EVROPSKÁ
KOMISE

V Bruselu dne 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014

(Text s významem pro EHP)

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

- Odůvodnění a cíle návrhu

Tento návrh je součástí balíčku právních předpisů v oblasti digitálních financí, což je soubor opatření, která dále umožní a podpoří rozvoj potenciálu digitálních financí, pokud jde o inovace a konkurenceschopnost, a současně zmírní s nimi související rizika. Je v souladu s prioritami Komise připravit Evropu na digitální věk a vybudovat ekonomiku připravenou na budoucnost, která bude fungovat ve prospěch občanů. Balíček pro digitální finance zahrnuje novou strategii v oblasti digitálních financí pro finanční sektor EU[1], jejímž cílem je zajistit, aby EU využila příležitostí, které nabízí digitální revoluce, a vedla tuto revoluci v čele s evropskými inovativními firmami tak, aby výhod digitálních financí mohli využívat i spotřebitelé a podniky. Kromě tohoto návrhu obsahuje balíček také návrh nařízení o trzích s kryptoaktivy[2], návrh nařízení o pilotním režimu pro tržní infrastruktury vedené na technologii sdíleného registru[3] a návrh směrnice s cílem vyjasnit či změnit některá související pravidla EU pro oblast finančních služeb[4]. Digitalizace a provozní odolnost ve finančním sektoru jsou dvě strany jedné mince. Digitální neboli informační a komunikační technologie (IKT) přinášejí příležitosti, ale i rizika. Ta je nutné správně chápat a řídit, zejména v obtížných obdobích.

Tvůrci politik a orgány dohledu se proto stále více zaměřují na rizika vyplývající ze závislosti na IKT. Zejména se pokoušejí posílit odolnost firem prostřednictvím stanovení norem a koordinace regulace a dohledu. Tato práce probíhá na mezinárodní i na evropské úrovni, a to napříč odvětvími i v rámci některých konkrétních odvětví, včetně finančních služeb.

Rizika v oblasti IKT nicméně nadále představují výzvu pro provozní odolnost, výkonnost a stabilitu finančního systému EU. Reforma po finanční krizi v roce 2008 primárně posílila finanční odolnost[5] finančního sektoru EU, přičemž riziky v oblasti IKT se zabývala pouze nepřímo a pouze v některých oblastech v rámci opatření šířeji zaměřených na operační rizika.

Zatímco v rámci změn právních předpisů týkajících se finančních služeb v EU po finanční krizi byl vytvořen jednotný soubor pravidel upravující velkou část finančních rizik spojených s finančními službami, tyto změny se plně nezabývaly digitální provozní odolností. Opatření přijatá v posledně zmíněné oblasti se vyznačují množstvím prvků, které omezují jejich účinnost. Například měla často formu směrnic s minimální harmonizací nebo předpisů založených na zásadách a ponechávala značný prostor pro rozdílné přístupy na jednotném trhu. Kromě toho byla v rámci pokrytí operačních rizik věnována pouze omezená či nedostatečná pozornost rizikům v oblasti IKT. V neposlední řadě se tato opatření v různých právních předpisech týkajících se finančních služeb liší. Intervence na úrovni Unie proto

---

1 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o strategii EU v oblasti digitálních financí, COM(2020) 591 ze dne 23. září 2020.

2 Návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937, COM(2020) 593.

3 Návrh nařízení Evropského parlamentu a Rady o pilotním režimu pro tržní infrastruktury vedené na technologii sdíleného registru, COM(2020) 594.

4 Návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341, COM(2020) 596.

5 Různá přijatá opatření se v zásadě zaměřovala na zvýšení kapitálových prostředků a likvidity finančních subjektů, jakož i na omezení tržních a úvěrových rizik.

neodpovídala v plné míře tomu, co evropské finanční subjekty potřebovaly pro řízení operačních rizik způsobem umožňujícím náležitou odolnost vůči incidentům souvisejícím s IKT, reakci na ně a zotavení se z jejich dopadů. Navíc nevybavila orgány finančního dohledu těmi nejvhodnějšími nástroji, aby mohly plnit své pověření předcházet finanční nestabilitě v případě, že by se rizika v oblasti IKT naplnila.

Absence podrobných a ucelených pravidel v oblasti digitální provozní odolnosti na úrovni EU vedla ke vzniku mnoha různých vnitrostátních regulačních iniciativ (např. v oblasti testování digitální provozní odolnosti) a přístupů k dohledu (např. zabývajících se závislostí na třetích stranách v oblasti IKT). Opatření na úrovni členských států však mají vzhledem k přeshraniční povaze rizik v oblasti IKT pouze omezený dopad. Nekoordinované vnitrostátní iniciativy se mimoto mnohdy překrývají, jsou nekonzistentní a vedou ke zdvojení požadavků, vysokým administrativním nákladům a nákladům na dodržování předpisů – zejména pro přeshraniční finanční subjekty – případně k tomu, že rizika v oblasti IKT zůstávají nezjištěna, a tedy neřešena. V důsledku této situace dochází k tříštění jednotného trhu, narušení stability a integrity finančního sektoru EU a ohrožení ochrany spotřebitelů a investorů.

Proto je nezbytné vytvořit podrobný a ucelený rámec pro digitální provozní odolnost finančních subjektů EU. Tento rámec prohloubí složku jednotného souboru pravidel věnovanou řízení digitálních rizik. Zejména zlepší a harmonizuje řízení rizik v oblasti IKT ze strany finančních subjektů, zavede důkladné testování systémů IKT, zvýší povědomí orgánů dohledu o kybernetických rizicích a incidentech souvisejících s IKT, jež finančním subjektům hrozí, a rovněž zavede nové pravomoci orgánů finančního dohledu za účelem kontroly rizik plynoucích ze závislosti finančních subjektů na poskytovatelích služeb IKT z řad třetích stran. Návrh vytvoří jednotný mechanismus hlášení incidentů, který pomůže snížit administrativní zátěž finančních subjektů a posílí účinnost dohledu.

- Soulad s platnými předpisy v dané oblasti politiky

Tento návrh je součástí širšího úsilí probíhajícího na evropské i mezinárodní úrovni s cílem zlepšit kybernetickou bezpečnost ve finančních službách a řešit širší operační rizika[6].

Reaguje rovněž na společné odborné doporučení[7] evropských orgánů dohledu (ESA) z roku 2019, které vyzvalo k soudržnějšímu přístupu při řešení rizik v oblasti IKT ve finančním sektoru a doporučilo Komisi přiměřeným způsobem posílit digitální provozní odolnost odvětví finančních služeb prostřednictvím odvětvové iniciativy na úrovni EU. Doporučení evropských orgánů dohledu bylo reakcí na akční plán Komise pro finanční technologie z roku 2018[8].

- Soulad s ostatními politikami Unie

Jak prohlásila ve svých politických směrech[9] předsedkyně von der Leyen a jak se uvádí ve sdělení „Formování digitální budoucnosti Evropy“[10], je pro Evropu zásadní, aby využívala všech výhod digitálního věku a v rámci bezpečných a etických hranic posilovala své

---

6 Basilejský výbor pro bankovní dohled, *Cyber-resilience: Range of practices*, prosinec 2018 a *Principles for sound management of operational risk (PSMOR)*, říjen 2014.

7 Společné doporučení evropských orgánů dohledu Evropské Komisi o potřebě zlepšení právních předpisů, pokud jde o požadavky na řízení rizik v oblasti IKT ve finančním sektoru EU, JC 2019 26 (2019).

8 Evropská komise, *Akční plán pro finanční technologie*, COM(2018) 109 final.

9 Předsedkyně Ursula Von Der Leyen, Politické směry pro příští Evropskou komisi, 2019–2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_cs.pdf.

10 Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, *Formování digitální budoucnosti Evropy*, COM(2020) 67 final.

průmyslové a inovační kapacity. Evropská strategie pro data[11] stanoví čtyři pilíře – ochranu údajů, základní práva, bezpečnost a kybernetickou bezpečnost – jako zásadní předpoklady pro společnost fungující na základě využívání dat. Evropský parlament začal nedávno pracovat na zprávě o digitálních financích, která mimo jiné požaduje společný přístup ke kybernetické odolnosti finančního sektoru[12]. Vytvoření legislativního rámce posilujícího digitální provozní odolnost finančních subjektů v EU je s těmito politickými cíli v souladu. Návrh rovněž podpoří politiky zaměřené na oživení po koronaviru, jelikož zajistí, aby zvýšené využívání digitálních financí bylo spojené s provozní odolností.

Díky tomu, že tato iniciativa ponechá finanční sektor v působnosti horizontálního rámce pro kybernetickou bezpečnost (např. směrnice o bezpečnosti sítí a informací), zůstanou výhody tohoto rámce zachovány. Bude zachováno úzké spojení finančního sektoru s orgánem spolupráce v oblasti bezpečnost sítí a informací a orgány finančního dohledu si budou moci vyměňovat informace v rámci stávajícího ekosystému bezpečnosti sítí a informací. Tato iniciativa je v souladu se směrnicí o určování a označování evropských kritických infrastruktur, která je v současné době předmětem revize za účelem posílení ochrany a odolnosti kritických infrastruktur vůči jiným než kybernetickým hrozbám. A tento návrh je rovněž plně v souladu se strategií bezpečnostní unie[13], která vzhledem k vysoké závislosti finančního sektoru na službách IKT a jeho vysoké zranitelnosti vůči kybernetickým útokům vybídla k vypracování iniciativy pro zvýšení jeho digitální provozní odolnosti.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

- Právní základ

Návrh nařízení vychází z článku 114 SFEU.

