koncentráciou citlivých informácií;

c) potrebnú spôsobilosť na zabezpečenie interoperability, pokiaľ ide o iné relevantné systémy nahlasovania;

d) prvky prevádzkového riadenia;

e) podmienky členstva;

f) technické dojednania prístupu finančných subjektov a príslušných vnútroštátnych orgánov k jednotnému centru EÚ;

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

3. Európske úrady dohľadu predložia správu uvedenú v odseku 1 Európskemu parlamentu, Rade a Komisii do 17. januára 2025.

Článok 22

Spätná väzba orgánov dohľadu

1. Bez toho, aby boli dotknuté technické vstupy, poradenstvo alebo nápravné opatrenia a následné úkony, ktoré jednotky CSIRT môžu v súlade s vnútroštátnym právom prípadne vykonať podľa smernice (EÚ) 2022/2555, príslušný orgán po prijatí počiatočného oznámenia a každej správy uvedenej v článku 19 ods. 4 potvrdí prijatie a v prípade, že je to uskutočniteľné, môže včas poskytnúť finančnému subjektu relevantnú a primeranú spätnú väzbu alebo usmernenie na vysokej úrovni, najmä sprístupnením akýchkoľvek relevantných anonymizovaných informácií a spravodajských informácií o podobných hrozbách, a môže prediskutovať nápravné opatrenia uplatnené na úrovni finančného subjektu a spôsoby minimalizovania a zmiernenia nepriaznivého vplyvu v celom finančnom sektore. Bez toho, aby bola dotknutá získaná spätná väzba orgánov dohľadu, finančné subjekty zostávajú plne zodpovedné za riešenie incidentov súvisiacich s IKT nahlásených podľa článku 19 ods. 1 a za ich dôsledky.

2. Európske úrady dohľadu podávajú každoročne prostredníctvom spoločného výboru anonymizované a súhrnné správy o závažných incidentoch súvisiacich s IKT, o ktorých ich informovali príslušné orgány v súlade s článkom 19 ods. 6, pričom uvedú aspoň počet závažných incidentov súvisiacich s IKT, ich povahu a ich vplyv na operácie finančných subjektov alebo klientov, prijaté nápravné opatrenia a vzniknuté náklady.

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

Článok 23

Prevádzkové alebo bezpečnostné incidenty súvisiace s platbami týkajúce sa úverových inštitúcií, platobných inštitúcií, poskytovateľov služieb informovania o účte a inštitúcií elektronického peňažníctva

Požiadavky stanovené v tejto kapitole sa vzťahujú aj na prevádzkové alebo bezpečnostné incidenty súvisiace s platbami a na závažné prevádzkové alebo bezpečnostné incidenty súvisiace s platbami, ak sa týkajú úverových inštitúcií, platobných inštitúcií, poskytovateľov služieb informovania o účte a inštitúcií elektronického peňažníctva.

KAPITOLA IV

Testovanie digitálnej prevádzkovej odolnosti

Článok 24

Všeobecné požiadavky na vykonávanie testovania digitálnej prevádzkovej odolnosti

1. Na účely posúdenia pripravenosti riešiť incidenty súvisiace s IKT, identifikácie slabých miest, nedostatkov a medzier v digitálnej prevádzkovej odolnosti a urýchleného vykonania nápravných opatrení finančné subjekty iné ako mikropodniky zriadia, udržiavajú a preskúmavajú spoľahlivý a komplexný program testovania digitálnej prevádzkovej odolnosti ako integrálnu súčasť rámca riadenia IKT rizika uvedeného v článku 6, pričom zohľadňujú kritériá stanovené v článku 4 ods. 2.

2. Program na testovanie digitálnej prevádzkovej odolnosti zahŕňa celý rad posúdení, testov, metodík, postupov a nástrojov, ktoré sa majú uplatňovať v súlade s článkami 25 a 26.

3. Pri vykonávaní programu testovania digitálnej prevádzkovej odolnosti uvedeného v odseku 1 tohto článku sa finančné subjekty iné ako mikropodniky riadia prístupom založeným na riziku, zohľadňujúc kritériá stanovené v článku 4 ods. 2, pričom náležite prihliadajú na vyvíjajúce sa prostredie IKT rizika, všetky špecifické riziká, ktorým je alebo by mohol byť dotknutý finančný subjekt vystavený, kritickosť informačných aktív a poskytovaných služieb, ako aj akýkoľvek iný faktor, ktorý finančný subjekt považuje za vhodný.

4. Finančné subjekty iné ako mikropodniky zabezpečia, aby testy vykonávali nezávislé strany, či už interné alebo externé. Ak testy vykonáva interný testovací subjekt, finančné subjekty vyčlenia dostatočné zdroje a zabezpečia, aby sa vo fáze navrhovania a vykonávania testu zabránilo konfliktom záujmov.

5. Finančné subjekty iné ako mikropodniky stanovia postupy a politiky na určenie priorít, klasifikáciu a nápravu všetkých problémov odhalených počas vykonávania testov a zavedú interné metodiky validácie s cieľom zabezpečiť úplné riešenie všetkých zistených slabých miest, nedostatkov a medzier.

6. Finančné subjekty iné ako mikropodniky zabezpečia, aby sa aspoň raz ročne vykonávali vhodné testy všetkých IKT systémov a aplikácií podporujúcich kritické alebo dôležité funkcie.

Článok 25

Testovanie IKT nástrojov a systémov

1. V rámci programu testovania digitálnej prevádzkovej odolnosti uvedeného v článku 24 sa v súlade s kritériami stanovenými v článku 4 ods. 2 zabezpečí vykonanie vhodných testov, ako sú posúdenia a vyhľadávania zraniteľnosti, analýzy otvorených zdrojov (analýzy open-source riešení), 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, testovania kompatibility, testovania výkonnosti, testovania medzi koncovými bodmi (end-to-end testovania) a penetračné testovania.

2. Centrálni depozitári cenných papierov a centrálne protistrany vykonávajú posúdenia zraniteľnosti pred akýmkoľvek nasadením alebo opätovným nasadením nových alebo existujúcich aplikácií a zložiek infraštruktúry a IKT služieb podporujúcich kritické alebo dôležité funkcie finančného subjektu.

3. Mikropodniky vykonávajú testy uvedené v odseku 1 tak, že kombinujú prístup založený na riziku so strategickým plánovaním testovania IKT, pričom náležite zohľadňujú potrebu zachovať vyvážený prístup medzi rozsahom zdrojov a časom, ktorý sa má venovať testovaniu IKT stanovenému v tomto článku, na jednej strane a naliehavosťou, typom rizika, kritickosťou informačných aktív a poskytovaných služieb, ako aj akýmkoľvek iným relevantným faktorom vrátane schopnosti finančného subjektu podstupovať predvídané riziká na strane druhej.

Článok 26

Pokročilé testovanie IKT nástrojov, systémov a procesov vychádzajúce z TLPT

1. Finančné subjekty iné ako subjekty uvedené v článku 16 ods. 1 prvom pododseku a iné ako mikropodniky, ktoré sú identifikované v súlade s odsekom 8 tretím pododsekom tohto článku, vykonávajú aspoň každé tri roky pokročilé testovanie prostredníctvom TLPT. Na základe rizikového profilu finančného subjektu a s prihliadnutím na prevádzkové okolnosti môže príslušný orgán v prípade potreby požiadať finančný subjekt o zníženie alebo zvýšenie tejto frekvencie.

2. Každý penetračný test na základe konkrétnej hrozby zahŕňa viaceré alebo všetky kritické alebo dôležité funkcie finančného subjektu a vykonáva sa na živých produkčných systémoch podporujúcich takéto funkcie.

Finančné subjekty identifikujú všetky relevantné podkladové IKT systémy, procesy a technológie podporujúce kritické alebo dôležité funkcie a všetky relevantné IKT služby vrátane tých, ktoré podporujú kritické alebo dôležité funkcie, ktoré sú externe zabezpečované formou outsourcingu alebo zmluvne dohodnuté s externým poskytovateľom IKT služieb.

Finančné subjekty posúdia, na ktoré kritické alebo dôležité funkcie, sa TLPT musí vzťahovať. Výsledok tohto posúdenia určí presný rozsah TLPT a validujú ho príslušné orgány.

3. Ak sú externí poskytovatelia IKT služieb zahrnutí do rozsahu pôsobnosti TLPT, finančný subjekt prijme potrebné opatrenia a záruky na zabezpečenie účasti takýchto externých poskytovateľov IKT služieb na TLPT a vždy si ponechá plnú zodpovednosť za zabezpečenie súladu s týmto nariadením.

4. Bez toho, aby bol dotknutý odsek 2 prvý a druhý pododsek, ak sa opodstatnene očakáva, že účasť externého poskytovateľa IKT služieb na TLPT uvedenom v odseku 3, by mala nepriaznivý vplyv na kvalitu alebo bezpečnosť služieb, ktoré externý poskytovateľ IKT služieb poskytuje zákazníkom, ktorí sú subjektmi, na ktoré sa toto nariadenie nevzťahuje, alebo na dôvernosť údajov súvisiacich s takýmito službami, finančný subjekt a externý poskytovateľ IKT služieb sa môžu písomne dohodnúť, že externý poskytovateľ IKT služieb priamo vstúpi do zmluvných dojednaní s externým testovacím subjektom na účely vykonania združeného TLPT riadeného jedným určeným finančným subjektom, ktoré zahŕňa niekoľko finančných subjektov (ďalej len „združené testovanie“), ktorým externý poskytovateľ IKT služieb poskytuje IKT služby.

Toto združené testovanie sa vzťahuje na príslušnú škálu IKT služieb podporujúcich kritické alebo dôležité funkcie, v súvislosti s ktorými finančné subjekty uzavreli zmluvy s príslušným externým poskytovateľom IKT služieb. Združené testovanie sa považuje za TLPT vykonané finančnými subjektmi, ktoré sa zúčastňujú na združenom testovaní.

Počet finančných subjektov zúčastňujúcich sa na združenom testovaní sa náležite kalibruje s prihliadnutím na zložitosť a typy príslušných služieb.

5. Finančné subjekty v spolupráci s externými poskytovateľmi IKT služieb a inými zainteresovanými stranami vrátane testovacích subjektov, ale s výnimkou príslušných orgánov, uplatňujú účinné kontroly riadenia rizík s cieľom zmierniť riziká akéhokoľvek potenciálneho vplyvu na údaje, poškodenie aktív a narušenie kritických alebo dôležitých funkcií, služieb alebo operácií samotného finančného subjektu, jeho protistrán alebo finančného sektora.

6. Na konci testovania po schválení správ a plánov nápravy finančný subjekt a v náležitých prípadoch externé testovacie subjekty poskytnú orgánu určenému v súlade s odsekom 9 alebo 10 zhrnutie príslušných zistení, plány nápravy a dokumentáciu preukazujúcu, že TLPT bolo vykonané v súlade s požiadavkami.

7. Orgány poskytnú finančným subjektom osvedčenie potvrdzujúce, že test bol vykonaný v súlade s požiadavkami uvedenými v dokumentácii, aby mohli príslušné orgány tieto penetračné testy na základe konkrétnej hrozby navzájom uznávať. Finančný subjekt oznámi osvedčenie, zhrnutie relevantných zistení a plány nápravy relevantnému príslušnému orgánu.

Bez toho, aby bolo dotknuté takéto osvedčenie, finančné subjekty zostávajú vždy plne zodpovedné za dôsledky testov uvedených v odseku 4.

8. Finančné subjekty uzatvárajú zmluvy s testovacími subjektmi na účely vykonávania TLPT v súlade s článkom 27. Ak finančné subjekty využívajú interné testovacie subjekty na účely vykonávania TLPT, uzatvoria zmluvu s externými testovacími subjektmi po každom treťom testovaní.

Úverové inštitúcie, ktoré sú klasifikované ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013, využívajú len externé testovacie subjekty v súlade s článkom 27 ods. 1 písm. a) až e).