Tím, že harmonizuje pravidla pro řízení rizik v oblasti IKT a pro hlášení, testování a rizika v oblasti IKT spojená s třetími stranami, odstraňuje překážky a zlepšuje vytváření a fungování vnitřního trhu s finančními službami. Stávající nesrovnalosti v této oblasti jak na legislativní úrovni, tak na úrovni dohledu a rovněž nesrovnalosti na úrovni členských států a EU narušují fungování jednotného trhu finančních služeb, jelikož finanční subjekty působící ve více členských státech musí vyjma případů, kdy dochází k překrývání, plnit rozdílné regulatorní požadavky či očekávání orgánů dohledu, což může bránit výkonu jejich svobody usazování a poskytování služeb. Rozdílná pravidla narušují rovněž hospodářskou soutěž finančních subjektů stejného druhu v různých členských státech. V oblastech, kde chybí harmonizace, nebo je pouze částečná či omezená, může navíc přijímání různých vnitrostátních pravidel či přístupů, již platných nebo v procesu schvalování a provádění na vnitrostátní úrovni, omezovat svobody jednotného trhu s finančními službami. Platí to zejména pro rámce testování digitální provozní odolnosti a dohled nad kritickými poskytovateli služeb IKT z řad třetích stran.

---

[11] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů, *Evropská strategie pro data*, COM(2020) 66 final.

[12] Zpráva s doporučeními Komisi ohledně digitálních financí: nově vznikající rizika související s kryptoaktivy – výzvy spojené s regulací a dohledem v oblasti finančních služeb, institucí a trhů (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

[13] Sdělení Komise Evropskému parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o strategii bezpečnostní unie EU, COM(2020) 605 final.

Protože má návrh dopad na několik směrnic Evropského parlamentu a Rady přijatých na základě čl. 53 odst. 1 SFEU, je současně přijímán i návrh směrnice, který zohledňuje nezbytné změny uvedených směrnic.

- Subsidiarita

Vysoká míra propojení finančních služeb, přeshraniční činnosti finančních subjektů a závislosti celého finančního sektoru na poskytovatelích služeb IKT z řad třetích stran, si ve společném zájmu o zachování zdravých finančních trhů EU žádá zajištění silné digitální provozní odolnosti. Nesrovnalosti vyplývající z nestejných nebo částečných režimů, překrývání nebo vícenásobných požadavků vztahujících se na stejné finanční subjekty, které působí ve více zemích nebo jsou držiteli několika oprávnění[14] na jednotném trhu lze účinně vyřešit pouze na úrovni Unie.

Tento návrh harmonizuje digitální provozní složku silně integrovaného a propojeného sektoru, který již využívá jednotný soubor pravidel a dohledu ve většině dalších klíčových oblastí. V případě otázek, jako je hlášení incidentů souvisejících s IKT, mohou míru administrativní zátěže a finanční náklady související s hlášením téhož incidentu souvisejícího s IKT různým unijním a vnitrostátním orgánům snížit pouze harmonizované předpisy Unie. Opatření na úrovni EU jsou zapotřebí rovněž k usnadnění vzájemného uznávání výsledků pokročilého testování digitální provozní odolnosti u subjektů působících ve více státech, které při absenci předpisů na úrovni Unie podléhají nebo mohou podléhat v různých členských státech různým právním rámcům. Rozdíly v přístupech k testování mezi členskými státy mohou vyřešit pouze opatření na úrovni Unie. Celounijní opatření jsou rovněž nezbytná za účelem řešení absence náležitých pravomocí v oblasti dohledu k monitorování rizik souvisejících s poskytováním služeb IKT třetími stranami, včetně rizika koncentrace a nákazy pro finanční sektor EU.

- Proporcionalita

Navrhovaná pravidla nepřekračují rámec toho, co je nezbytné pro dosažení cílů návrhu. Zabývají se pouze aspekty, které členské státy nemohou realizovat samy a u nichž jsou administrativní zátěž a náklady úměrné konkrétním a obecným cílům, kterých má být dosaženo.

K proporcionalitě se přistupuje z hlediska rozsahu a intenzity s použitím kvalitativních a kvantitativních kritérií. Ta mají zajistit, že ačkoli se nové předpisy vztahují na všechny finanční subjekty, budou současně přizpůsobeny rizikům a potřebám odpovídajícím jejich specifickému charakteru z hlediska velikosti a profilu činnosti. Proporcionalita je rovněž začleněna do pravidel řízení rizik v oblasti IKT, testování digitální odolnosti, hlášení závažných incidentů souvisejících s IKT a dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran.

- Volba nástroje

Opatření potřebná k regulaci řízení rizik v oblasti IKT, hlášení incidentů souvisejících s IKT, testování a dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran musí být pojata do nařízení, aby bylo zajištěno, že podrobné požadavky budou účinně, jednotným způsobem a přímo použitelné, aniž je dotčena proporcionalita a zvláštní pravidla stanovená

[14] Tentýž finanční subjekt může být držitelem licencí pro bankovnictví, jako investiční podnik a jako platební instituce vydaných různými orgány dohledu v jednom či více členských státech.

tímto nařízením. Konzistentní přístup k řešení digitálních operačních rizik přispívá ke zvýšení důvěry ve finanční systém a zachovává jeho stabilitu. Jelikož použití nařízení napomáhá ke zjednodušení právní úpravy, posiluje sbližování dohledu a zvyšuje právní jistotu, přispěje toto nařízení rovněž ke snížení nákladů finančních subjektů na dodržování předpisů, zejména subjektů působících ve více zemích, a tím i k narovnání hospodářské soutěže.

Toto nařízení rovněž odstraňuje legislativní nesrovnalosti a nestejné vnitrostátní přístupy k regulaci či dohledu v oblasti rizik spojených s IKT, a tím i překážky fungování jednotného trhu s finančními službami, zejména překážky bránící finančním subjektům působícím ve více státech nerušeně požívat svobody usazování a poskytování služeb.

Obsah jednotného soubor pravidel byl povětšinou rovněž vytvářen prostřednictvím nařízení, a při jeho aktualizaci o složku věnovanou digitální provozní odolnosti by tudíž měl být zvolen stejný právní nástroj.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

- Hodnocení *ex post* / kontroly účelnosti platných právních předpisů

Dosud žádné právní předpisy Unie týkající se finančních služeb se nezaměřují na provozní odolnost a žádný z nich dosud uceleně neřeší rizika plynoucí z digitalizace, a to ani ty, jež se rizikům v oblasti IKT věnují v rámci svých ustanovení obecněji se zabývajících operačními riziky. Intervence Unie dosud pomáhala řešit požadavky a problémy, které nastaly po finanční krizi z roku 2008: úvěrové instituce nedisponovaly dostatečným kapitálem, finanční trhy nebyly dostatečně integrované a harmonizace byla do té doby minimální. Rizika v oblasti IKT nebyla v té době považována za prioritu, a v důsledku toho se právní rámce různých finančních pododvětví vyvíjely nekoordinovaně. Přesto opatření Unie splnila svůj účel zajistit finanční stabilitu a vytvořit jednotný soubor harmonizovaných obezřetnostních pravidel a pravidel chování na trhu platných pro finanční subjekty v celé EU. Jelikož faktory, které vedly k legislativní intervenci Unie v minulosti, neumožňovaly přijetí specifických nebo ucelených pravidel zabývajících se širokým používáním digitálních technologií a z něj plynoucími riziky pro oblast financí, jeví se provedení jasného hodnocení jako problematické. Výsledky předpokládaného hodnocení a následné změny právních předpisů jsou vtěleny do jednotlivých pilířů tohoto nařízení.

- Konzultace se zúčastněnými stranami

Komise vedla konzultace se zúčastněnými stranami během celého procesu přípravy tohoto návrhu, zejména:

i) Komise uskutečnila zvláštní otevřenou veřejnou konzultaci (19. prosince 2019 – 19. března 2020)[15];

ii) Komise konzultovala veřejnost prostřednictvím počátečního posouzení dopadů (19. prosince 2019 – 16. ledna 2020)[16];

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

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

iii) Útvary Komise dvakrát (18. května 2020 a 16. července 2020) konzultovaly odborníky z členských států v rámci odborné skupiny pro bankovnictví, platební styk a pojišťovnictví[17];

iv) Útvary Komise uspořádaly zvláštní webinář o digitální provozní odolnosti v rámci série věnované digitálním financím (Digital Finance Outreach 2020) (19. května 2020).

Veřejná konzultace měla Komisi přinést informace ohledně vývoje potenciálního průřezového rámce EU pro digitální provozní odolnost platného napříč odvětvími v oblasti finančních služeb. Odpovědi ukázaly na širokou podporu zavedení zvláštního rámce s opatřeními zaměřenými na čtyři oblasti, jež byly předmětem konzultací, přičemž byla současně zdůrazňována nutnost zajistit proporcionalitu a pečlivě zvážit a vysvětlit vzájemné působení s horizontálními pravidly směrnice o bezpečnosti sítí a informací. Pokud jde o počáteční posouzení dopadů, obdržela Komise dvě odpovědi, v nichž se respondenti zabývali konkrétními aspekty souvisejícími s jejich oblastí činnosti.