Príslušné orgány určia finančné subjekty, od ktorých sa vyžaduje vykonávanie TLPT, pričom zohľadnia kritériá stanovené v článku 4 ods. 2, a to na základe posúdenia:

a) faktorov súvisiacich s vplyvom, najmä rozsahom, v akom služby poskytované a činnosti vykonávané finančným subjektom majú vplyv na finančný sektor;

b) prípadných obáv o finančnú stabilitu vrátane systémového charakteru finančného subjektu na úrovni Únie alebo na vnútroštátnej úrovni, podľa toho, čo je uplatniteľné;

c) konkrétneho IKT rizikového profilu, úrovne IKT vyspelosti finančného subjektu alebo súvisiacich technologických prvkov.

9. Členské štáty môžu určiť jeden verejný orgán vo finančnom sektore, ktorý bude zodpovedný za záležitosti súvisiace s TLPT vo finančnom sektore na vnútroštátnej úrovni, a poveria ho všetkými právomocami a úlohami na tento účel.

10. Ak neexistuje určenie v súlade s odsekom 9 tohto článku a bez toho, aby bola dotknutá právomoc identifikovať finančné subjekty, od ktorých sa vyžaduje, aby vykonávali TLPT, príslušný orgán môže delegovať vykonávanie niektorých alebo všetkých úloh uvedených v tomto článku a článku 27 na iný vnútroštátny orgán vo finančnom sektore.

11. Európske orgány dohľadu po dohode s *ECB* vypracujú spoločný návrh regulačných technických predpisov *v* súlade s rámcom TIBER–EU s cieľom bližšie špecifikovať:

a) kritériá používané na účely uplatňovania odseku 8 druhého pododseku;

b) požiadavky a normy, ktorými sa riadi využívanie interných testovacích subjektov;

c) požiadavky v súvislosti s:

   i) rozsahom pôsobnosti TLPT uvedeným v odseku 2;

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

   iii) výsledkami, záverečnými a nápravnými štádiami testovania;

d) druh spolupráce v oblasti dohľadu a v iných relevantných oblastiach, ktorá je potrebná na vykonávanie TLPT, ako aj na uľahčenie vzájomného uznávania uvedeného testovania 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.

Pri vypracúvaní tohto návrhu regulačných technických predpisov európske orgány dohľadu náležite zohľadnia všetky špecifické aspekty vyplývajúce z odlišnej povahy činností v rôznych sektoroch finančných služieb.

Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. júla 2024.

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. 1094/2010 a (EÚ) č. 1095/2010.

Článok 27

Požiadavky na testovacie subjekty pri vykonávaní TLPT

1. Finančné subjekty využívajú na vykonávanie TLPT iba testovacie subjekty, ktoré:

a) sú najvhodnejšie a najuznávanejšie;

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

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

d) poskytujú nezávislé uistenie alebo audítorskú správu v súvislosti so správnym riadením rizík spojených s vykonávaním TLPT vrátane náležitej ochrany dôverných informácií finančného subjektu a nápravy obchodných rizík finančného subjektu;

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

2. Ak využívajú interné testovacie subjekty, finančné subjekty musia zabezpečiť, aby okrem požiadaviek v odseku 1, boli splnené aj tieto podmienky:

a) takéto využitie schválil relevantný príslušný orgán alebo jeden verejný orgán určený v súlade s článkom 26 ods. 9 a 10;

b) relevantný príslušný orgán overil, že finančný subjekt má dostatočné vyčlenené zdroje a zabezpečil, aby sa vo fáze navrhovania a vykonávania testu zabránilo konfliktom záujmov, a

c) poskytovateľ spravodajských informácií o hrozbách je vo vzťahu k finančnému subjektu externým subjektom.

3. Finančné subjekty zabezpečia, aby sa v zmluvách uzavretých s externými testovacími subjektmi vyžadovalo správne riadenie výsledkov TLPT a aby akékoľvek spracúvanie z toho vyplývajúcich údajov vrátane akéhokoľvek generovania, uchovávania, agregácie, navrhovania, podávania správ, komunikácie alebo likvidácie nevytváralo pre finančný subjekt riziká.

KAPITOLA V

Riadenie externého IKT rizika

Oddiel I

Kľúčové zásady správneho riadenia externého IKT rizika

Článok 28

Všeobecné zásady

1. Finančné subjekty riadia externé IKT riziko ako integrálnu súčasť IKT rizika v medziach svojho rámca riadenia IKT rizika, ako je uvedené v článku 6 ods. 1, a v súlade s týmito zásadami:

a) 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 uplatniteľného práva v oblasti finančných službách;

b) riadenie externého IKT rizika finančnými subjektmi sa vykonáva so zreteľom na zásadu proporcionality, pričom sa zohľadňujú tieto aspekty:

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

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

2. Finančné subjekty iné ako subjekty uvedené v článku 16 ods. 1 prvom pododseku a iné ako mikropodniky prijmú a pravidelne preskúmavajú stratégiu týkajúcu sa externého IKT rizika ako súčasť svojho rámca riadenia IKT rizika, pričom v náležitých prípadoch zohľadnia stratégiu viacerých dodávateľov uvedenú v článku 6 ods. 9 Stratégia týkajúca sa externého IKT rizika zahŕňa politiku využívania IKT služieb podporujúcich kritické alebo dôležité funkcie poskytované externými poskytovateľmi IKT služieb a uplatňuje sa na individuálnom, a v relevantných prípadoch na subkonsolidovanom a konsolidovanom základe. Riadiaci orgán na základe posúdenia celkového rizikového profilu finančného subjektu a rozsahu a zložitosti obchodných služieb pravidelne preskúmava riziká identifikované v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie.

3. 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 IKT služby podporujúce kritické alebo dôležité funkcie, a tými, ktoré sa na ne nevzťahujú.

Finančné subjekty aspoň raz ročne nahlasujú príslušným orgánom počet nových dojednaní o využívaní IKT služieb, kategórie externých poskytovateľov IKT služieb, druh zmluvných dojednaní a poskytované IKT služby a funkcie.

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 každom plánovanom zmluvnom dojednaní o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie, ako aj o tom, kedy sa funkcia stala kritickou alebo dôležitou.

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

a) posúdia, či sa zmluvné dojednanie vzťahuje na využívanie IKT služieb podporujúcich kritickú alebo dôležitú funkciu;

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

c) identifikujú a posúdia všetky relevantné riziká v súvislosti so zmluvným dojednaním vrátane možnosti, že takéto zmluvné dojednania môžu prispieť k posilneniu rizika koncentrácie IKT, ako sa uvádza v článku 29;

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) identifikujú a posúdia konflikty záujmu, ktoré môže zmluvné dojednanie spôsobiť.

5. Finančné subjekty môžu uzatvárať zmluvné dojednania len s externými poskytovateľmi IKT služieb, ktorí spĺňajú primerané normy v oblasti informačnej bezpečnosti. V prípade, že sa uvedené zmluvné dojednania týkajú kritických alebo dôležitých funkcií, finančné subjekty pred uzatvorením dojednaní náležite zohľadnia, ako externí poskytovatelia IKT služieb využívajú najaktuálnejšie a najprísnejšie normy kvality v oblasti informačnej bezpečnosti.

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

V prípade, že zmluvné dojednania o využívaní IKT služieb uzatvorené s externými poskytovateľmi IKT služieb so sebou prinášajú vysokú technickú zložitosť, finančný subjekt overí, či audítori, a to interní alebo externí, alebo združenie audítorov, majú primerané zručnosti a znalosti na účinné vykonávanie príslušných auditov a posúdení.

7. Finančné subjekty zabezpečia, aby sa zmluvné dojednania o využívaní IKT služieb mohli ukončiť za ktorýchkoľvek z týchto okolností:

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

b) okolnosti zistené počas monitorovania externého IKT rizika, 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 slabé stránky externého poskytovateľa IKT služieb, týkajúce sa jeho celkového riadenia IKT rizika, a najmä spôsobu, akým zaisťuje dostupnosť, pravosť, integritu a dôvernosť údajov, či už osobných alebo inak citlivých údajov, alebo iných ako osobných údajov;

d) ak príslušný orgán už nemôže účinne vykonávať dohľad nad finančným subjektom v dôsledku podmienok alebo okolností súvisiacich s príslušným zmluvným dojednaním.

8. Pokiaľ ide o IKT služby podporujúce kritické alebo dôležité funkcie, finančné subjekty zavedú stratégie ukončenia angažovanosti. Stratégie ukončenia angažovanosti zohľadňujú riziká, ktoré môžu vzniknúť na úrovni externých poskytovateľov IKT služieb, najmä ich možné zlyhanie, zhoršenie kvality poskytovaných IKT služieb, akékoľvek narušenie obchodnej činnosti v dôsledku neprimeraného alebo neúspešného poskytovania IKT služieb alebo akéhokoľvek závažného rizika vyplývajúceho z primeraného a nepretržitého využívania príslušnej IKT služby, alebo v prípade ukončenia zmluvných dojednaní s externými poskytovateľmi IKT služieb za akýchkoľvek okolností uvedených v odseku 7.

Finančné subjekty zabezpečia, aby mohli ukončiť zmluvné dojednania bez:

a) narušenia svojej obchodnej činnosti;

b) obmedzenia dodržiavania regulačných požiadaviek;

c) ohrozenia kontinuity a kvality služieb poskytovaných klientom.

Plány ukončenia angažovanosti musia byť komplexné, zdokumentované a v súlade s kritériami stanovenými v článku 4 ods. 2 dostatočne otestované a pravidelne preskúmavané.

Finančné subjekty určia alternatívne riešenia a vypracujú plány transformácie, ktoré im umožnia odstrániť zmluvne dohodnuté IKT služby 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 majú zavedené primerané pohotovostné opatrenia na zachovanie kontinuity činností v prípade okolností uvedených v prvom pododseku.

9. Európske orgány dohľadu vypracujú prostredníctvom spoločného výboru návrh vykonávacích technických predpisov na stanovenie štandardných vzorov na účely registra informácií uvedeného v odseku 3 vrátane informácií, ktoré sú spoločné pre všetky zmluvné dojednania o využívaní IKT služieb. Európske orgány dohľadu predložia uvedený návrh vykonávacích technických predpisov Komisii do 17. januára 2024.

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

10. Európske orgány dohľadu prostredníctvom spoločného výboru vypracujú návrh regulačných technických predpisov s cieľom bližšie špecifikovať podrobný obsah politiky uvedenej v odseku 2 v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie, ktoré poskytujú externí poskytovatelia IKT služieb.

Európske orgány dohľadu pri vypracúvaní tohto návrhu regulačných technických predpisov zohľadňujú veľkosť a celkový rizikový profil finančného subjektu, ako aj povahu, rozsah a zložitosť jeho služieb, činností a operácií. Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. januára 2024.

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. 1094/2010 a (EÚ) č. 1095/2010.

Článok 29

Predbežné posúdenie rizika koncentrácie IKT na úrovni subjektu

1. Pri vykonávaní identifikácie a posudzovania rizík uvedených v článku 28 ods. 4 písm. c) finančné subjekty zohľadňujú aj to, či by plánované uzavretie zmluvného dojednania v súvislosti s IKT službami podporujúcimi kritické alebo dôležité funkcie 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 podporujúcich kritické alebo dôležité funkcie 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 dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie zahŕňajú možnosť, že externý poskytovateľ IKT služieb ďalej subdodávateľsky zabezpečí IKT služby podporujúce kritickú alebo dôležitú funkciu iným externým poskytovateľom IKT služieb, finančné subjekty zvážia prínosy a riziká, ktoré môžu vzniknúť v súvislosti s takýmto subdodávateľským zabezpečením, najmä v prípade subdodávateľa IKT usadeného v tretej krajine.

Ak sa zmluvné dojednania týkajú IKT služieb podporujúcich kritické alebo dôležité funkcie, finančné subjekty náležite zohľadnia ustanovenia insolvenčného práva, ktoré by sa uplatnili v prípade konkurzu externého poskytovateľa IKT služieb, ako aj akékoľvek obmedzenia, ktoré môžu vzniknúť v súvislosti s naliehavým obnovením údajov finančného subjektu.

Ak sa zmluvné dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie uzatvoria s externým poskytovateľom IKT služieb usadeným v tretej krajine, finančné subjekty okrem aspektov uvedených v druhom pododseku zvážia aj súlad s pravidlami Únie v oblasti ochrany údajov a účinné presadzovanie práva v tejto tretej krajine.

Ak zmluvné dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie umožňujú využívanie subdodávateľských vzťahov, 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 účinne vykonávať dohľad nad finančným subjektom v tejto súvislosti.

Článok 30

Kľúčové zmluvné ustanovenia

1. Práva a povinnosti finančného subjektu a externého poskytovateľa IKT služieb sa jasne pridelia a stanovia písomne. Úplná zmluva zahŕňa dohody o úrovni poskytovaných služieb a zdokumentuje sa v jednom písomnom dokumente, ktorý majú zmluvné strany k dispozícii v papierovej forme, alebo v dokumente v inom stiahnuteľnom, trvalom a prístupnom formáte.

2. Zmluvné dojednania o využívaní IKT služieb zahŕňajú aspoň tieto prvky:

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

b) miesta, konkrétne regióny alebo krajiny, kde sa majú poskytovať zmluvne dohodnuté alebo subdodávateľsky zabezpečované funkcie a IKT služby a kde sa majú údaje spracúvať vrátane miesta uchovávania, ako aj požiadavka, aby externý poskytovateľ IKT služieb vopred informoval finančný subjekt, ak plánuje zmeniť takéto miesto;

c) ustanovenia o dostupnosti, pravosti, integrite alebo dôvernosti v súvislosti s ochranou údajov vrátane osobných údajov;

d) ustanovenia o zabezpečení obnovy a návratu osobných údajov a iných ako osobných údajov spracúvaných finančným subjektom v ľahko prístupnom formáte v prípade platobnej neschopnosti, riešenia krízových situácií alebo ukončenia obchodných operácií externého poskytovateľa IKT služieb, alebo v prípade ukončenia zmluvných dojednaní, a prístupu k takýmto údajom;

e) opis úrovne poskytovaných služieb vrátane ich aktualizácií a revízií;

f) povinnosť externého poskytovateľa IKT služieb poskytovať pomoc finančnému subjektu bez dodatočných nákladov alebo za náklady stanovené ex ante, keď dôjde k IKT incidentu, ktorý súvisí s IKT službou poskytnutou finančnému subjektu;

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

h) právo ukončiť zmluvný vzťah a súvisiaca minimálna výpovedná lehota na ukončenie zmluvných dojednaní v súlade s očakávaniami príslušných orgánov a orgánov pre riešenie krízových situácií;

i) podmienky účasti externých poskytovateľov IKT služieb na programoch zvyšovania informovanosti finančných subjektov v oblasti bezpečnosti IKT a na školení v oblasti digitálnej prevádzkovej odolnosti v súlade s článkom 13 ods. 6

3. Zmluvné dojednania o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie zahŕňajú okrem prvkov uvedených v odseku 2 aspoň tieto prvky:

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

b) výpovedné lehoty a nahlasovacie povinnosti externého poskytovateľa IKT služieb voči finančnému subjektu vrátane oznamovania akéhokoľvek vývoja, ktorý by mohol mať významný vplyv na schopnosť externého poskytovateľa IKT služieb účinne poskytovať IKT služby podporujúce kritické alebo dôležité funkcie v súlade s dohodnutými úrovňami služieb;

c) 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 poskytujú primeranú úroveň bezpečnosti na poskytovanie služieb zo strany finančného subjektu v súlade s jeho regulačným rámcom;

d) povinnosť externého poskytovateľa IKT služieb zúčastňovať sa a plne spolupracovať na TLPT finančného subjektu, ako sa uvádza v článkoch 26 a 27;

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

i) neobmedzené práva na prístup, inšpekciu a audit vykonávané finančným subjektom alebo vymenovanou treťou stranou a príslušným orgánom, ako aj právo vyhotovovať kópie príslušnej dokumentácie na mieste, ak je kritická pre operácie externého poskytovateľa IKT služieb, 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) povinnosť externého poskytovateľa IKT služieb plne spolupracovať počas inšpekcií na mieste a auditov vykonávaných príslušnými orgánmi, hlavným orgánom dozoru, finančným subjektom alebo vymenovanou treťou stranou; a

iv) povinnosť poskytnúť podrobnosti o rozsahu, postupoch, ktoré sa majú dodržiavať, a frekvencii takýchto inšpekcií a auditov;

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

i) počas ktorého bude externý poskytovateľ IKT služieb naďalej poskytovať príslušné funkcie alebo IKT služby s cieľom znížiť riziko narušenia na úrovni finančného subjektu alebo zabezpečiť efektívne riešenie jeho krízovej situácie a reštrukturalizáciu;

ii) ktoré umožňuje finančnému subjektu prejsť k inému externému poskytovateľovi IKT služieb alebo začať využívať vlastné riešenia v závislosti od zložitosti poskytovanej služby.

Odchylne od písmena e) sa externý poskytovateľ IKT služieb a finančný subjekt, ktorý je mikropodnikom, môžu dohodnúť, že práva finančného subjektu na prístup, inšpekciu a audit možno delegovať na nezávislú tretiu stranu, ktorú určí externý poskytovateľ IKT služieb, a že finančný subjekt môže kedykoľvek od tretej strany požadovať informácie a uistenie o výkonnosti externého poskytovateľa IKT služieb.

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

5. Európske orgány dohľadu prostredníctvom spoločného výboru vypracujú návrh regulačných technických predpisov s cieľom bližšie špecifikovať prvky uvedené v odseku 2 písm. a), ktoré musí finančný subjekt určiť a posúdiť pri využívaní subdodávateľov v prípade IKT služieb podporujúcich kritické alebo dôležité funkcie.

Pri vypracúvaní uvedeného návrhu regulačných technických predpisov by Európske orgány dohľadu mali zohľadniť veľkosť a celkový rizikový profil finančného subjektu, ako aj povahu, rozsah a zložitosť jeho služieb, činností a operácií.

Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. júla 2024.

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. 1094/2010 a (EÚ) č. 1095/2010.

Oddiel II

Rámec dozoru nad kritickými externými poskytovateľmi IKT služieb

Článok 31

Určenie kritických externých poskytovateľov IKT služieb

1. Európske orgány dohľadu prostredníctvom spoločného výboru a na základe odporúčania fóra pre dozor zriadeného podľa článku 32 ods. 1:

a) určia externých poskytovateľov IKT služieb, ktorí sú pre finančné subjekty kritickí, a to na základe posúdenia, ktoré zohľadňuje kritériá uvedené v odseku 2;

b) vymenujú za hlavný orgán dozoru pre každého kritického externého poskytovateľa IKT služieb európsky orgán dohľadu, ktorý je v súlade s nariadením (EÚ) č. 1093/2010 (EÚ), (EÚ) č. 1094/2010 alebo (EÚ) č. 1095/2010 zodpovedný za finančné subjekty, ktoré majú spolu najväčší podiel celkových aktív na hodnote celkových aktív všetkých finančných subjektov využívajúcich služby príslušného kritického externého poskytovateľa IKT služieb, ako to dokazuje suma individuálnych súvah uvedených finančných subjektov.

2. Určenie uvedené v odseku 1 písm. a) vychádza v súvislosti s IKT službami poskytovanými externým poskytovateľom IKT služieb 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 v poskytovaní svojich služieb, so zohľadnením počtu finančných subjektov a celkovej hodnoty aktív 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 (ďalej len „G-SII“) alebo inak systémovo významných inštitúcií (ďalej len „O-SII“), ktoré závisia od príslušného externého poskytovateľa IKT služieb;

   ii) vzájomná závislosť medzi G-SII alebo O-SII uvedenými 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 prostredníctvom subdodávateľských dojednaní;

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

   i) neexistencia skutočných, hoci len 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 v súvislosti s čiastočným alebo úplným presunom príslušných údajov a pracovného zaťaženia z príslušného externého poskytovateľa IKT služieb na iného externého poskytovateľa IKT služieb, a to buď z dôvodu značných finančných nákladov, času alebo iných zdrojov, ktoré môže takýto presun predstavovať, alebo z dôvodu zvýšeného IKT rizika alebo iných prevádzkových rizík, ktorým môže byť finančný subjekt vystavený pri takomto presune.

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

4. Kritickí externí poskytovatelia IKT služieb, ktorí sú súčasťou skupiny, určia jednu právnickú osobu ako koordinačné miesto na zabezpečenie primeraného zastúpenia a komunikácie s hlavným orgánom dozoru.

5. Hlavný orgán dozoru oznámi externému poskytovateľovi IKT služieb výsledok posúdenia vedúceho k určeniu uvedenému v odseku 1 písm. a). Do šiestich týždňov od dátumu oznámenia môže externý poskytovateľ IKT služieb predložiť hlavnému orgánu dozoru odôvodnené vyhlásenie so všetkými relevantnými informáciami na účely posúdenia. Hlavný orgán dozoru zváži odôvodnené vyhlásenie a môže požiadať o predloženie dodatočných informácií do 30 kalendárnych dní od prijatia takéhoto vyhlásenia.

Po určení externého poskytovateľa IKT služieb za kritického európske orgány dohľadu prostredníctvom spoločného výboru oznámia externému poskytovateľovi IKT služieb takéto určenie a dátum, od ktorého bude skutočne podliehať činnostiam dozoru. Uvedený počiatočný dátum nesmie byť neskôr ako jeden mesiac po oznámení. Externý poskytovateľ IKT služieb oznámi finančným subjektom, ktorým poskytuje služby, že bol určený ako kritický.

6. Komisia je splnomocnená prijať delegovaný akt v súlade s článkom 57 na doplnenie tohto nariadenia bližšou špecifikáciou kritérií uvedených v odseku 2 tohto článku do 17. júla 2024.

7. Určenie uvedené v odseku 1 písm. a) sa nepoužije dovtedy, kým Komisia neprijme delegovaný akt v súlade s odsekom 6.

8. Určenie uvedené v odseku 1 písm. a) sa nevzťahuje na:

i) finančné subjekty poskytujúce IKT služby iným finančným subjektom;

ii) externých poskytovateľov IKT služieb, ktorí podliehajú rámcom dozoru zriadeným na účely podpory úloh uvedených v článku 127 ods. 2 Zmluvy o fungovaní Európskej únie;

iii) vnútroskupinových poskytovateľov IKT služieb;

iv) externých poskytovateľov IKT služieb, ktorí poskytujú IKT služby výhradne v jednom členskom štáte finančným subjektom, ktoré pôsobia len v danom členskom štáte.

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

10. Na účely odseku 1 písm. a) príslušné orgány každoročne a súhrnne zasielajú správy uvedené v článku 28 ods. 3 treťom pododseku fóru pre dozor zriadenému podľa článku 32. Fórum pre dozor posudzuje externé závislosti finančných subjektov v oblasti IKT na základe informácií získaných od príslušných orgánov.

11. Externí poskytovatelia IKT služieb, ktorí nie sú zahrnutí v zozname uvedenom v odseku 9, môžu požiadať, aby boli určení ako kritickí v súlade s odsekom 1 písm. a).

Na účely prvého pododseku externý poskytovateľ IKT služieb predloží odôvodnenú žiadosť orgánom EBA, ESMA alebo EIOPA, ktoré prostredníctvom spoločného výboru rozhodnú o tom, či určiť tohto externého poskytovateľa IKT služieb ako kritického 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.

12. Finančné subjekty využívajú služby externého poskytovateľa IKT služieb usadeného v tretej krajine, ktorý bol určený ako kritický v súlade s odsekom 1 písm. a), len ak tento poskytovateľ založil dcérsky podnik v Únii do 12 mesiacov od určenia.

13. Kritický externý poskytovateľ IKT služieb uvedený v odseku 12 oznámi hlavnému orgánu dozoru všetky zmeny v štruktúre riadenia dcérskeho podniku usadeného v Únii.

Článok 32

Štruktúra rámca dozoru

1. Spoločný výbor v súlade s článkom 57 ods. 1 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 31 ods. 1 písm. b) v oblasti externého IKT rizika vo všetkých finančných sektoroch. Fórum pre dozor pripravuje návrhy spoločných pozícií a návrhy spoločných aktov spoločného výboru v tejto oblasti.

Fórum pre dozor pravidelne rokuje o relevantnom vývoji v oblasti IKT rizika a zraniteľných miest a podporuje konzistentný prístup pri monitorovaní externého IKT rizika na úrovni Únie.