Na zasedání odborné skupiny pro bankovnictví dne 18. května 2020 vyjádřily členské státy vysokou podporu posílení digitální provozní odolnosti ve finančním sektoru prostřednictvím opatření ve čtyřech oblastech navržených Komisí. Členské státy rovněž zdůraznily nutnost jasného propojení nových pravidel s pravidly pro operační rizika (v rámci právních předpisů EU pro finanční služby) a s horizontálními pravidly pro kybernetickou bezpečnost (směrnice o bezpečnosti sítí a informací). Během druhého zasedání některé členské státy zdůraznily nutnost zajistit proporcionalitu a zohlednit specifickou situaci malých společností nebo dceřiných subjektů velkých skupin a rovněž nutnost silného mandátu pro vnitrostátní kontrolní orgány podílející se na činnostech dohledu.

Návrh rovněž vychází ze zpětné vazby ze setkání se zúčastněnými stranami a institucemi a orgány EU a začleňuje její výstupy. Zúčastněné strany včetně poskytovatelů služeb IKT z řad třetích stran návrh celkově podpořily. Z analýzy zpětné vazby vyplývá požadavek na zachování proporcionality a požadavek přístupu k navrhování předpisů založeného na zásadách a vycházejícího z rizik. Z institucí přispěly zejména Evropská rada pro systémová rizika (ESRB), evropské orgány dohledu, Agentura Evropské unie pro kybernetickou bezpečnost (ENISA), Evropská centrální banka (ECB) a rovněž příslušné orgány členských států.

- Sběr a využití výsledků odborných konzultací

Při přípravě tohoto návrhu vycházela Komise z kvalitativních a kvantitativních údajů získaných z uznávaných zdrojů, včetně obou společných odborných doporučení evropských orgánů dohledu. Tyto údaje byly doplněny o příspěvky důvěrné povahy a veřejně dostupné zprávy orgánů dohledu, mezinárodních normalizačních orgánů a předních výzkumných institucí a rovněž o kvantitativní a kvalitativní příspěvky vybraných zúčastněných stran z celého globálního finančního sektoru.

- Posouzení dopadů

K tomuto návrhu je připojeno posouzení dopadů[18], které bylo předloženo Výboru pro kontrolu regulace dne 29. dubna 2020 a schváleno dne 29. května 2020. Výbor pro kontrolu regulace

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

doporučil v některých oblastech zlepšení s cílem: i) poskytnout více informací o tom, jak bude zajištěna proporcionalita; ii) lépe zdůraznit rozsah, v němž se upřednostňovaná možnost liší od společného odborného doporučení evropských orgánů dohledu, a proč je tato možnost optimální; a iii) lépe zdůraznit, jaké jsou vzájemné vztahy mezi návrhem a stávajícími právními předpisy EU, včetně předpisů, jež jsou v současné době předmětem přezkumu. Posouzení dopadů bylo upraveno s ohledem na tyto připomínky a rovněž na podrobnější připomínky Výboru pro kontrolu regulace.

Komise zvažovala několik možných strategií pro vypracování rámce digitální provozní odolnosti:

- „nedělat nic“: pravidla provozní odolnosti by byla i nadále stanovena stávajícím různorodým souborem ustanovení EU o finančních službách, zčásti směrnicí o bezpečnosti sítí a informací a zčásti stávajícími či budoucími vnitrostátními režimy,
- možnost 1: posílení kapitálových rezerv: byly by zavedeny další kapitálové rezervy s cílem zvýšit schopnost finančních subjektů absorbovat ztráty, jež by mohly vzniknout v důsledku nedostatečné digitální provozní odolnosti,
- možnost 2: přijetí právního předpisu o digitální provozní odolnosti finančních služeb: zavedení uceleného rámce na úrovni EU s jednotnými pravidly pro řešení potřeb digitální provozní odolnosti u všech regulovaných finančních subjektů a vytvoření rámce dohledu pro kritické poskytovatele služeb IKT z řad třetích stran,
- možnost 3: právní předpis o digitální provozní odolnosti finančních služeb v kombinaci s centralizovaným dohledem nad kritickými poskytovateli služeb IKT z řad třetích stran: kromě právního předpisu o digitální provozní odolnosti (možnost 2) by byl zřízen nový orgán pro dohled nad poskytováním služeb IKT třetími stranami.

Byla zvolena druhá možnost, jelikož dosahuje většiny zamýšlených cílů způsobem, který je účinný, efektivní a soudržný s ostatními politikami Unie. Tuto možnost upřednostňovala rovněž většina zúčastněných stran.

Zvolená možnost přinese jednorázové i opakující se náklady[19]. Jednorázové náklady vzniknou zejména v důsledku investic do systémů IT, a jsou proto obtížně vyčíslitelné vzhledem k různému stavu celkových struktur IT podniků, a zejména jejich stávajících systémů IT. Přesto budou pravděpodobně tyto náklady u velkých podniků omezené vzhledem ke značným investicím, které již tyto podniky do IKT vložily. Omezené náklady se očekávají rovněž u menších podniků, neboť se na ně s ohledem na jejich nižší míru rizika budou vztahovat proporcionální opatření.

Zvolená možnost by měla příznivé ekonomické, sociální a environmentální dopady u malých a středních podniků působících v odvětví finančních služeb. Návrh zlepší přehled malých a středních podniků ohledně použitelných předpisů, což sníží náklady na jejich dodržování.

Hlavní sociální dopady zvolené možnosti se budou týkat spotřebitelů a investorů. Vyšší úroveň digitální provozní odolnosti finančního systému EU sníží počet incidentů a průměrné

---

[18] Pracovní dokument útvarů Komise – Zpráva o posouzení dopadů – průvodní dokument k nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, SWD(2020) 198 ze dne 24. září 2020.

[19] *Tamtéž, s. 89–94.*

náklady s nimi spojené. Zvýšená důvěra v odvětví finančních služeb prospěje celé společnosti.

Pokud jde o environmentální dopady, zvolená možnost bude podporovat vyšší míru využívání infrastruktur a služeb IKT poslední generace, u nichž se očekává, že budou ekologicky udržitelnější.

- Účelnost právních předpisů a zjednodušení

Odstranění překrývajících se požadavků na hlášení incidentů souvisejících s IKT sníží administrativní zátěž a související náklady. Harmonizované testování digitální provozní odolnosti se vzájemným uznáváním na celém jednotném trhu navíc sníží náklady, zejména pro přeshraniční firmy, které by jinak musely absolvovat v různých členských státech několik testů[20].

- Základní práva

EU se zasazuje o zajišťování vysoké úrovně ochrany základních práv. Veškerá dobrovolná ujednání o sdílení informací mezi finančními subjekty, jež toto nařízení podporuje, budou prováděna v důvěryhodném prostředí a v jejich rámci budou plně dodržována pravidla Unie pro ochranu osobních údajů, zejména nařízení Evropského parlamentu a Rady (EU) 2016/679[21], a to především v případech, kdy je zpracování osobních údajů nezbytné pro účely oprávněného zájmu správce.

4. ROZPOČTOVÉ DŮSLEDKY

Jelikož toto nařízení počítá s posílením úlohy evropských orgánů dohledu prostřednictvím pravomocí jim udělených za účelem příslušného dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran, znamenal by tento návrh z rozpočtového hlediska použití navýšených prostředků, zejména za účelem plnění úkolů dohledu (např. provádění kontrol a auditů na místě i on-line) a nasazení personálu se specifickými odbornými znalostmi v oblasti bezpečnosti IKT.

Rozsah a rozdělení těchto nákladů bude záviset na rozsahu nových pravomocí dohledu a na (přesných) úkolech prováděných evropskými orgánu dohledu. Pokud jde o zajištění nového personálu, budou EBA, ESMA a EIOPA potřebovat celkem 18 pracovníků na plný úvazek – šest pracovníků na plný úvazek pro každý orgán – jakmile se různá ustanovení tohoto návrhu stanou použitelnými (odhadem 15,71 milionu EUR na období 2022–2027). Evropským orgánům dohledu rovněž vzniknou další náklady související s IT, výdaje na služební cesty za účelem kontrol na místě a náklady na překlady (odhadem 12 milionů EUR na období 2022–2027), jakož i další administrativní výdaje (odhadem 2,48 milionu EUR na období 2022–2027). Proto se celkový dopad s ohledem na náklady odhaduje přibližně na 30,19 milionu EUR na období 2022–2027.

Rovněž je třeba poznamenat, že ačkoli náklady na počet pracovníků (např. noví zaměstnanci a další výdaje spojené s novými úkoly) potřebných pro výkon přímého dohledu budou v budoucnu záviset na vývoji počtu a velikosti kritických poskytovatelů služeb IKT z řad třetích stran podléhajících dohledu, příslušné výdaje budou plně hrazeny z poplatků vybíraných od

[20] *Tamtéž.*

[21] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

těchto účastníků trhu. Nepředpokládá se proto žádný dopad na rozpočet EU (kromě dalšího personálu), neboť tyto náklady budou plně hrazeny z poplatků.

Finanční a rozpočtové důsledky tohoto návrhu jsou podrobně vysvětleny v legislativním finančním výkazu připojeném k tomuto návrhu.

5. OSTATNÍ PRVKY

- Plány provádění a způsoby monitorování, hodnocení a podávání zpráv

Návrh zahrnuje obecný plán monitorování a hodnocení dopadů na specifické cíle, který vyžaduje, aby Komise alespoň tři roky po vstupu v platnost provedla přezkum a o svých hlavních zjištěních informovala Evropský parlament a Radu.

Přezkum bude proveden v souladu s pokyny Komise pro zlepšování právní úpravy.

- Podrobné vysvětlení konkrétních ustanovení návrhu

Návrh je strukturován do několika hlavních oblastí, jež jsou klíčovými vzájemně propojenými pilíři konsensuálně začleněnými do evropských a mezinárodních pokynů a osvědčených postupů zaměřených na zlepšení kybernetické a provozní odolnosti finančního sektoru.

Oblast působnosti nařízení a uplatnění proporcionality u nutných opatření (článek 2)

Aby byla zajištěna konzistentnost v souvislosti s požadavky na řízení rizik v oblasti IKT platnými pro finanční sektor, vztahuje se nařízení na řadu finančních subjektů regulovaných na úrovni Unie, konkrétně na úvěrové instituce, platební instituce, instituce elektronických peněz, investiční podniky, poskytovatele služeb souvisejících s kryptoaktivy, centrální depozitáře cenných papírů, ústřední protistrany, obchodní systémy, registry obchodních údajů, správce alternativních investičních fondů a správcovské společnosti, poskytovatele služeb hlášení údajů, pojišťovny a zajišťovny, zprostředkovatele pojištění, zprostředkovatele zajištění a zprostředkovatele doplňkového pojištění, instituce zaměstnaneckého penzijního pojištění, ratingové agentury, statutární auditory a auditorské společnosti, správce kritických referenčních hodnot a poskytovatele služeb skupinového financování.

Takto vymezená oblast působnosti usnadňuje homogenní a jednotné uplatňování všech složek řízení rizik v oblastech souvisejících s IKT a současně zajišťuje rovné podmínky mezi finančními subjekty, pokud jde o jejich regulační povinnosti související s riziky v oblasti IKT. Nařízení zároveň respektuje existenci významných rozdílů mezi finančními subjekty, pokud jde o jejich velikost, profil činnosti nebo v souvislosti s jejich expozicí digitálním rizikům. Jelikož větší finanční subjekty mají více zdrojů, je například požadováno pouze od finančních subjektů jiných než mikropodniky, aby zavedly komplexní mechanismy správy a řízení a speciální řídicí funkce, aby po velkých změnách v síti a v infrastrukturách informačních systémů prováděly hloubková posouzení a aby pravidelně prováděly analýzu rizik dříve zavedených systémů IKT a rozšířily testování zachování provozu a plány reakce a obnovy provozu tak, aby zahrnovaly i scénáře přepínání mezi primární infrastrukturou IKT a rezervními prostředky. Dále pouze finanční subjekty považované za významné pro účely pokročilého testování digitální odolnosti budou povinny provádět penetrační testy na základě hrozeb.

Ačkoli je působnost takto rozsáhlá, není vyčerpávající. Toto nařízení se konkrétně nevztahuje na provozovatele systémů podle čl. 2 písm. p) směrnice 98/26/ES[22] o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry ani na žádné účastníky systému, není-li takový účastník sám finančním subjektem regulovaným na úrovni Unie (tj. úvěrová instituce, investiční podnik, ústřední protistrana) – pak by se na něj toto nařízení vztahovalo v každém případě. Dále do oblasti působnosti nespadá registr Unie pro emisní povolenky, který funguje podle směrnice 2003/87/ES[23] pod záštitou Evropské komise.

Tyto výjimky ze směrnice o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry zohledňují nutnost dalšího přezkumu právních a politických otázek týkajících se provozovatelů systémů a účastníků podle uvedené směrnice a současně patřičně přihlížejí k dopadu rámců v současné době platných pro platební systémy[24] provozované centrálními bankami. Jelikož součástí těchto otázek mohou být aspekty odlišné od problematiky, již upravuje toto nařízení, bude Komise pokračovat v posuzování nutnosti dalšího rozšiřování jeho oblasti působnosti na subjekty a infrastruktury IKT, na něž se v současnosti nevztahuje, a dopadů takového rozšiřování.

Požadavky týkající se správy a řízení (článek 4)

Toto nařízení je navrženo tak, aby docházelo k lepšímu sladění obchodních strategií finančních subjektů a provádění řízení rizik v oblasti IKT. Za tím účelem bude od vedoucích orgánů vyžadováno, aby zastávaly klíčovou, aktivní úlohu při vedení rámce řízení rizik v oblasti IKT a zasazovaly se o dodržování přísné kybernetické hygieny. Plná odpovědnost vedoucího orgánu při řízení rizik IKT finančního subjektu bude zastřešujícím principem, který bude dále promítnut do souboru konkrétních požadavků, jako je přidělení jasných úloh a odpovědností pro všechny funkce související s IKT, neustálá kontrola monitorování řízení rizik v oblasti IKT a rovněž do celé škály schvalovacích a kontrolních postupů a vhodného rozdělení investic a školení v oblasti IKT.

Požadavky na řízení rizik v oblasti IKT (články 5 až 14)

Digitální provozní odolnost vychází ze souboru klíčových zásad a požadavků na rámec řízení rizik v oblasti IKT, který je v souladu se společným odborným doporučením evropských orgánů dohledu. Tyto požadavky, inspirované příslušnými mezinárodními, vnitrostátními a odvětvovými normami, pokyny a doporučeními, se týkají specifických funkcí řízení rizik v oblasti IKT (identifikace, ochrana a prevence, detekce, reakce a obnova provozu, vzdělávání a rozvoj a komunikace). Aby finanční subjekty udržely krok s rychle se rozvíjející oblastí kybernetických hrozeb, musí jako nedílnou součást provozní strategie zachování provozu vytvořit a spravovat systémy a nástroje IKT, které minimalizují dopad rizik v oblasti IKT, nepřetržitě identifikovat všechny zdroje rizik v oblasti IKT, vytvořit ochranná a preventivní opatření, rychle zjišťovat anomální činnosti, uplatňovat specializované a komplexní strategie zachování provozu a plány pro případ havárie a plány obnovy provozu. Poslední uvedené

[22] Směrnice Evropského parlamentu a Rady 98/26/ES ze dne 19. května 1998 o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry (Úř. věst. L 166, 11.6.1998, s. 45).

[23] Směrnice Evropského parlamentu a Rady 2003/87/ES ze dne 13. října 2003 o vytvoření systému pro obchodování s povolenkami na emise skleníkových plynů ve Společenství a o změně směrnice Rady 96/61/ES (Úř. věst. L 275, 25.10.2003, s. 32).

[24] Zejména nařízení Evropské centrální banky (EU) č. 795/2014 ze dne 3. července 2014 o požadavcích v oblasti dozoru nad systémově významnými platebními systémy.

složky jsou nezbytné pro rychlou obnovu provozu po incidentech souvisejících s IKT, zejména kybernetických útocích, pomocí omezení škod a upřednostnění činností pro obnovu bezpečnosti. Samotné nařízení nestanoví konkrétní normalizaci, spíše vychází z evropských a mezinárodně uznávaných technických norem nebo odvětvových osvědčených postupů, pokud zcela odpovídají pokynům orgánů dohledu pro použití a začlenění těchto mezinárodních norem. Toto nařízení se rovněž týká integrity, bezpečnosti a odolnosti fyzických infrastruktur a prostředků podporujících využívání technologií a příslušných procesů a pracovníků z oblasti IKT v rámci digitální stopy činností finančního subjektu.

Požadavky na hlášení incidentů souvisejících s IKT (články 15 až 20)

Harmonizace a zjednodušení hlášení incidentů souvisejících s IKT je dosaženo, zaprvé, obecným požadavkem, aby finanční subjekty vytvořily a uplatňovaly proces řízení sledování a evidence incidentů souvisejících s IKT a dále povinností jejich klasifikace podle kritérií uvedených v tomto nařízení a dále rozvíjených evropskými orgány dohledu prostřednictvím stanovení limitů významnosti. Zadruhé, příslušným orgánům musí být hlášeny pouze incidenty související s IKT, které jsou považovány za závažné. Hlášení je třeba zpracovávat podle společného vzoru a harmonizovaným postupem vypracovaným evropskými orgány dohledu. Finanční subjekty by měly předkládat prvotní, průběžné a závěrečné zprávy a informovat své uživatele a klienty v případech, kdy incident má nebo může mít dopad na jejich finanční zájmy. Příslušné orgány by měly poskytnout dotčené údaje o incidentech ostatním institucím nebo orgánům: evropským orgánům dohledu, Evropské centrální bance a jednotným kontaktním místům stanoveným podle směrnice (EU) 2016/1148.

Za účelem zahájení dialogu mezi finančními subjekty a příslušnými orgány, který by pomohl minimalizovat dopad a identifikovat vhodné nápravné prostředky, by mělo být hlášení závažných incidentů souvisejících s IKT doplněno o zpětnou vazbu a pokyny orgánu dohledu.

A konečně, možnost centralizace hlášení incidentů souvisejících s IKT by měla být dále prozkoumána ve společné zprávě evropských orgánů dohledu, Evropské centrální banky a ENISA, kde bude posouzena proveditelnost vytvoření jednotného centra EU pro hlášení závažných incidentů souvisejících s IKT finančními subjekty.

Testování digitální provozní odolnosti (články 21 až 24)

Prostředky a funkce obsažené v rámci řízení rizik v oblasti IKT musí být pravidelně testovány na připravenost a identifikaci slabin, nedostatků či mezer a také rychlé uplatňování nápravných opatření. Toto nařízení umožňuje proporcionální použití požadavků na testování digitální provozní odolnosti podle velikosti a profilů činnosti a rizik finančních subjektů: zatímco testování IKT nástrojů a systémů by měly provádět všechny subjekty, pokročilé testování prostřednictvím penetračních testů na základě hrozeb by se mělo týkat pouze subjektů určených příslušnými orgány (podle kritérií tohoto nařízení a dalších kritérií vypracovaných evropskými orgány dohledu) jako významné a kyberneticky vyspělé. Toto nařízení rovněž stanoví požadavky na subjekty provádějící testování a uznávání výsledků penetračních testů na základě hrozeb u finančních subjektů působících v několika členských státech v celé Unii.