2. Fórum pre dozor vykonáva každoročne kolektívne posudzovanie výsledkov a zistení činností dozoru vykonávaných v prípade všetkých kritických externých poskytovateľov IKT služieb a podporuje koordinačné opatrenia s cieľom zvyšovať 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 týkajúce sa kritických externých poskytovateľov 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 dohľad má toto zloženie:

a) predsedovia Európskych orgánov dohľadu;

b) jeden zástupca na vysokej úrovni zo súčasných zamestnancov relevantného príslušného orgánu uvedeného v článku 46 z každého členského štátu;

c) výkonní riaditelia každého európskeho orgánu dohľadu a jeden zástupca Komisie, výboru ESRB, ECB a agentúry ENISA ako pozorovatelia;

d) v náležitých prípadoch jeden dodatočný zástupca príslušného orgánu uvedeného v článku 46 z každého členského štátu ako pozorovateľ;

e) v náležitých prípadoch jeden zástupca príslušných orgánov určených alebo zriadených v súlade so smernicou (EÚ) 2022/2555 zodpovedných za dohľad nad kľúčovým alebo dôležitým subjektom, na ktorý sa vzťahuje uvedená smernica, ktorý bol určený ako kritický externý poskytovateľ IKT služieb, ako pozorovateľ.

Fórum pre dozor môže v náležitých prípadoch požiadať o radu nezávislých expertov vymenovaných v súlade s odsekom 6.

5. Každý členský štát určí relevantný príslušný orgán, ktorého zamestnanec bude zástupcom na vysokej úrovni uvedeným v odseku 4 prvom pododseku písm. b), a informuje o tom hlavný orgán dozoru.

Európske orgány dohľadu uverejnia na svojom webovom sídle zoznam zástupcov na vysokej úrovni zo súčasných zamestnancov príslušného orgánu určených členskými štátmi.

6. Nezávislých expertov uvedených v odseku 4 druhom pododseku vymenúva fórum pre dozor zo skupiny expertov vybraných na základe verejného a transparentného postupu podávania žiadostí.

Nezávislí experti sú vymenovaní na základe svojich odborných znalostí v oblasti finančnej stability, digitálnej prevádzkovej odolnosti a otázok bezpečnosti IKT. Konajú nezávisle a objektívne a výhradne v záujme Únie ako celku a nepožadujú ani neprijímajú pokyny od inštitúcií alebo orgánov Únie, od žiadnej vlády členského štátu ani od akýchkoľvek iných verejných alebo súkromných subjektov.

7. V súlade s článkom 16 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1094/2010 a (EÚ) č. 1095/2010 európske orgány dohľadu do 17. júla 2024 vydajú na účely tohto oddielu usmernenia o spolupráci medzi európskymi orgánmi dohľadu a príslušnými orgánmi týkajúce sa podrobných postupov a podmienok rozdelenia a vykonávania úloh medzi príslušnými orgánmi a európskymi orgánmi dohľadu a podrobností o výmene informácií, ktoré príslušné orgány potrebujú na zabezpečenie dodržiavania odporúčaní podľa článku 35 ods. 1 písm. d) určených kritickým externým poskytovateľom IKT služieb.

8. Požiadavkami stanovenými v tomto oddiele nie je dotknuté uplatňovanie smernice (EÚ) 2022/2555 ani iných pravidiel Únie o dozore, ktoré sa vzťahujú na poskytovateľov služieb cloud computingu.

9. Európske orgány dohľadu prostredníctvom spoločného výboru a na základe prípravných prác, ktoré vykonáva fórum pre dozor, každoročne predkladajú Európskemu parlamentu, Rade a Komisii správu o uplatňovaní tohto oddielu.

Článok 33

Úlohy hlavného orgánu dozoru

1. Hlavný orgán dozoru vymenovaný v súlade s článkom 31 ods. 1 písm. b) vykonáva dozor nad pridelenými kritickými externými poskytovateľmi IKT služieb a na účely všetkých záležitostí týkajúcich sa dozoru je hlavným kontaktným miestom pre týchto kritických externých poskytovateľov IKT služieb.

2. Na účely odseku 1 hlavný orgán dozoru posudzuje, či každý kritický externý poskytovateľ IKT služieb zaviedol komplexné, riadne a účinné pravidlá, postupy, mechanizmy a opatrenia na riadenie IKT rizika, ktoré kritický externý poskytovateľ IKT služieb môže predstavovať pre finančné subjekty.

Posúdenie uvedené v prvom pododseku sa zameriava najmä na IKT služby, ktoré poskytuje kritický externý poskytovateľ IKT služieb, podporujúce kritické alebo dôležité funkcie finančných subjektov. Ak je to potrebné na riešenie všetkých relevantných rizík, uvedené posúdenie sa vzťahuje aj na IKT služby podporujúce funkcie, ktoré nie sú kritické alebo dôležité.

3. Posúdenie uvedené v odseku 2 zahŕňa:

a) požiadavky na IKT s cieľom zaistiť najmä bezpečnosť, dostupnosť, kontinuitu, škálovateľnosť a kvalitu služieb, ktoré kritický externý poskytovateľ IKT služieb poskytuje finančným subjektom, ako aj schopnosť neustále zachovávať vysokú úroveň dostupnosti, pravosti, integrity alebo dôvernosti 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, politík kontinuity činností v oblasti IKT a plánov reakcie a obnovy 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 významných 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 kritického externého poskytovateľa IKT služieb finančným subjektom.

4. Na základe posúdenia uvedeného v odseku 2 a v koordinácii so spoločnou sieťou dozoru uvedenou v článku 34 ods. 1 hlavný orgán dozoru prijme jasný, podrobný a odôvodnený individuálny plán dozoru opisujúci ročné ciele dozoru a hlavné opatrenia dozoru plánované pre každého kritického externého poskytovateľa IKT služieb. Uvedený plán sa každoročne oznamuje kritickému externému poskytovateľovi IKT služieb.

Pred prijatím plánu dozoru hlavný orgán dozoru oznámi návrh plánu dozoru kritickému externému poskytovateľovi IKT služieb.

Po doručení návrhu plánu dozoru môže kritický externý poskytovateľ IKT služieb do 15 kalendárnych dní predložiť odôvodnené vyhlásenie, v ktorom preukáže očakávaný vplyv na zákazníkov, ktorí sú subjektmi, ktoré nepatria do rozsahu pôsobnosti tohto nariadenia, a v náležitých prípadoch vypracuje riešenia na zmiernenie rizík.

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

Článok 34

Operatívna koordinácia medzi hlavnými orgánmi dozoru

1. S cieľom zabezpečiť jednotný prístup k činnostiam dozoru a s cieľom umožniť koordinované stratégie všeobecného dozoru a súdržné operatívne prístupy a pracovné metodiky tri hlavné orgány dozoru vymenované v súlade s článkom 31 ods. 1 písm. b) zriadia spoločnú sieť dozoru na vzájomnú koordináciu v prípravných fázach a koordináciu vykonávania činností dozoru nad ich príslušnými kritickými externými poskytovateľmi IKT služieb, nad ktorými vykonávajú dozor, ako aj koordináciu počas akéhokoľvek postupu, ktorý môže byť potrebný podľa článku 42.

2. Na účely odseku 1 hlavné orgány dozoru vypracujú spoločný protokol o dozore, v ktorom sa stanovia podrobné postupy, ktoré sa majú dodržiavať pri vykonávaní každodennej koordinácie a na zabezpečenie rýchlych výmen a reakcií. Protokol sa pravidelne reviduje s cieľom zohľadniť operatívne potreby, najmä vývoj praktických opatrení dozoru.

3. Hlavné orgány dozoru môžu ad hoc vyzvať ECB a agentúru ENISA, aby poskytli technické poradenstvo, vymieňali si praktické skúsenosti alebo sa zapojili do konkrétnych koordinačných zasadnutí spoločnej siete dozoru.

Článok 35

Právomoci hlavného orgánu dozoru

1. Hlavný orgán dozoru má na účely plnenia povinností stanovených v tomto oddiele tieto právomoci, pokiaľ ide o kritických externých poskytovateľov IKT služieb:

a) požadovať všetky relevantné informácie a dokumentáciu v súlade s článkom 37;

b) vykonávať všeobecné vyšetrovania a inšpekcie v súlade s článkami 38 a 39;

c) žiadať o správy po ukončení činností dozoru, v ktorých sa bližšie špecifikujú opatrenia, ktoré prijali alebo nápravné opatrenia, ktoré vykonali kritickí externí poskytovatelia IKT služieb v súvislosti s odporúčaniami uvedenými v písmene d) tohto odseku;

d) vydávať odporúčania týkajúce sa oblastí uvedených v článku 33 ods. 3, 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 IKT bezpečnosti služieb poskytovaných finančným subjektom;

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

   iii) akékoľvek plánované subdodávky, pri ktorých sa hlavný orgán dozoru domnieva, že ďalšie subdodávky vrátane subdodávateľských dojednaní, ktoré kritickí externí poskytovatelia IKT služieb plánujú uzavrieť s externými poskytovateľmi IKT služieb alebo so subdodávateľmi IKT usadenými v tretej krajine, môžu vyvolať riziká pre poskytovanie služieb, ktoré vykonáva finančný subjekt, alebo riziká pre finančnú stabilitu, a to na základe preskúmania informácií zhromaždených v súlade s článkami 37 a 38;

   iv) zdržanie sa uzatvorenia ďalších subdodávateľských dohôd, ak sú splnené tieto kumulatívne podmienky:

      — plánovaný subdodávateľ je externým poskytovateľom IKT služieb alebo subdodávateľom IKT usadeným v tretej krajine,

      — subdodávky sa týkajú kritických alebo dôležitých funkcií finančného subjektu a

— hlavný orgán dozoru sa domnieva, že využívanie takýchto subdodávok predstavuje jasné a vážne riziko pre finančnú stabilitu Únie alebo pre finančné subjekty vrátane schopnosti finančných subjektov dodržiavať požiadavky dohľadu.

Na účely bodu iv) tohto písmena externí poskytovatelia IKT služieb s použitím vzoru uvedeného v článku 41 ods. 1 písm. b) zasielajú informácie týkajúce sa subdodávok hlavnému orgánu dozoru.

2. Hlavný orgán dozoru pri výkone právomocí uvedených v tomto článku:

a) zabezpečuje pravidelnú koordináciu v rámci spoločnej siete dozoru, a v náležitých prípadoch sa najmä usiluje o uplatnenie konzistentných prístupov, pokiaľ ide o dozor nad kritickými externými poskytovateľmi IKT služieb;

b) náležite zohľadňuje rámec stanovený smernicou (EÚ) 2022/2555 a v prípade potreby konzultuje s relevantnými príslušnými orgánmi určenými alebo zriadenými v súlade s uvedenou smernicou s cieľom zabrániť duplicite technických a organizačných opatrení, ktoré by sa mohli uplatňovať na kritických externých poskytovateľov IKT služieb podľa uvedenej smernice;

c) usiluje sa v čo najväčšej možnej miere minimalizovať riziko narušenia služieb, ktoré poskytujú kritickí externí poskytovatelia IKT služieb zákazníkom, ktorí sú subjektmi, ktoré nepatria do rozsahu pôsobnosti tohto nariadenia.

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

Pred adresovaním odporúčaní v súlade s odsekom 1 písm. d) hlavný orgán dozoru poskytne externému poskytovateľovi IKT služieb príležitosť predložiť do 30 kalendárnych dní relevantné informácie preukazujúce očakávaný vplyv na zákazníkov, ktorí sú subjektmi, ktoré nepatria do rozsahu pôsobnosti tohto nariadenia, a v náležitých prípadoch vypracuje riešenia na zmiernenie rizík.

4. Hlavný orgán dozoru informuje spoločnú sieť dozoru o výsledku výkonu právomocí uvedených v odseku 1 písm. a) a b). Hlavný orgán dozoru bez zbytočného odkladu postúpi správy uvedené v odseku 1 písm. c) spoločnej sieti dozoru a príslušným orgánom finančných subjektov využívajúcich IKT služby daného kritického externého poskytovateľa IKT služieb.