Rizika v oblasti IKT spojená s třetími stranami (články 25 až 39)

Nařízení je navrženo tak, aby bylo zajištěno stabilní sledování rizik v oblasti IKT spojených s třetími stranami. Tohoto cíle bude dosaženo zaprvé dodržováním pravidel založených na zásadách, která platí pro sledování rizik, jež představují poskytovatelé služeb IKT z řad třetích stran. Zadruhé, toto nařízení harmonizuje hlavní prvky služeb a vztahů s poskytovateli služeb IKT z řad třetích stran. Tyto prvky se týkají minimálních aspektů považovaných za zásadní pro umožnění úplného sledování rizik v oblasti IKT spojeného s třetími stranami finančním

subjektem v průběhu uzavírání smlouvy, jejího plnění, ukončení a následných fází po ukončení jejich vztahu.

Zejména bude požadováno, aby smlouvy, jimiž se tento vztah řídí, obsahovaly úplný popis služeb, uváděly místa, kde budou údaje zpracovávány, dále úplný popis úrovně služeb doplněný o kvantitativní i kvalitativní výkonové cíle, příslušná ustanovení o přístupnosti, dostupnosti, integritě, zabezpečení a ochraně osobních údajů a aby zaručovaly přístup, obnovu a vrácení v případě selhání poskytovatelů služeb IKT z řad třetích stran, aby uváděly lhůty a povinnosti hlášení poskytovatelů služeb IKT z řad třetích stran, právo na přístup, kontrolu a audit finančním subjektem nebo určeným třetím subjektem, jasná práva na vypovězení a specializované strategie pro ukončení smluvního vztahu. Protože mohou být některé z těchto smluvních prvků navíc standardizovány, podporuje toto nařízení dobrovolné používání standardních smluvních doložek, které by měla Komise vypracovat pro oblast používání cloudových výpočetních služeb.

Nakonec toto zařízení podporuje sbližování dohledových přístupů nad riziky v oblasti IKT spojenými s třetími stranami ve finančním sektoru tím, že se na kritické poskytovatele služeb IKT z řad třetích stran bude vztahovat rámec dohledu Unie. Prostřednictvím nového harmonizovaného legislativního rámce získá evropský orgán dohledu stanovený jako hlavní orgán dohledu pro každého dodavatele služeb IKT z řad třetích stran pravomoci zajistit, aby byli poskytovatelé technologických služeb, kteří plní klíčovou úlohu ve fungování finančního sektoru, v celé Evropě řádně sledováni. Rámec dohledu navrhovaný tímto nařízením vychází ze stávající institucionální architektury v oblasti finančních služeb, přičemž společný výbor evropských orgánů dohledu zajistí v souladu se svými úkoly v oblasti kybernetické bezpečnosti koordinaci ohledně všech záležitostí rizik v oblasti IKT, v tom mu pomůže příslušný podvýbor (fórum dohledu) provádějící přípravné práce pro individuální rozhodnutí a kolektivní doporučení kritickým třetím stranám poskytujícím služby.

Sdílení informací (článek 40)

Za účelem zvýšení povědomí o rizicích IKT, minimalizace jejich šíření, podpory obranných prostředků finančních subjektů a technik zjišťování hrozeb toto nařízení umožňuje, aby finanční subjekty zajistily vzájemnou výměnu operativních a jiných informací o kybernetických hrozbách.

2020/0266 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY

o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014

(Text s významem pro EHP)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropské centrální banky,[25]

s ohledem na stanovisko Evropského hospodářského a sociálního výboru,[26]

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) V digitálním věku podporují informační a komunikační technologie (IKT) složité systémy používané pro každodenní společenské činnosti. Udržují v chodu klíčová odvětví našich ekonomik, včetně finančního sektoru, a zlepšují fungování jednotného trhu. Vyšší míra digitalizace a vzájemné propojenosti rovněž zvýrazňuje rizika v oblasti IKT, díky nimž se celá společnost – a zejména finanční systém – stávají zranitelnějšími vůči finančním hrozbám nebo narušením v oblasti IKT. Zatímco všudypřítomné používání systémů IKT a vysoká míra digitalizace a propojení nyní tvoří základní charakteristiky všech činností finančních subjektů Unie, digitální odolnost dosud není ve svých provozních rámcích dostatečná.

(2) Použití IKT získalo v posledních desetiletích v oblasti financí klíčovou úlohu a dnes má zásadní význam při provádění obvyklých běžných funkcí všech finančních subjektů. Digitalizace se například týká plateb, které se stále více přesouvají od hotovostních a papírových metod k používání digitálních řešení, a rovněž clearingu a vypořádání cenných papírů, elektronického a algoritmického obchodování, operací půjčování a financování, sdíleného financování, úvěrového hodnocení, upisování pojištění, správy pohledávek a činnosti provozních útvarů. Finanční sektor nejenže se digitalizoval jako celek, ale v důsledku digitalizace se rovněž prohloubila jeho interní propojení a závislosti a rovněž propojení a závislosti mezi ním a poskytovateli infrastruktury a služeb z řad třetích stran.

(3) Evropská rada pro systémová rizika (ESRB) ve své zprávě z roku 2020 zabývající se systémovými kybernetickými riziky[27] potvrdila, jak stávající vysoká míra vzájemného

[25] [*doplňte odkaz*] Úř. věst C , , s. .
[26] [*doplňte odkaz*] Úř. věst C , , s. .

propojení finančních subjektů, finančních trhů a infrastruktur finančních trhů, a zejména vzájemná závislost jejich systémů IKT, může potenciálně představovat systémovou zranitelnost, protože se místní kybernetické incidenty mohou rychle rozšířit z kteréhokoliv z přibližně 22 000 finančních subjektů Unie[28] na celý finanční systém, čemuž nezabrání ani geografické hranice. Závažná narušení IKT, k nimž dochází v odvětví financí, nedopadají pouze na izolované finanční subjekty. Rovněž usnadňují šíření lokalizovaných rizik napříč finančními přenosovými kanály a potenciálně vytvářejí negativní důsledky pro stabilitu finančního systému Unie, neboť vedou k hromadným výběrům hotovosti a celkové ztrátě jistoty a důvěry na finančních trzích.

(4) Rizika v oblasti IKT v poslední době přitahují pozornost vnitrostátních, evropských i mezinárodních tvůrců politik, regulátorů a standardizačních orgánů, které se snaží o zlepšení odolnosti, stanovení norem a koordinaci regulatorních a dohledových činností. Na mezinárodní úrovni se Basilejský výbor pro bankovní dohled, Výbor pro platební a vypořádací systémy, Rada pro finanční stabilitu, Institut pro finanční stabilitu a rovněž skupiny zemí G7 a G20 zaměřují na vybavení příslušných orgánů a účastníků trhu v různých jurisdikcích nástroji pro posílení odolnosti jejich finančních systémů.

(5) Přes cílené politiky a legislativní iniciativy na vnitrostátní i evropské úrovni představují rizika v oblasti IKT problém pro provozní odolnost, výkonnost a stabilitu finančního systému Unie. Reforma, která následovala po finanční krizi z roku 2008, primárně posílila finanční odolnost finančního sektoru Unie a zaměřovala se na zajištění konkurenceschopnosti a stability z hlediska ekonomiky, obezřetnosti a chování na trhu. Přestože jsou zabezpečení IKT a digitální odolnost součástí operačních rizik, regulatorní agenda se jim po krizi věnovala méně a rozvíjely se pouze v některých oblastech strategického a regulatorního rámce finančních služeb Unie nebo jen v několika málo členských státech.

(6) Akční plán Komise pro finanční technologie z roku 2018[29] zdůrazňoval nejvyšší důležitost zlepšení odolnosti finančního sektoru Unie rovněž z provozního z hlediska, aby byla zajištěna jeho technologická bezpečnost a správné fungování, jeho rychlé zotavení z narušení a incidentů souvisejících s IKT a konečně aby mohly být finanční služby efektivně a bezproblémově poskytovány v celé Unii, a to i v krizových situacích, a aby byla současně zachována důvěra a jistota spotřebitelů a trhu.

(7) V dubnu 2019 Evropský orgán pro bankovnictví (EBA), Evropský orgán pro cenné papíry a trhy (ESMA) a Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní

---

27 Zpráva ESRB Systémová kybernetická rizika z února 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Podle posouzení dopadů přiložených k přezkumu evropských orgánů dohledu, (SWD(2017) 308, existuje asi 5 665 úvěrových institucí, 5 934 investičních podniků, 2 666 pojišťoven, 1 573 institucí důchodového pojištění, 2 500 společností správy investic, 350 tržních infrastruktur (například ústředních protistran, burz, systematických internalizátorů, registrů obchodních údajů a systémů obchodování), 45 ratingových agentur a 2 500 schválených platebních institucí a institucí elektronických peněz. Dohromady tvoří přibližně 21 233 subjektů bez subjektů skupinového financování, statutárních auditorů a auditorských společností, poskytovatelů služeb souvisejících s kryptoaktivy a správců referenčních hodnot.

29 Sdělení Komise Evropskému parlamentu, Radě, Evropské centrální bance, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů *Akční plán pro finanční technologie: Za konkurenceschopnější a inovativnější evropský finanční sektor*, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

pojištění (EIOPA) (společně nazývané „evropské orgány dohledu“ nebo „ESA“) společně vydaly dvoudílné odborné doporučení požadující jednotný přístup k rizikům v oblasti IKT ve finančním sektoru a doporučující proporcionální posílení digitální provozní odolnosti odvětví finančních služeb prostřednictvím konkrétní odvětvové iniciativy Unie.