5. Kritickí externí poskytovatelia IKT služieb spolupracujú v dobrej viere s hlavným orgánom dozoru a pomáhajú mu pri plnení jeho úloh.

6. Hlavný orgán dozoru v prípade úplného alebo čiastočného nedodržiavania opatrení, ktorých prijatie sa vyžaduje na základe výkonu právomocí podľa odseku 1 písm. a), b a c), a po uplynutí lehoty najmenej 30 kalendárnych dní odo dňa, keď bolo kritickému externému poskytovateľovi IKT služieb doručené oznámenie o príslušných opatreniach, prijme rozhodnutie, ktorým sa ukladá pravidelná platba penále s cieľom prinútiť kritického externého poskytovateľa IKT služieb, aby uvedené opatrenia dodržiaval.

7. Pravidelná platba penále uvedená v odseku 6 sa ukladá za každý deň až do dosiahnutia súladu a nie dlhšie ako šesť mesiacov po oznámení rozhodnutia o uložení pravidelnej platby penále kritickému externému poskytovateľovi IKT služieb.

8. Výška pravidelnej platby penále vypočítaná od dátumu stanoveného v rozhodnutí, ktorým sa ukladá pravidelná platba penále, predstavuje najviac 1 % priemerného denného celosvetového obratu kritického externého poskytovateľa IKT služieb v predchádzajúcom finančnom roku. Hlavný orgán dozoru pri určovaní výšky penále zohľadní tieto kritériá týkajúce sa nedodržania opatrení uvedených v odseku 6:

a) závažnosť a trvanie nedodržiavania opatrení;

b) či k nedodržiavaniu opatrení došlo úmyselne alebo z nedbanlivosti;

c) úroveň spolupráce externého poskytovateľa IKT služieb s hlavným orgánom dozoru.

Na účely prvého pododseku sa hlavný orgán dozoru v záujme zabezpečenia jednotného prístupu zapája do konzultácií v rámci spoločnej siete dozoru.

9. Platba penále je administratívnej povahy a je vymáhateľná. Vymáhanie sa riadi platnými predpismi občianskeho práva procesného členského štátu, na území ktorého sa inšpekcie 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.

10. Hlavný orgán dozoru zverejňuje verejnosti všetky pravidelné platby penále, ktoré boli uložené, pokiaľ ich zverejnenie vážne neohrozuje finančné trhy alebo nespôsobuje neprimeranú škodu zúčastneným stranám.

11. Pred uložením pravidelnej platby penále podľa odseku 6 hlavný orgán dozoru poskytne zástupcom kritického externého poskytovateľa IKT služieb, voči ktorému sa vedie konanie, príležitosť vyjadriť sa k zisteniam a pri svojich rozhodnutiach vychádza len zo zistení, ku ktorým mal kritický externý poskytovateľ IKT služieb, voči ktorému sa vedie konanie, možnosť vyjadriť sa.

Právo na obhajobu osôb, voči ktorým sa vedie konanie, sa počas konania plne rešpektuje. Kritický externý poskytovateľ IKT služieb, voči ktorému sa vedie konanie, má 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 36

Výkon právomocí hlavného orgánu dozoru mimo Únie

1. Ak ciele dozoru nemožno dosiahnuť prostredníctvom interakcie s dcérskym podnikom založeným na účely článku 31 ods. 12 alebo vykonávaním činností dozoru v priestoroch nachádzajúcich sa v Únii, hlavný orgán dozoru môže vykonávať právomoci uvedené v nasledujúcich ustanoveniach, v akýchkoľvek priestoroch nachádzajúcich sa v tretej krajine, ktoré vlastní alebo akýmkoľvek spôsobom používa na účely poskytovania služieb finančným subjektom Únie kritický externý poskytovateľ IKT služieb v súvislosti so svojimi obchodnými operáciami, funkciami alebo službami vrátane akýchkoľvek administratívnych, obchodných alebo prevádzkových úradov, priestorov, pozemkov, budov alebo iných nehnuteľností:

a) v článku 35 ods. 1 písm. a) a

b) v článku 35 ods. 1 písm. b) v súlade s článkom 38 ods. 2 písm. a), b) a d), a v článku 39 ods. 1 a článku 39 ods. 2 písm. a).

Právomoci uvedené v prvom pododseku sa môžu vykonávať za predpokladu, že sú splnené všetky tieto podmienky:

i) hlavný orgán dozoru považuje vykonanie inšpekcie v tretej krajine za potrebné, aby mohol v plnej miere a účinne vykonávať svoje povinnosti podľa tohto nariadenia;

ii) inšpekcia v tretej krajine priamo súvisí s poskytovaním IKT služieb finančným subjektom v Únii;

iii) dotknutý kritický externý poskytovateľ IKT služieb súhlasí s vykonaním inšpekcie v tretej krajine a

iv) relevantný orgán dotknutej tretej krajiny bol oficiálne informovaný hlavným orgánom dozoru a nevzniesol voči nemu žiadne námietky.

2. Bez toho, aby boli dotknuté príslušné právomoci inštitúcií Únie a členských štátov, na účely odseku 1 EBA, ESMA alebo EIOPA uzatvoria dohody o administratívnej spolupráci s príslušným orgánom tretej krajiny s cieľom umožniť plynulé vykonávanie inšpekcií v dotknutej tretej krajine hlavným orgánom dozoru a jeho tímom určeným na jeho misiu v danej tretej krajine. Uvedenými dohodami o spolupráci sa pre Úniu a jej členské štáty nevytvárajú právne záväzky ani sa členským štátom a ich príslušným orgánom nebráni uzatvárať dvojstranné alebo viacstranné dohody s týmito tretími krajinami a ich príslušnými orgánmi.

V uvedených dohodách o spolupráci sa stanovia aspoň tieto prvky:

a) postupy koordinácie činností dozoru vykonávaných podľa tohto nariadenia a akékoľvek analogické monitorovanie externého IKT rizika vo finančnom sektore, ktoré vykonáva relevantný orgán dotknutej tretej krajiny, vrátane podrobností o postúpení súhlasu tohto orgánu s cieľom umožniť hlavnému orgánu dozoru a jeho určenému tímu vykonávať všeobecné vyšetrovania a inšpekcie na mieste, ako sa uvádza v odseku 1 prvom pododseku, na území, ktoré patrí do jej jurisdikcie;

b) mechanizmus zasielania všetkých relevantných informácií medzi orgánmi EBA, ESMA alebo EIOPA a relevantným orgánom dotknutej tretej krajiny, najmä v súvislosti s informáciami, o ktoré môže požiadať hlavný orgán dozoru podľa článku 37;

c) mechanizmy, na základe ktorých relevantný orgán dotknutej tretej krajiny bezodkladne oznámi orgánom EBA, ESMA alebo EIOPA prípady, keď sa predpokladá, že externý poskytovateľ IKT služieb usadený v tretej krajine a určený za kritického v súlade s článkom 31 ods. 1 písm. a) porušil požiadavky, ktoré je podľa príslušného práva dotknutej tretej krajiny povinný dodržiavať pri poskytovaní služieb finančným inštitúciám v danej tretej krajine, ako aj uplatnené nápravné opatrenia a sankcie;

d) pravidelné zasielanie aktuálnych informácií o vývoji v oblasti regulácie alebo dohľadu, pokiaľ ide o monitorovanie externého IKT rizika finančných inštitúcií v dotknutej tretej krajine;

e) podrobnosti, ktoré v prípade potreby umožnia účasť jedného zástupcu relevantného orgánu tretej krajiny na inšpekciách vykonávaných hlavným orgánom dozoru a určeným tímom.

3. Ak hlavný orgán dozoru nie je schopný vykonávať činnosti dozoru mimo Únie uvedené v odsekoch 1 a 2, hlavný orgán dozoru:

a) vykonáva svoje právomoci podľa článku 35 na základe všetkých skutočností a dokumentov, ktoré má k dispozícii;

b) zdokumentuje a vysvetlí všetky dôsledky svojej neschopnosti vykonávať plánované činnosti dozoru, ako sa uvádza v tomto článku.

Potenciálne dôsledky uvedené v písmene b) tohto odseku sa zohľadnia v odporúčaniach hlavného orgánu dozoru vydaných podľa článku 35 ods. 1 písm. d).

Článok 37

Žiadosť o informácie

1. Hlavný orgán dozoru môže jednoduchou žiadosťou alebo rozhodnutím požadovať od kritických externých poskytovateľov 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, politík, dokumentácie, audítorských správ o bezpečnosti IKT, správ o incidentoch súvisiacich s IKT, ako aj akýchkoľvek informácií týkajúcich sa strán, prostredníctvom ktorých na základe outsourcingu kritický externý poskytovateľ IKT služieb 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 kritického externého poskytovateľa 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 na základe rozhodnutia 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 35 ods. 6 za poskytnutie neúplných požadovaných informácií alebo keď tieto informácie nie sú poskytnuté v lehote uvedenej v písmene d) tohto odseku;

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 kritického externého poskytovateľa 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 kritickí externí poskytovatelia IKT služieb.

5. Hlavný orgán dozoru bezodkladne zašle kópiu rozhodnutia o poskytnutí informácií príslušným orgánom finančných subjektov využívajúcich služby relevantných kritických externých poskytovateľov IKT služieb a spoločnej sieti dozoru.

Článok 38

Všeobecné vyšetrovania

1. Ak je to potrebné, hlavný orgán dozoru, ktorému pomáha spoločný prieskumný tím uvedený v článku 40 ods. 1, môže na účely plnenia svojich povinností podľa tohto nariadenia vykonávať vyšetrovania kritických 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) vyhotovovať alebo získavať overené kópie alebo výpisy z týchto záznamov, údajov, zdokumentovaných postupov a akýchkoľvek iných materiálov;

c) predvolávať zástupcov kritického 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 získať 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 účel vyšetrovania.

V uvedenom poverení sa takisto upozorní na pravidelné platby penále stanovené v článku 35 ods. 6, ak poskytnuté požadované záznamy, údaje, zdokumentované postupy alebo akékoľvek iné materiály, alebo odpovede na otázky položené zástupcom externého poskytovateľa IKT služieb nie sú poskytnuté alebo sú neúplné.

4. Zástupcovia kritických 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 35 ods. 6, 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 v primeranom čase pred začatím vyšetrovania príslušné orgány finančných subjektov využívajúcich IKT služby kritického externého poskytovateľa IKT služieb o plánovanom vyšetrovaní a o totožnosti poverených osôb.

Hlavný orgán dozoru oznámi spoločnej sieti dozoru všetky informácie zaslané podľa prvého pododseku.

Článok 39

Inšpekcie

1. Na účely vykonávania svojich povinnosti podľa tohto nariadenia môže hlavný orgán dozoru za pomoci spoločných prieskumných tímov uvedených v článku 40 ods. 1 vykonávať všetky potrebné inšpekcie na mieste, pokiaľ ide o akékoľvek obchodné priestory, pozemky alebo majetok externých poskytovateľov IKT služieb, ako sú napríklad ústredia, prevádzkové strediská, vedľajšie priestory, a vstupovať do týchto priestorov, na pozemky alebo do majetku, ako aj vykonávať všetky potrebné inšpekcie na diaľku.

Na účely vykonávania právomocí uvedených v prvom pododseku vedie hlavný orgán dozoru konzultácie so spoločnou sieťou dozoru.

2. Úradníci a ostatné osoby oprávnené hlavným orgánom dozoru vykonať inšpekciu na mieste majú právomoc:

a) vstupovať do všetkých takýchto obchodných priestorov, na pozemky alebo do majetku, a

b) zapečatiť všetky takéto obchodné priestory, účtovné knihy alebo záznamy na obdobie inšpekcie a v rozsahu potrebnom na jej vykonanie.

Úradníci a ostatné osoby oprávnené hlavným orgánom dozoru vykonávajú svoje právomoci na základe písomného poverenia, v ktorom sa uvádza predmet a účel inšpekcie a pravidelné platby penále stanovené v článku 35 ods. 6, ak sa zástupcovia dotknutých kritických externých poskytovateľov IKT služieb nepodrobia inšpekcii.

3. Hlavný orgán dozoru informuje v primeranom čase pred začatím inšpekcie príslušné orgány finančných subjektov využívajúcich tohto externého poskytovateľa IKT služieb.