(8) Finanční sektor Unie je upraven harmonizovaným jednotným souborem pravidel a řídí jej evropský systém dohledu nad finančním trhem. Nicméně ustanovení zabývající se digitální provozní odolností a zabezpečením IKT nejsou dosud plně nebo konzistentně harmonizovaná, přestože je digitální provozní odolnost klíčová pro zajištění finanční stability a integrity trhu v digitálním věku a není o nic méně důležitá než například společné normy pro obezřetnost nebo chování na trhu. Proto je třeba vypracovat jednotný soubor pravidel a systém dohledu, aby byla rovněž zahrnuta tato složka, pomocí rozšíření mandátů orgánů finančního dohledu pověřených sledováním a ochranou finanční stability a integrity trhu.

(9) Legislativní nesrovnalosti a nerovné vnitrostátní regulatorní nebo dohledové přístupy k rizikům v oblasti IKT jsou příčinou překážek pro jednotný trh s finančními službami a brání bezproblémovému výkonu svobody usazování a poskytování služeb finančním subjektům s přeshraniční přítomností. Rovněž může docházet k narušení hospodářské soutěže stejného druhu finančních subjektů činných v různých členských státech. Zejména v oblastech, kde je harmonizace Unie velmi omezená – například testování digitální provozní odolnosti – nebo chybí – například sledování rizik v oblasti IKT spojených s třetími stranami – mohou nesrovnalosti pocházející z předpokládaného vývoje na vnitrostátní úrovni vytvářet další překážky fungování jednotného trhu, což poškozuje účastníky trhu a finanční stabilitu.

(10) Částečný způsob, kterým byla ustanovení týkající se rizik v oblasti IKT dosud řešena na úrovni Unie, vykazuje mezery či přesahy ve významných oblastech, jako je hlášení incidentů souvisejících s IKT a testování digitální provozní odolnosti, a vytváří nesrovnalosti vyplývající z rozdílných vnitrostátních předpisů nebo nákladově neefektivního používání překrývajících se pravidel. Poškozuje to zejména intenzivní uživatele IKT, jako je finanční sektor, protože technologická rizika neznají hranice a finanční sektor poskytuje své služby ve velké míře přeshraničně jak v rámci Unie, tak mimo ni.

Jednotlivé finanční subjekty fungující na přeshraničním základě nebo vlastnící několik oprávnění (např. jeden finanční subjekt může vlastnit licence pro bankovnictví, investiční podnik a platební instituci vydané jiným příslušným orgánem v jednom či několika členských státech) čelí provozním problémům při řešení rizik v oblasti IKT a zmírňování dopadů incidentů souvisejících s IKT vlastními silami a jednotným nákladově efektivním způsobem.

(11) Protože není jednotný soubor pravidel doprovázen komplexním rámcem pro rizika v oblasti IKT nebo operační rizika, je nutná harmonizace klíčových požadavků na provozní digitální odolnost pro všechny finanční subjekty. Prostředky a celková odolnost, které budou finanční subjekty na základě těchto klíčových požadavků rozvíjet, aby odolaly výpadkům provozu, pomohou zachovat stabilitu a integritu finančních trhů Unie, což přispěje k zajištění vysoké úrovně ochrany investorů a spotřebitelů v Unii. Protože se toto nařízení zaměřuje na bezproblémové fungování jednotného trhu, mělo by vycházet z ustanovení článku 114 SFEU, jak je interpretováno v souladu s konzistentní judikaturou Evropského soudního dvora.

(12) Toto nařízení se zaměřuje na konsolidaci a aktualizaci požadavků týkajících se rizik v oblasti IKT, které byly dosud samostatně řešeny v různých nařízeních a směrnicích. Zatímco se tyto právní akty Unie zabývají hlavními kategoriemi finančních rizik (např. úvěrovým rizikem, tržním rizikem, úvěrovým rizikem protistrany a rizikem likvidity, rizikem chováním trhu), nedokázaly v době svého přijetí komplexně vyřešit všechny složky provozní odolnosti. Požadavky týkající se operačních rizik, jsou-li dále rozpracovány prostřednictvím těchto právních aktů Unie, často upřednostňují při řešení těchto rizik tradiční kvantitativní přístup (konkrétně stanovení kapitálových požadavků na krytí rizik v oblasti IKT) namísto zahrnutí cílených kvalitativních požadavků na podporu prostředků prostřednictvím požadavků proti incidentům souvisejícím s IKT spočívajících v ochraně, odhalování, izolaci, zotavení a obnově, nebo prostřednictvím stanovení hlášení a digitálního testování. Tyto směrnice a předpisy byly primárně určeny k pokrytí základních pravidel obezřetnostního dohledu, integrity trhu nebo chování na něm.

V tomto dokumentu, který konsoliduje a aktualizuje pravidla pro rizika v oblasti IKT, jsou poprvé konzistentně a v rámci jediného legislativního aktu shrnuta všechna ustanovení zabývající se digitálními riziky v odvětví financí. Tato iniciativa by tedy měla zaplnit mezery či napravit nesrovnalosti v některých těchto právních aktech, včetně v nich použité terminologie, a měla by výslovně řešit rizika v oblasti IKT prostřednictvím cílených pravidel pro prostředky řízení rizik v oblasti IKT, hlášení a testování a sledování rizik spojených s třetími stranami.

(13) Finanční subjekty by měly při řešení rizik v oblasti IKT postupovat stejně a dodržovat stejná pravidla založená na zásadách. Konzistentnost přispívá ke zvýšení důvěry ve finanční systém a zachování jeho stability, zejména v době nadměrného užívání IKT systémů, platforem a infrastruktur se zvýšenými digitálními riziky.

Dodržování základní kybernetické hygieny by rovněž mělo zabránit vysokým ekonomickým výdajům, protože minimalizuje dopad a náklady narušení IKT.

(14) Použití tohoto nařízení pomáhá snižovat složitost právních předpisů, posiluje konvergenci dohledu, zvyšuje právní jistotu a současně rovněž přispívá ke snížení nákladů na dodržování předpisů, zejména u finančních subjektů působících přeshraničně, a omezuje narušení hospodářské soutěže. Výběr nařízení pro vytvoření společného rámce digitální provozní odolnosti finančních subjektů se proto jeví jako nejvhodnější způsob zaručení homogenního a jednotného využívání všech složek řízení rizik v oblasti IKT ve finančních odvětvích Unie.

(15) Kromě právních předpisů o finančních službách je současným hlavním rámcem kybernetické bezpečnosti na úrovni Unie směrnice Evropského parlamentu a Rady (EU) 2016/1148[30]. V sedmi kritických odvětvích se tato směrnice vztahuje rovněž na tři druhy finančních subjektů, konkrétně na úvěrové instituce, obchodní systémy a ústřední protistrany. Protože však směrnice (EU) 2016/1148 stanoví mechanismus vnitrostátní identifikace provozovatelů zásadních služeb, jsou v praxi do její oblasti působnosti zahrnuty pouze některé úvěrové instituce, obchodní systémy a ústřední protistrany identifikované členskými státy, které tak musí splňovat v této směrnici stanovené požadavky na bezpečnost IKT a hlášení incidentů.

[30] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

(16) Protože toto nařízení zvyšuje zavedením požadavků na řízení rizik v oblasti IKT a hlášení incidentů souvisejících s IKT, které jsou přísnější než požadavky stanovené v současných právních předpisech Unie pro finanční služby, úroveň harmonizace složek digitální odolnosti, představuje lepší harmonizaci i ve srovnání s požadavky uvedenými ve směrnici (EU) 2016/1148. Proto toto nařízení představuje *lex specialis* pro směrnici (EU) 2016/1148.

Je zásadní zachovat silný vztah mezi finančním sektorem a horizontální rámec Unie pro kybernetickou bezpečnost zajistí konzistentnost se strategiemi kybernetické bezpečnosti již přijatými členskými státy a umožní informovanost orgánů finančního dohledu o kybernetických incidentech dopadajících na další odvětví upravená směrnicí (EU) 2016/1148.

(17) Aby byl možný meziodvětvový proces učení a efektivní čerpání zkušeností při řešení kybernetických hrozeb z ostatních odvětví, měly by finanční subjekty uvedené ve směrnici (EU) 2016/1148 zůstat součástí „ekosystému“ podle této směrnice (např. skupina pro spolupráci v oblasti bezpečnosti sítí a informací – NIS a pracovní skupiny pro řešení kybernetických bezpečnostních incidentů – CSIRT).

Evropské orgány dohledu a případně vnitrostátní příslušné orgány by rovněž měly být schopny účastnit se politických diskusí o strategii a případně technických činností skupiny pro spolupráci NIS, vyměňovat si informace a dále spolupracovat s jednotnými kontaktními místy stanovenými směrnicí (EU) 2016/1148. Příslušné orgány podle tohoto nařízení by rovněž měly konzultovat a spolupracovat s vnitrostátními skupinami CSIRT uvedenými v článku 9 směrnice (EU) 2016/1148.

(18) Je rovněž důležité zajistit soulad se směrnicí o určování a označování evropských kritických infrastruktur (EKI), která je nyní revidována za účelem zlepšení ochrany a odolnosti kritických infrastruktur před jinými než kybernetickými hrozbami s možnými dopady na finanční sektor[31].