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

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

6. Kritický externý poskytovateľ IKT služieb sa podrobí inšpekciám na mieste nariadeným na základe rozhodnutia hlavného orgánu dozoru. V rozhodnutí sa uvádza predmet a účel inšpekcie, stanoví sa v ňom dátum, kedy inšpekcia začne, a upozorní sa na pravidelné platby penále stanovené v článku 35 ods. 6, 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 kritický externý poskytovateľ IKT služieb sa bráni inšpekcii nariadenej podľa tohto článku, hlavný orgán dozoru informuje kritického externého poskytovateľa IKT služieb o dôsledkoch takéhoto správania vrátane možnosti, aby príslušné orgány relevantných finančných subjektov vyžadovali od finančných subjektov, aby ukončili zmluvné dojednania uzavreté s týmto kritickým externým poskytovateľom IKT služieb.

Článok 40

Priebežný dozor

1. Pri vykonávaní činností dozoru, najmä všeobecných vyšetrovaní alebo inšpekcií, pomáha hlavnému orgánu dozoru spoločný prieskumný tím zriadený pre každého kritického externého poskytovateľa IKT služieb.

2. Spoločný prieskumný tím uvedený v odseku 1 sa skladá zo zamestnancov:

a) európskych orgánov dohľadu;

b) relevantných príslušných orgánov vykonávajúcich dohľad nad finančnými subjektmi, ktorým kritický externý poskytovateľ IKT služieb poskytuje IKT služby;

c) príslušného vnútroštátneho orgánu uvedeného v článku 32 ods. 4 písm. e), a to na dobrovoľnom základe;

d) jedného príslušného vnútroštátneho orgánu z členského štátu, v ktorom je usadený kritický externý poskytovateľ IKT služieb, a to na dobrovoľnom základe.

Členovia spoločného prieskumného tímu musia mať odborné znalosti v oblasti IKT záležitostí a prevádzkového rizika. Prácu spoločného prieskumného tímu koordinuje určený zamestnanec hlavného orgánu dozoru (ďalej len „koordinátor hlavného orgánu dozoru“).

3. Hlavný orgán dozoru po konzultácii s fórom pre dozor prijme do troch mesiacov od ukončenia vyšetrovania alebo inšpekcie odporúčania, ktoré sa majú adresovať kritickému externému poskytovateľovi IKT služieb v súlade s právomocami uvedenými v článku 35.

4. Odporúčania uvedené v odseku 3 sa okamžite oznámia kritickému externému poskytovateľovi IKT služieb a príslušným orgánom finančných subjektov, ktorým tento kritický externý poskytovateľ IKT služieb poskytuje IKT 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 kritický externý poskytovateľ IKT služieb.

Článok 41

Harmonizácia podmienok umožňujúcich vykonávanie činností dozoru

1. Európsky orgán dohľadu vypracujú prostredníctvom spoločného výboru návrh regulačných technických predpisov s cieľom upresniť:

a) informácie, ktoré má poskytnúť externý poskytovateľ IKT služieb v žiadosti o dobrovoľnú požiadavku, aby bol určený ako kritický podľa článku 31 ods. 11;

b) obsah, štruktúru a formát informácií, ktoré sa majú predložiť, zverejniť alebo oznámiť externým poskytovateľom IKT služieb podľa článku 35 ods. 1 vrátane vzoru na poskytovanie informácií o subdodávateľských dojednaniach;

c) kritériá na určenie zloženia spoločného prieskumného tímu, ktorými sa zabezpečí vyvážená účasť zamestnancov európskych orgánov dohľadu a relevantných príslušných orgánov, ich určenie, úlohy a pracovné podmienky;

d) podrobnosti o tom, ako príslušné orgány posudzujú opatrenia prijaté kritickými externými poskytovateľmi IKT služieb na základe odporúčaní hlavného orgánu dozoru podľa článku 42 ods. 3.

2. Európske orgány dohľadu predložia uvedený návrh regulačných technických predpisov Komisii do 17. júla 2024.

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

Článok 42

Následné opatrenia príslušných orgánov

1. Do 60 kalendárnych dní od prijatia odporúčaní vydaných hlavným orgánom dozoru podľa článku 35 ods. 1 písm. d) kritickí externí poskytovatelia IKT služieb oznámia hlavnému orgánu dozoru, že majú v úmysle postupovať podľa týchto odporúčaní, alebo poskytnú odôvodnené vysvetlenie, ak podľa týchto odporúčaní postupovať nebudú. Hlavný orgán dozoru okamžite postúpi tieto informácie príslušným orgánom dotknutých finančných subjektov.

2. Hlavný orgán dozoru zverejní verejnosti, ak kritický externý poskytovateľ IKT služieb neinformuje hlavný orgán dozoru v súlade s odsekom 1 alebo ak sa vysvetlenie, ktoré poskytol kritický externý poskytovateľ IKT služieb, nepovažuje za dostatočné. V uverejnených informáciách sa uvedie totožnosť kritického externého poskytovateľa IKT služieb, ako aj informácie o druhu a povahe nesúladu. Takéto informácie sa obmedzujú na to, čo je relevantné a primerané na účely zabezpečenia informovanosti verejnosti, s výnimkou situácie, keď by takéto uverejnenie spôsobilo neprimeranú škodu zúčastneným stranám alebo by mohlo vážne ohroziť riadne fungovanie a integritu finančných trhov alebo stabilitu celého finančného systému Únie alebo jeho časti.

Hlavný orgán dozoru informuje externého poskytovateľa IKT služieb o tomto zverejnení.

3. Príslušné orgány informujú relevantné finančné subjekty o rizikách identifikovaných v odporúčaniach adresovaných kritickým externým poskytovateľom IKT služieb v súlade s článkom 35 ods. 1 písm. d).

Pri riadení externého IKT rizika finančné subjekty zohľadňujú riziká uvedené v prvom pododseku.

4. Ak sa príslušný orgán domnieva, že finančný subjekt v rámci svojho riadenia externého IKT rizika nezohľadňuje alebo dostatočne nerieši špecifické riziká identifikované v odporúčaniach, oznámi finančnému subjektu možnosť prijatia rozhodnutia podľa odseku 6 do 60 kalendárnych dní od prijatia takého oznámenia, ak neexistujú primerané zmluvné dojednania zamerané na riešenie takýchto rizík.

5. Po doručení správ uvedených v článku 35 ods. 1 písm. c) a pred prijatím rozhodnutia ako sa uvádza v odseku 6 tohto článku môžu príslušné orgány dobrovoľne konzultovať s príslušnými orgánmi určenými alebo zriadenými v súlade so smernicou (EÚ) 2022/2555, ktoré sú zodpovedné za dohľad nad kľúčovým alebo dôležitým subjektom, na ktorý sa vzťahuje uvedená smernica, ktorý bol určený ako kritický externý poskytovateľ IKT služieb.

6. Príslušné orgány môžu ako krajné opatrenie, v nadväznosti na oznámenie a prípadne po konzultácii, ako sa stanovuje v odsekoch 4 a 5 tohto článku, v súlade s článkom 50 prijať rozhodnutie, ktorým sa od finančných subjektov požaduje, aby čiastočne alebo úplne dočasne pozastavili používanie alebo zavádzanie služby, ktorú poskytuje kritický externý poskytovateľ IKT služieb, a to dovtedy, pokiaľ sa nevyriešia riziká identifikované v odporúčaniach, ktoré boli adresované kritickým externým poskytovateľom IKT služieb. Príslušné orgány môžu v prípade potreby od finančných subjektov požadovať, aby čiastočne alebo úplne ukončili príslušné zmluvné dojednania uzavreté s kritickými externými poskytovateľmi IKT služieb.

7. Ak kritický externý poskytovateľ IKT služieb odmietne súhlasiť s odporúčaniami na základe odlišného prístupu od prístupu odporúčaného hlavným orgánom dozoru a takýto odlišný prístup môže mať nepriaznivý vplyv na veľký počet finančných subjektov alebo významnú časť finančného sektora a individuálne varovania vydané príslušnými orgánmi neviedli ku konzistentným prístupom zmierňujúcim potenciálne riziko pre finančnú stabilitu, hlavný orgán dozoru môže po konzultácii s fórom pre dozor vydať nezáväzné a neverejné stanoviská pre príslušné orgány s cieľom podporiť konzistentné a konvergentné následné opatrenia dohľadu, podľa toho, ako je to vhodné.

8. Na základe doručenia správ uvedených v článku 35 ods. 1 písm. c) príslušné orgány pri prijímaní rozhodnutí uvedených v odseku 6 tohto článku zohľadňujú druh a rozsah rizika, ktoré kritický externý poskytovateľ 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 kritického externého poskytovateľa IKT služieb;

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

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

e) či pozastavenie alebo ukončenie zmluvných dojednaní predstavuje riziko pre kontinuitu obchodných operácií finančného subjektu bez ohľadu na úsilie finančného subjektu zabrániť narušeniu poskytovania jeho služieb;

f) v náležitých prípadoch stanovisko príslušných orgánov určených alebo zriadených v súlade so smernicou (EÚ) 2022/2555 zodpovedných za dohľad nad kľúčovým alebo dôležitým subjektom, na ktorý sa vzťahuje uvedená smernica, ktorý bol určený ako kritický externý poskytovateľ IKT služieb, požadované na dobrovoľnom základe v súlade s odsekom 5 tohto článku.

Príslušné orgány poskytnú finančným subjektom lehotu potrebnú na to, aby mohli upraviť zmluvné dojednania s kritickými externými poskytovateľmi IKT služieb s cieľom zabrániť škodlivým účinkom na ich digitálnu prevádzkovú odolnosť a umožniť im zaviesť stratégie ukončenia angažovanosti a plány transformácie ako sa uvádza v článku 28.

9. Rozhodnutie uvedené v odseku 6 tohto článku sa oznámi členom fóra pre dozor uvedeným v článku 32 ods. 4 písm. a), b) a c) a spoločnej sieti dozoru.

Kritickí externí poskytovatelia IKT služieb, ktorých sa týkajú rozhodnutia stanovené v odseku 6, plne spolupracujú s dotknutými finančnými subjektmi, najmä v kontexte procesu pozastavenia alebo ukončenia ich zmluvných dojednaní.

10. 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 dojednaniach uzavretých finančnými subjektmi, ak kritickí externí poskytovatelia IKT služieb čiastočne alebo úplne nesúhlasili s im adresovanými odporúčaniami hlavného orgánu dozoru.

11. Hlavný orgán dozoru môže na požiadanie poskytnúť ďalšie objasnenia odporúčaní vydaných s cieľom usmerniť príslušné orgány v súvislosti s následnými opatreniami.

Článok 43

Poplatky za dozor

1. Hlavný orgán dozoru účtuje v súlade s delegovaným aktom uvedeným v odseku 2 tohto článku kritickým externým poskytovateľom IKT služieb poplatky, ktoré v plnej miere pokrývajú nevyhnutné výdavky hlavného orgánu dozoru v súvislosti s vykonávaním úloh dozoru podľa tohto nariadenia, vrátane úhrady všetkých nákladov, ktoré môžu vzniknúť v dôsledku práce vykonanej spoločným prieskumným tímom uvedeným v článku 40, ako aj nákladov na poradenstvo poskytnuté nezávislými expertmi, ako sa uvádza v článku 32 ods. 4 druhom pododseku, v súvislosti so záležitosťami, ktoré patria do pôsobnosti priamych činností dozoru.

Výška poplatku účtovaného kritickému externému poskytovateľovi IKT služieb pokrýva všetky náklady vyplývajúce z vykonávania povinností stanovených v tomto oddiele a je úmerná jeho obratu.

2. Komisia je splnomocnená prijať do 17. júla 2024 delegovaný akt v súlade s článkom 57 s cieľom doplniť toto nariadenie určením výšky poplatkov a spôsobu ich úhrady.