(19) Poskytovatelé cloudových výpočetních služeb jsou jednou z kategorií poskytovatelů digitálních služeb upravených směrnicí (EU) 2016/1148. Proto podléhají následnému dohledu prováděnému vnitrostátními orgány stanovenými touto směrnicí, který je omezen na požadavky na bezpečnost IKT a hlášení incidentů podle tohoto aktu. Protože rámec dohledu vytvořený tímto nařízením platí pro všechny kritické poskytovatele služeb IKT z řad třetích stran, včetně poskytovatelů cloudových výpočetních služeb, pokud poskytují služby IKT finančním subjektům, měl by být považován za doplnění dohledu prováděného podle směrnice (EU) 2016/1148. Kromě toho by se měl rámec dohledu vytvořený tímto nařízením vztahovat i na poskytovatele cloudových výpočetních služeb, neboť v Unii neexistuje horizontální rámec nerozlišující mezi jednotlivými odvětvími.

(20) Aby zůstala zajištěna úplná kontrola nad riziky v oblasti IKT, musí mít finanční subjekty k dispozici komplexní prostředky umožňující silné a účinné řízení rizik v oblasti IKT a specifické mechanismy a strategie pro hlášení incidentů souvisejících s IKT, testování systémů, kontrolních mechanismů a procesů v oblasti IKT a pro řízení rizik v oblasti IKT spojených s třetími stranami. Je třeba zvýšit práh digitální provozní odolnosti finančního systému a současně umožnit proporcionální uplatňování

[31] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu (Úř. věst. L 345, 23.12.2008, s. 75).

požadavků na finanční subjekty, které jsou mikropodniky podle doporučení Komise 2003/361/ES[32].

(21) Prahové hodnoty a taxonomie pro hlášení incidentů souvisejících s IKT se na vnitrostátní úrovni významně liší. Zatímco je možné společného cíle u finančních subjektů podle směrnice (EU) 2016/1148 dosáhnout relevantní prací Agentury Evropské unie pro kybernetickou bezpečnost (ENISA)[33] a Skupiny pro spolupráci NIS, mohou u ostatních finančních subjektů stále existovat různé přístupy k mezním hodnotám a taxonomiím. To zahrnuje několik požadavků, které musí finanční subjekty dodržovat, zejména při fungování ve víceru unijních jurisdikcí a v rámci finanční skupiny. Tyto rozdíly mohou navíc omezovat vytváření dalších unijních jednotných nebo centralizovaných mechanismů urychlujících proces hlášení a podporujících rychlou a bezproblémovou výměnu informací mezi příslušnými orgány, která je zásadní pro řešení rizik v oblasti IKT v případě rozsáhlých útoků s potenciálními dopady na systémy.

(22) Aby mohly příslušné orgány plnit své dohledové funkce získáním úplného přehledu o povaze, četnosti, významu a dopadu incidentů souvisejících s IKT a zlepšila se výměna informací mezi relevantními veřejnými orgány, včetně donucovacích orgánů a orgánů příslušných k řešení krize, je nutné stanovit pravidla doplňující režim hlášení incidentů souvisejících s IKT o požadavky, které v současné době chybí v právních předpisech pro finanční pododvětví, a odstranit stávající překrytí a zdvojení, což sníží náklady. Proto je zásadní harmonizovat režim hlášení incidentů souvisejících s IKT tím, že všechny finanční subjekty budou muset podávat hlášení pouze svým příslušným orgánům. Kromě toho by měly evropské orgány dohledu získat pravomoc dále upřesnit prvky hlášení incidentů souvisejících s IKT, jako jsou taxonomie, časové rámce, soubory údajů, vzory a platné mezní hodnoty.

(23) Požadavky na testování digitální provozní odolnosti jsou v některých finančních pododvětvích stanoveny v mnoha nekoordinovaných vnitrostátních rámcích, které řeší stejné otázky různým způsobem. To vede ke zdvojení nákladů pro přeshraniční finanční subjekty a ztěžuje vzájemné uznávání výsledků. Nekoordinované testování proto může jednotný trh rozdělovat.

(24) Dále, nebude-li požadováno testování, zůstanou nezjištěny slabiny, které významně ohrožují finanční subjekt a v konečném důsledku i stabilitu a integritu finančního sektoru. Bez zásahu Unie by bylo testování digitální provozní odolnosti nadále roztříštěné a neexistovalo by vzájemné uznávání výsledků testování v různých jurisdikcích. Protože je rovněž nepravděpodobné, že by další finanční pododvětví přijala tato schémata ve smysluplném rozsahu, promarnily by potenciální výhody, například odhalení zranitelných míst a rizik, prostředky testování bezpečnosti a zachování provozu, a zvýšenou důvěru klientů, dodavatelů a obchodních partnerů. K odstranění těchto přesahů, rozdílů a mezer je nutné stanovit pravidla zaměřená na koordinaci testování finančními subjekty a kompetentními orgány, což usnadní vzájemné uznávání pokročilého testování u významných finančních subjektů.

---

[32] Doporučení Komise ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

[33] Referenční taxonomie pro klasifikaci incidentů ENISA, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

(25) Závislost finančních subjektů na službách IKT je zčásti vyvolána jejich potřebou přizpůsobit se rozvíjející se konkurenční digitální globální ekonomice, zvýšit efektivitu svých činností a uspokojovat poptávku spotřebitelů. Povaha a rozsah této závislosti se v posledních letech nepřetržitě vyvíjí, přičemž se tím snižují náklady finančního zprostředkování, umožňuje expanze podniků a škálovatelnost využívání finančních aktivit a současně se nabízí celá řada nástrojů IKT pro řízení složitých vnitřních procesů.

(26) Toto rozsáhlé využívání IKT dokládají složitá smluvní ujednání, přičemž se finanční subjekty často potýkají s potížemi při sjednávání smluvních podmínek přizpůsobených obezřetnostním normám nebo jiným regulatorním požadavkům, jež se na ně vztahují, nebo jinak při prosazování konkrétních práv, jako jsou práva na přístup nebo práva týkající se auditů, která jsou do těchto ujednání začleněna. Kromě toho mnoho těchto smluv neobsahuje dostatečné pojistky umožňující plnohodnotné sledování subdodavatelských procesů, což snižuje schopnost finančního subjektu posoudit související rizika. Dále protože poskytovatelé služeb IKT z řad třetích stran často nabízejí standardizované služby různým druhům klientů, nemusí takové smlouvy vždy přiměřeně ošetřovat individuální nebo konkrétní požadavky subjektů z finančního odvětví.

(27) Přes určitá obecná pravidla o subdodavatelích v některých právních předpisech Unie o finančních službách není sledování smluvního rozměru v legislativě Unie plně zakotveno. Vzhledem k absenci jasných a přesných unijních norem vztahujících se na smluvní ujednání uzavřená s poskytovateli služeb IKT z řad třetích stran není externí zdroj rizik v oblasti IKT vyřešen komplexně. Proto je nezbytné stanovit některé klíčové principy upravující řízení rizik v oblasti IKT spojených s třetími stranami u finančních subjektů, které budou doplněny souborem základních smluvních práv týkajících se několika prvků plnění a vypovídání smluv s cílem začlenit určité minimální pojistky podporující schopnost finančních subjektů účinně sledovat všechna rizika objevující se na úrovni třetích stran v oblasti IKT.

(28) U rizik v oblasti IKT spojených s třetími stranami a závislosti na poskytovatelích služeb IKT z řad třetích stran chybí dostatečná homogenita a konvergence. Přes určité úsilí o vyřešení specifické oblasti externí spolupráce, jako jsou doporučení z roku 2017 o spolupráci s externími poskytovateli cloudových služeb[34], se právní předpisy Unie jen velmi omezeně zabývají problémem systémového rizika, které může vzniknout při vystavení finančního sektoru omezenému počtu kritických poskytovatelů služeb IKT z řad třetích stran. Tento nedostatek na úrovni Unie je spojen s absencí konkrétních mandátů a nástrojů umožňujících vnitrostátním orgánům dohledu správně pochopit závislosti na třetích stranách v oblasti IKT a adekvátně sledovat rizika vyplývající z koncentrace těchto závislostí na třetích stranách v oblasti IKT.

(29) S přihlédnutím k potenciálním systémovým rizikům souvisejícím se zvýšeným externím poskytováním služeb a koncentrací závislosti na třetích stranách v oblasti IKT a s ohledem na nedostatečné vnitrostátní mechanismy umožňující orgánům finančního dohledu kvantifikovat, kvalifikovat a napravovat důsledky rizik v oblasti IKT, které se objevují u kritických poskytovatelů služeb IKT z řad třetích stran, je nezbytné vytvořit vhodný rámec dohledu Unie, který umožní nepřetržité sledování

[34] Doporučení pro spolupráci s externími poskytovateli cloudových služeb (EBA/REC/2017/03), nyní zrušeno Pokyny EBA pro externí služby (EBA/GL/2019/02).

činností poskytovatelů služeb IKT z řad třetích stran, kteří jsou kritickými dodavateli finančních subjektů.

(30) Jak se hrozby v oblasti IKT stávají složitějšími a sofistikovanějšími, závisí správná detekční a preventivní opatření ve značné míře na pravidelném sdílení operativních informací o hrozbách a zranitelnosti mezi finančními subjekty. Sdílení informací přispívá ke zvýšenému povědomí o kybernetických hrozbách, což zase zlepšuje schopnost finančních subjektů zabránit tomu, aby se z hrozeb staly skutečné incidenty, a umožňuje těmto subjektům lépe omezit dopady incidentů souvisejících s IKT a efektivněji se zotavit. Vzhledem k absenci pokynů na úrovni Unie se zdá, že tomuto sdílení operativních informací brání několik faktorů, zejména nejistota ohledně kompatibility v rámci předpisů pro ochranu osobních údajů, antimonopolních předpisů a předpisů upravujících odpovědnost.