Článok 44

Medzinárodná spolupráca

1. Bez toho, aby bol dotknutý článok 36, orgány EBA, ESMA a EIOPA môžu v súlade s článkom 33 nariadení (EÚ) č. 1093/2010, (EÚ) č. 1095/2010 a (EÚ) č. 1094/2010 uzatvárať administratívne dojednania s regulačnými orgánmi a orgánmi dohľadu tretích krajín s cieľom posilniť medzinárodnú spoluprácu v oblasti externého IKT rizika 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 externého IKT rizika a dôsledky pre finančnú stabilitu, integritu trhu, ochranu investorov a fungovanie vnútorného trhu.

KAPITOLA VI

Dojednania o výmene informácií

Článok 45

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

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 spôsobilostí obrany, techník odhaľovania hrozieb, stratégií zmierňovania alebo fáz reakcie a obnovy;

b) uskutočňovala v rámci dôveryhodných skupín 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 v súlade s nariadením (EÚ) 2016/679 a usmernení pre politiku hospodárskej súťaže.

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, o zapojení externých poskytovateľov IKT služieb a 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 svojho členstva alebo prípadne ukončenie svojho členstva, keď nadobudne účinnosť.

KAPITOLA VII

Príslušné orgány

Článok 46

Príslušné orgány

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

a) v prípade úverových inštitúcií a inštitúcií vyňatých podľa smernice 2013/36/EÚ príslušný orgán určený v súlade s článkom 4 uvedenej smernice a v prípade úverových inštitúcií klasifikovaných ako významné v súlade s článkom 6 ods. 4 nariadenia (EÚ) č. 1024/2013 ECB v súlade s právomocami a úlohami udelenými uvedeným nariadením;

b) v prípade platobných inštitúcií vrátane platobných inštitúcií vyňatých podľa smernice (EÚ) 2015/2366, inštitúcií elektronického peňažníctva vrátane tých, ktoré sú vyňaté podľa smernice 2009/110/ES, a poskytovateľov služieb informovania o účte uvedených v článku 33 ods. 1 smernice (EÚ) 2015/2366 príslušný orgán určený v súlade s článkom 22 smernice (EÚ) 2015/2366;

c) v prípade investičných spoločností príslušný orgán určený v súlade s článkom 4 smernice Európskeho parlamentu a Rady (EÚ) 2019/2034 ([38]);

d) v prípade poskytovateľov služieb kryptoaktív, ktorým bolo udelené povolenie podľa nariadenia o trhoch s kryptoaktívami, a emitentov tokenov krytých aktívami príslušný orgán určený v súlade s príslušným ustanovením uvedeného nariadenia;

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

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

g) v prípade obchodných miest a poskytovateľov služieb vykazovania údajov príslušný orgán určený v súlade s článkom 67 smernice 2014/65/EÚ a príslušný orgán vymedzený v článku 2 ods. 1 bode 18 nariadenia (EÚ) č. 600/2014;

h) v prípade archívov obchodných údajov príslušný orgán určený v súlade s článkom 22 nariadenia (EÚ) č. 648/2012;

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

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

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

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

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

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

o) v prípade správcov kritických referenčných hodnôt príslušný orgán určený v súlade s článkami 40 a 41 nariadenia (EÚ) 2016/1011;

([38]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/2034 z 27. novembra 2019 o prudenciálnom dohľade nad investičnými spoločnosťami a o zmene smerníc 2002/87/ES, 2009/65/ES, 2011/61/EÚ, 2013/36/EÚ, 2014/59/EÚ a 2014/65/EÚ (Ú. v. EÚ L 314, 5.12.2019, s. 64).

p) v prípade poskytovateľov služieb hromadného financovania príslušný orgán určený v súlade s článkom 29 nariadenia (EÚ) 2020/1503;

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

Článok 47

Spolupráca so štruktúrami a orgánmi zriadenými smernicou (EÚ) 2022/2555

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 14 smernice (EÚ) 2022/2555 sa môžu európske orgány dohľadu a príslušné orgány zúčastňovať na činnostiach skupiny pre spoluprácu v prípade záležitostí, ktoré sa týkajú ich činností súvisiacich s finančnými subjektmi. Európske orgány dohľadu a príslušné orgány môžu požiadať, aby boli prizvané zúčastniť sa na činnostiach skupiny pre spoluprácu v prípade záležitostí, ktoré sa týkajú kľúčových alebo dôležitých subjektov, na ktoré sa vzťahuje uvedená smernica (EÚ) 2022/2555, ktoré boli zároveň určené ako kritickí externí poskytovatelia IKT služieb podľa článku 31 tohto nariadenia.

2. Ak je to vhodné, príslušné orgány môžu konzultovať a zdieľať informácie s jednotnými kontaktnými miestami a jednotkami CSIRT určenými alebo zriadenými v súlade so smernicou (EÚ) 2022/2555.

3. Ak je to vhodné, príslušné orgány môžu požiadať o akékoľvek relevantné technické poradenstvo a pomoc zo strany príslušných orgánov určených alebo stanovených v súlade so smernicou (EÚ) 2022/2555 a stanoviť dojednania v oblasti spolupráce s cieľom umožniť zriadenie účinných a rýchlo reagujúcich koordinačných mechanizmov.

4. V dojednaniach uvedených v odseku 3 tohto článku sa môžu okrem iného upresniť postupy koordinácie činností dohľadu a dozoru vo vzťahu ku kľúčovým alebo dôležitým subjektom, na ktoré sa vzťahuje smernica (EÚ) 2022/2555, ktoré boli určené ako kritickí externí poskytovatelia IKT služieb podľa článku 31 tohto nariadenia, vrátane vedenia vyšetrovaní a inšpekcií na mieste v súlade s vnútroštátnym právom, ako aj mechanizmov výmeny informácií medzi príslušnými orgánmi podľa tohto nariadenia a príslušnými orgánmi určenými alebo zriadenými v súlade s uvedenou smernicou, čo zahŕňa prístup k informáciám požadovaným príslušnými orgánmi určenými alebo zriadenými v súlade s uvedenou smernicou.

Článok 48

Spolupráca medzi orgánmi

1. Príslušné orgány úzko spolupracujú vzájomne a v náležitých prípadoch s hlavným orgánom dozoru.

2. Príslušné orgány a hlavný orgán dozoru si včas navzájom vymieňajú všetky relevantné informácie týkajúce sa kritických externých poskytovateľov IKT služieb, ktoré sú pre nich potrebné na plnenie ich príslušných povinností podľa tohto nariadenia, najmä v súvislosti so zistenými rizikami, prístupmi a opatreniami prijatými v rámci úloh hlavného orgánu dozoru v oblasti dozoru.

Článok 49

Finančné medzisektorové cvičenia, komunikácia a spolupráca

1. Európske orgány dohľadu môžu prostredníctvom spoločného výboru a v spolupráci s príslušnými orgánmi, vnútroštátnymi orgánmi pre riešenie krízových situácií uvedenými v článku 3 smernice 2014/59/EÚ, ECB, Jednotnou radou pre riešenie krízových situácií, pokiaľ ide o informácie týkajúce sa subjektov, ktoré patria do rozsahu pôsobnosti nariadenia (EÚ) č. 806/2014, výborom ESRB a agentúrou ENISA, podľa toho, ktorý z týchto subjektov je relevantný, vytvoriť mechanizmy, ktoré umožnia výmenu účinných postupov vo finančných sektoroch s cieľom zlepšiť situačnú informovanosť a identifikovať spoločné kybernetické zraniteľné miesta a riziká naprieč sektormi.

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

Týmito cvičeniami sa náležite môžu takisto testovať závislosti finančného sektora od ostatných hospodárskych odvetví.

2. Príslušné orgány, európske orgány dohľadu a ECB navzájom úzko spolupracujú a vymieňajú si informácie na plnenie svojich povinností podľa článkov 47 až 54. 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 50

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 aspoň tieto právomoci:

a) mať prístup ku každému dokumentu alebo údaju v akejkoľvek forme, ktorý príslušný orgán považuje za relevantný pre plnenie svojich povinností, a dostať alebo si vyhotoviť jeho kópiu;

b) vykonávať inšpekcie na mieste alebo vyšetrovania, ktoré zahŕňajú, ale neobmedzujú sa na:

   i) predvolanie zástupcov finančných subjektov, aby podali ústne alebo písomné vysvetlenie k skutočnostiam alebo dokumentom týkajúcim sa predmetu a účelu vyšetrovania, a zaznamenávanie odpovedí;

   ii) vypočutie akejkoľvek inej fyzickej alebo právnickej osoby, ktorá s týmto vypočutím súhlasí, s cieľom získať informácie týkajúce sa predmetu vyšetrovania;

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

3. Bez toho, aby bolo dotknuté právo členských štátov ukladať trestnoprávne sankcie v súlade s článkom 52, 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 ukončila konanie, ktoré je porušením tohto nariadenia, 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 odsek 2 písm. c) a odsek 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 51

Výkon právomoci ukladať administratívne sankcie a nápravné opatrenia

1. Príslušné orgány vykonávajú právomoc ukladať administratívne sankcie a nápravné opatrenia uvedené v článku 50 v súlade so svojimi vnútroštátnymi právnymi rámcami, ak je to vhodné, týmto spôsobom:

a) priamo;

b) v spolupráci s inými orgánmi;

c) v rámci svojej zodpovednosti delegovaním na iné orgány alebo

d) podaním žiadosti na príslušné súdne orgány.

2. Pri určovaní druhu a úrovne administratívnej sankcie alebo nápravného opatrenia, ktoré sa majú uložiť podľa článku 50, 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 fyzická alebo právnická osoba dosiahla, alebo strát, ktorým zabránila;

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

Článok 52

Trestné 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 53

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 17. januára 2025. Členské štáty oznámia Komisii a orgánom ESMA, EBA a EIOPA bez zbytočného odkladu akékoľvek ďalšie súvisiace zmeny.

Článok 54

Uverejnenie administratívnych sankcií

1. Príslušné orgány uverejnia na svojich oficiálnych 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, vrátane rizika súvisiaceho s ochranou osobných údajov, 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) odloží jeho uverejnenie dovtedy, kým prestanú existovať všetky dôvody na neuverejnenie;

b) uverejní ho anonymne v súlade s vnútroštátnym právom alebo

c) upustí 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) možno uverejnenie príslušných informácií odložiť.

5. Ak príslušný orgán uverejní rozhodnutie o uložení administratívnej sankcie, voči ktorému sa podalo odvolanie na príslušné súdne orgány, príslušné orgány okamžite uvedú na svojom oficiálnom 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 oficiálnych webových sídlach len kým je to potrebné na uplatnenie tohto článku. Toto obdobie nesmie presiahnuť päť rokov po uverejnení.

Článok 55

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 zachovávania služobného tajomstva sa vzťahuje na všetky osoby, ktoré pracujú alebo pracovali pre príslušné orgány podľa tohto nariadenia, alebo pre akýkoľvek orgán alebo trhový podnik alebo fyzickú alebo právnickú osobu, na ktoré tieto príslušné orgány delegovali právomoci, vrátane ich zmluvných audítorov a expertov.

3. Informácie, na ktoré sa vzťahuje služobné tajomstvo, vrátane výmeny informácií medzi príslušnými orgánmi podľa tohto nariadenia a príslušnými orgánmi určenými alebo zriadenými v súlade so smernicou (EÚ) 2022/2555, 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.

Článok 56

Ochrana údajov

1. Európske orgány dohľadu a príslušné orgány môžu spracúvať osobné údaje len vtedy, ak je to potrebné na účely plnenia ich príslušných povinností a úloh podľa tohto nariadenia, najmä pokiaľ ide o vyšetrovanie, inšpekciu, žiadosť o informácie, komunikáciu, uverejňovanie, hodnotenie, overovanie, posudzovanie a vypracúvanie plánov dozoru. Osobné údaje sa spracúvajú v súlade s nariadením (EÚ) 2016/679 alebo nariadením (EÚ) 2018/1725, podľa toho, ktoré je uplatniteľné.

2. Pokiaľ nie je v iných odvetvových aktoch stanovené inak, osobné údaje uvedené v odseku 1 sa uchovávajú až do vykonania príslušných povinností v oblasti dohľadu a v každom prípade najviac 15 rokov, s výnimkou prebiehajúceho súdneho konania, ktoré si vyžaduje ďalšie uchovávanie takýchto údajov.

KAPITOLA VIII

Delegované akty

Článok 57

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 31 ods. 6 a článku 43 ods. 2 sa Komisii udeľuje na obdobie piatich rokov od 17. januára 2024. Komisia vypracuje správu týkajúcu sa delegovania právomoci najneskôr deväť mesiacov pred uplynutím tohto päťročného obdobia. Delegovanie právomoci sa automaticky predlžuje o rovnako dlhé obdobia, pokiaľ Európsky parlament alebo Rada nevznesú voči takémuto predĺženiu námietku najneskôr tri mesiace pred koncom každého obdobia.

3. Delegovanie právomoci uvedené v článku 31 ods. 6 a článku 43 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 expertmi 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 31 ods. 6 a článku 43 ods. 2 nadobudne účinnosť, len ak Európsky parlament alebo Rada voči nemu nevzniesli námietku v lehote troch 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 tri mesiace.

KAPITOLA IX

Prechodné a záverečné ustanovenia

Oddiel I

Článok 58

Doložka o preskúmaní

1. Do 17. januára 2028 Komisia po konzultáciách s európskymi orgánmi dohľadu a výborom ESRB, podľa toho, ktorý z týchto subjektov je relevantný, vykoná preskúmanie a predloží Európskemu parlamentu a Rade správu, ku ktorej v náležitých prípadoch pripojí legislatívny návrh. Preskúmanie zahŕňa aspoň:

a) kritéria na určenie kritických externých poskytovateľov IKT služieb podľa článku 31 ods. 2;

b) dobrovoľný charakter oznamovania významných kybernetických hrozieb uvedených v článku 19;

c) režim uvedený v článku 31 ods. 12 a právomoci hlavného orgánu dozoru stanovené v článku 35 ods. 1 písm. d) bode iv) prvej zarážke s cieľom posúdiť účinnosť týchto ustanovení, pokiaľ ide o zabezpečenie účinného dozoru nad kritickými externými poskytovateľmi IKT služieb usadenými v tretej krajine, a potrebu založiť dcérsku spoločnosť v Únii.

Na účely prvého pododseku tohto písmena preskúmanie zahŕňa analýzu režimu uvedeného v článku 31 ods. 12 vrátane podmienok prístupu finančných subjektov Únie k takýmto službám z tretích krajín a dostupnosti služieb na trhu Únie a zohľadňuje ďalší vývoj na trhoch so službami, na ktoré sa vzťahuje toto nariadenie, praktické skúsenosti finančných subjektov a orgánov dohľadu nad finančnými subjektmi, pokiaľ ide o uplatňovanie tohto režimu a dohľad nad ním, a akýkoľvek relevantný vývoj v oblasti regulácie a dohľadu, ku ktorému dochádza na medzinárodnej úrovni.

d) vhodnosť zahrnutia finančných subjektov, ktoré využívajú automatizované predajné systémy, uvedených v článku 2 ods. 3 písm. e) do rozsahu pôsobnosti tohto nariadenia vzhľadom na budúci vývoj na trhu s používaním takýchto systémov;

e) fungovanie a účinnosť spoločnej siete dozoru pri podpore konzistentnosti dozoru a efektívnosti výmeny informácií v rámci dozoru.

2. V kontexte preskúmania smernice (EÚ) 2015/2366 Komisia posúdi potrebu zvýšenej kybernetickej odolnosti platobných systémov a činností spracovania platieb a vhodnosť rozšírenia rozsahu pôsobnosti tohto nariadenia na prevádzkovateľov platobných systémov a subjekty zapojené do činností spracovania platieb. Na základe tohto posúdenia Komisia v rámci preskúmania smernice (EÚ) 2015/2366 predloží Európskemu parlamentu a Rade správu najneskôr do 17. júla 2023.

Na základe uvedenej správy a po konzultácii s európskymi orgánmi dohľadu, ECB a ESRB môže Komisia v náležitých prípadoch a ako súčasť legislatívneho návrhu, ktorý môže prijať podľa článku 108 druhého odseku smernice (EÚ) 2015/2366, predložiť návrh na zabezpečenie toho, aby všetci prevádzkovatelia platobných systémov a subjekty zapojené do činností spracovania platieb podliehali primeranému dozoru, pričom sa zohľadní existujúci dohľad centrálnej banky.

3. Do 17. januára 2026 Komisia po konzultácii s európskymi orgánmi dohľadu a Výborom európskych orgánov pre dohľad nad výkonom auditu vykoná preskúmanie a predloží správu Európskemu parlamentu a Rade, ku ktorej v náležitých prípadoch pripojí legislatívny návrh, týkajúcu sa vhodnosti posilnených požiadaviek pre štatutárnych audítorov a audítorské spoločnosti, pokiaľ ide o digitálnu prevádzkovú odolnosť, prostredníctvom zahrnutia štatutárnych audítorov a audítorských spoločností do rozsahu pôsobnosti tohto nariadenia alebo prostredníctvom zmien smernice Európskeho parlamentu a Rady 2006/43/ES ([39]).

Oddiel II

Zmeny

Článok 59

Zmeny nariadenia (ES) č. 1060/2009

Nariadenie (ES) č. 1060/2009 sa mení takto:

1. V prílohe I oddiele A odseku 4 sa 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) 2022/2554 (*).

_____

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022, s. 1).“

2. V prílohe III sa bod 12 nahrádza takto:

„12. Ratingová agentúra porušuje článok 6 ods. 2 v spojení s prílohou I oddielom A bodom 4 tým, že nemá správne administratívne alebo účtovné postupy, mechanizmy vnútornej kontroly, účinné postupy hodnotenia rizika alebo účinné kontrolné alebo ochranné mechanizmy riadenia systémov IKT v súlade s nariadením (EÚ) 2022/2554, alebo tým, že nevykonáva alebo nezachováva rozhodovacie postupy alebo organizačné štruktúry, ako sa vyžaduje v uvedenom bode.**“**

Článok 60

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. Využíva vhodné a primerané systémy, zdroje a postupy vrátane systémov IKT riadených v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2022/2554 (*).

_____

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022, s. 1).**“**

([39]) Smernica Európskeho parlamentu a Rady 2006/43/ES zo 17. mája 2006 o štatutárnom audite ročných účtovných závierok a konsolidovaných účtovných závierok, ktorou sa menia a dopĺňajú smernice Rady 78/660/EHS a 83/349/EHS a ktorou sa zrušuje smernica Rady 84/253/EHS (Ú. v. EÚ L 157, 9.6.2006, s. 87).

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 politiku kontinuity podnikateľskej činnosti v oblasti IKT a plány reakcie a obnovy v oblasti IKT, ktoré sú zavedené a vykonávané v súlade s nariadením (EÚ) 2022/2554, s cieľom zaistiť zachovanie svojich funkcií, včasnú obnovu činnosti a plnenie povinností centrálnej protistrany.**“**

b) V odseku 3 sa prvý pododsek nahrádza takto:

„3. S cieľom zabezpečiť konzistentné uplatňovanie tohto článku ESMA po konzultácii s členmi ESCB vypracuje návrh regulačných technických noriem, v ktorých sa s výnimkou politiky kontinuity podnikateľskej 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 vypracuje ESMA návrh regulačných technických predpisov, 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) 2022/2554.

2. Archív obchodných údajov zavedie, vykonáva a udržiava zodpovedajúcu politiku kontinuity podnikateľskej činnosti a plán obnovy po havárii vrátane politiky kontinuity podnikateľskej činnosti v oblasti IKT a plánov reakcie a obnovy v oblasti IKT zavedených v súlade s nariadením (EÚ) 2022/2554 s cieľom zaistiť zachovanie svojich funkcií, včasnú obnovu činnosti a plnenie povinností archívu obchodných údajov.**“**

5. V článku 80 sa vypúšťa odsek 1.

6. V prílohe I sa oddiel II sa mení takto:

a) Písmená a) a b) sa nahrádzajú takto:

„a) archív obchodných údajov porušuje článok 79 ods. 1 tým, že neurčí zdroje prevádzkového rizika alebo ich neminimalizuje prostredníctvom vývoja vhodných systémov, kontrolných mechanizmov a postupov vrátane systémov IKT riadených v súlade s nariadením (EÚ) 2022/2554;

b) archív obchodných údajov porušuje článok 79 ods. 2 tým, že nezavedie, nevykonáva alebo neudržiava zodpovedajúcu politiku zabezpečenia kontinuity podnikateľskej činnosti a plán obnovy po havárii zavedené v súlade s nariadením (EÚ) 2022/2554, s cieľom zaistiť zachovanie svojich funkcií, včasnej obnovy činnosti a plnenia povinností archívu obchodných údajov;“.

b) Písmeno c) sa vypúšťa.

7. Príloha III sa mení takto:

a) Oddiel II sa mení takto:

i) písmeno c) sa nahrádza takto:

„c) centrálna protistrana Tier 2 porušuje článok 26 ods. 3 tým, že neudržiava alebo neprevádzkuje organizačnú štruktúru, ktorá zabezpečuje kontinuitu a riadne fungovanie pri vykonávaní jej služieb a činností, alebo tým, že nepoužíva vhodné a primerané systémy, zdroje alebo postupy vrátane systémov IKT riadených v súlade s nariadením (EÚ) 2022/2554;“

ii) písmeno f) sa vypúšťa.

b) V oddiele III sa písmeno a) nahrádza takto:

„a) centrálna protistrana Tier 2 porušuje článok 34 ods. 1 tým, že nezavedie, nevykonáva alebo neudržiava primeranú politiku zabezpečovania kontinuity podnikateľskej činnosti a plán reakcie a obnovy stanovené v súlade s nariadením (EÚ) 2022/2554 s cieľom zaistiť zachovanie svojich funkcií, včasnú obnovu činnosti a plnenie povinností centrálnej protistrany, ktorý umožňuje minimálne obnovu všetkých transakcií v čase výpadku, aby centrálna protistrana mohla pokračovať v činnosti s istotou a dokončiť vyrovnanie k plánovanému dátumu;“.

Článok 61

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) 2022/2554 (*), 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) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011(Ú. v. EÚ L 333, 27.12.2022, s. 1).“

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 činností a plán obnovy po katastrofe vrátane politiky kontinuity činností v oblasti IKT a plánov reakcie a obnovy v oblasti IKT v súlade s nariadením (EÚ) 2022/2554, 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 12 ods. 5 a 7 nariadenia (EÚ) 2022/2554.“

4. Odsek 6 sa nahrádza takto:

„6. 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:

„7. 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 riziko, ako aj metódy na testovanie, odstránenie alebo minimalizáciu týchto rizík vrátane politík kontinuity činností a plánov obnovy po katastrofe uvedených v odsekoch 3 a 4 a spôsobov ich posudzovania.“

Článok 62

Zmeny nariadenia (EÚ) č. 600/2014

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

1. Článok 27g sa mení takto:

   a) Odsek 4 sa nahrádza takto:

   „4. APA spĺňa požiadavky týkajúce sa bezpečnosti sietí a informačných systémov stanovené v nariadení Európskeho parlamentu a Rady (EÚ) 2022/2554 (*).

   (*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011(Ú. v. EÚ L 333, 27.12.2022, s. 1).“

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

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

2. Článok 27 h sa mení takto:

   a) Odsek 5 sa nahrádza takto:

   „5. CTP spĺňa požiadavky týkajúce sa bezpečnosti sietí a informačných systémov stanovené v nariadení (EÚ) 2022/2554.“

   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 nahrádza takto:

   „3. ARM spĺňa požiadavky týkajúce sa bezpečnosti sietí a informačných systémov stanovené v nariadení (EÚ) 2022/2554.“

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

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

Článok 63

Zmeny nariadenia (EÚ) 2016/1011

V článku 6 nariadenia (EÚ) 2016/1011 sa dopĺňa tento odsek:

„6. Pokiaľ ide o kritické referenčné hodnoty, správca má zavedené 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) 2022/2554 (*).

(*) Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011(Ú. v. EÚ L 333, 27.12.2022, s. 1).“

Článok 64

Nadobudnutie účinnosti a uplatňovanie

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

Uplatňuje sa od 17. januára 2025.

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

V Štrasburgu 14. decembra 2022

Za Európsky parlament	*Za Radu*
predsedníčka	*predseda*
R. METSOLA	M. BEK