(31) Kromě toho pochybnosti týkající se druhu informací, které je možné sdílet s ostatními účastníky trhu nebo jinými orgány nevykonávajícími dohled (například ENISA u analytických údajů nebo Europol pro účely prosazování práva), způsobují zadržování užitečných informací. Rozsah a kvalita sdílení informací zůstávají omezené, roztříštěné a příslušné výměny informací probíhají zejména na místní úrovni (prostřednictvím vnitrostátních iniciativ) a bez konzistentních celounijních dohod o sdílení informací přizpůsobených požadavkům integrovaného finančního sektoru.

(32) Finanční subjekty by proto měly být vybízeny, aby kolektivně využívaly svých individuálních znalostí a praktických zkušeností na strategické, taktické a provozní úrovni, a zlepšily tak své schopnosti adekvátního posuzování a sledování kybernetických hrozeb, obrany před nimi a reakce na ně. Je tedy nezbytné umožnit, aby na úrovni Unie vznikly mechanismy ujednání o dobrovolném sdílení informací, které při zavedení v důvěryhodných prostředích pomohou finančnímu společenství bránit se a společně reagovat na hrozby rychlým omezením šíření rizik souvisejících s IKT a zabráněním potenciálnímu šíření krize finančními kanály. Tyto mechanismy by měly být prováděny v úplném souladu s platnými právními předpisy Unie pro ochranu hospodářské soutěže[35] a rovněž způsobem zaručujícím úplné dodržování předpisů Unie pro ochranu osobních údajů, zejména nařízení Evropského parlamentu a Rady (EU) 2016/679,[36] zejména v souvislosti se zpracováním osobních údajů nezbytným pro účely oprávněného zájmu správce údajů nebo třetího subjektu, jak je uvedeno v čl. 6 odst. 1 písm. f) uvedeného nařízení.

(33) Bez ohledu na širokou platnost uvedenou v tomto nařízení by mělo používání pravidel pro digitální provozní odolnost zohledňovat výrazné rozdíly ve velikosti, profilech činnosti nebo expozici digitálním rizikům jednotlivých finančních subjektů. Obecným principem při rozdělování zdrojů a prostředků na realizaci rámce řízení rizik souvisejících s IKT by mělo být, že finanční subjekty správně vyváží své požadavky na IKT podle své velikosti a profilu činnosti, zatímco příslušné orgány budou nadále hodnotit a revidovat způsob tohoto rozdělování.

(34) Protože mohou větší finanční subjekty využívat více prostředků a dokážou rychle přidělovat finance na rozvoj řídicích struktur a vytvářet různé podnikové strategie,

---

35 Sdělení Komise – Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci, 2011/C 11/01.

36 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

měly by mít povinnost zřizovat komplexnější systémy správy a řízení pouze ty finanční subjekty, které nejsou ve smyslu tohoto nařízení považovány za mikropodniky. Tyto subjekty jsou lépe vybaveny pro vytváření specializovaných vedoucích funkcí pro dohled nad dohodami s poskytovateli služeb IKT z řad třetích stran nebo pro zvládání krizového řízení, k organizaci svého řízení rizik souvisejících s IKT podle tří linií modelu obrany nebo ke schválení personálního dokumentu komplexně vysvětlujícího zásady přístupových oprávnění.

Proto by mělo být pouze po těchto finančních subjektech požadováno, aby prováděly hloubková posouzení po velkých změnách infrastruktur sítí a informačních systémů a procesů, aby pravidelně analyzovaly rizika stávajících IKT systémů nebo aby rozšiřovaly testování zachování provozu a plánů na reakci a obnovu provozu, které zachytí scénáře přepínání mezi primární infrastrukturou IKT a redundantními zařízeními.

(35) Protože bude navíc požadováno provádění penetračních testů na základě hrozeb pouze u finančních subjektů označených za významné pro účely pokročilého testování digitální odolnosti, měly by se administrativní procesy a finanční náklady související s těmito testy týkat malého procenta finančních subjektů. Konečně s ohledem na snižování regulatorního zatížení by mělo být pravidelné hlášení všech nákladů a ztrát způsobených narušením IKT a hlášení výsledků přezkumů po incidentech závažného narušení IKT požadováno pouze po jiných finančních subjektech, než jsou mikropodniky.

(36) Aby byla zajištěna úplná harmonizace a celková konzistentnost obchodních strategií finančních subjektů na jedné straně a provádění řízení rizik v oblasti IKT na straně druhé, je třeba po vedoucím orgánu požadovat, aby si zachovával klíčovou a aktivní úlohu při řízení a přizpůsobování rámce řízení rizik v oblasti IKT a celkové strategie digitální odolnosti. Přístup vedoucího orgánu by se neměl zaměřovat pouze na prostředky k zajištění odolnosti systémů IKT, ale měl by zahrnovat rovněž osoby a procesy prostřednictvím strategií, které na každé úrovni společnosti a pro všechny pracovníky kultivují silné povědomí o kybernetických rizicích a závazek k dodržování striktní kybernetické hygieny na všech úrovních.

Nejvýznamnějším úkolem vedoucího orgánu při řízení rizik finančního subjektu v oblasti IKT by měl být zastřešující princip tohoto komplexního přístupu dále vyjádřeného prostřednictvím nepřetržitého angažování vedoucího orgánu při kontrole sledování řízení rizik v oblasti IKT.

(37) Dále jde plná odpovědnost vedoucího orgánu ruku v ruce se zabezpečením úrovně investic do IKT a celkového rozpočtu finančního subjektu, aby dokázal dosáhnout své základní linie digitální provozní odolnosti.

(38) Toto nařízení, které je inspirováno příslušnými mezinárodními, vnitrostátními a odvětvovými normami, pokyny, doporučeními nebo přístupy pro řízení kybernetických rizik[37], podporuje soubor funkcí usnadňujících celkovou strukturalizaci řízení rizik v oblasti IKT. Budou-li hlavní prostředky, kterými disponují

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7 *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Rámec kybernetické bezpečnosti NIST, https://www.nist.gov/cyberframework; FSB *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

finanční subjekty, odpovídat cílům těchto funkcí (identifikace, ochrana a prevence, odhalování, reakce a obnova provozu, poučení a vývoj a komunikace), které jsou uvedeny v tomto nařízení, mohou finanční subjekty nadále používat modely řízení rizik v oblasti IKT s různými rámci nebo kategoriemi.

(39) Aby finanční subjekty udržely krok s rozvíjející se oblastí kybernetických hrozeb, měly by udržovat aktualizované systémy IKT, které budou spolehlivé a budou disponovat dostatečnou kapacitou nejen k zajištění zpracování údajů v rozsahu nezbytném k realizaci jejich služeb, ale rovněž k zajištění technologické odolnosti umožňující finančním subjektům adekvátně se vypořádat s dalšími požadavky na zpracování, které ztěžují podmínky na trhu nebo mohou vytvářet jiné nepříznivé stavy. Přestože toto nařízení neobsahuje žádnou standardizaci konkrétních systémů, nástrojů nebo technologií IKT, vychází z toho, že finanční subjekty budou vhodně využívat evropsky a mezinárodně uznávané technické normy (např. ISO) nebo odvětvové osvědčené postupy, bude-li takové využití zcela v souladu s konkrétními pokyny dohledu pro používání a začlenění mezinárodních norem.

(40) Účinné plány zachování provozu a plány obnovy jsou nutné k tomu, aby mohly finanční subjekty neprodleně a rychle řešit incidenty související s IKT, zejména kybernetické útoky, prostřednictvím omezení škod a upřednostnění obnovy činností a nápravných opatření. Přestože by však záložní systémy měly začít se zpracováním bez zbytečného prodlení, neměl by takový začátek nijak ohrožovat integritu a bezpečnost sítě a informačních systémů ani důvěrnost údajů.

(41) I když toto nařízení umožňuje, aby finanční subjekty pružně stanovily časové cíle obnovy, tedy aby stanovily tyto cíle s úplným zohledněním povahy a významu relevantní funkce a všech konkrétních požadavků podniku, mělo by být při stanovování těchto cílů rovněž požadováno vyhodnocení potenciálního celkového dopadu na tržní efektivitu.

(42) Vážné dopady kybernetických útoků se zesilují, když se objeví ve finančním sektoru, oblasti, kde mnohem více hrozí, že se stane cílem zločinců hledajících finanční zisky přímo u zdroje. Aby se zmírnila tato rizika a zabránilo ztrátě integrity systémů IKT či jejich nedostupnosti a prolomení důvěrných údajů nebo poškození fyzické infrastruktury IKT, je třeba výrazně zlepšit hlášení závažných incidentů souvisejících s IKT finančními subjekty.

Hlášení incidentů souvisejících s IKT by mělo být pro všechny finanční subjekty harmonizováno, a to tak, že budou požádány, aby podávaly hlášení pouze svým příslušným orgánům. Přestože by se povinnost uvedených hlášení měla vztahovat na všechny finanční subjekty, nebude platit pro všechny stejně, neboť příslušné mezní hodnoty významnosti a časové rámce je třeba nastavit tak, aby zachytily pouze závažné incidenty související s IKT. Přímá hlášení by umožnila finančnímu dohledu přístup k informacím o incidentech souvisejících s IKT. Finanční dohled by měl nicméně předávat tyto informace jiným než finančním veřejným orgánům (příslušné orgány NIS, vnitrostátní orgány ochrany osobních údajů a donucovací orgány pro incidenty protiprávní povahy). Informace o incidentech souvisejících s IKT by měly být sdělovány vzájemně: orgány finančního dohledu by měly finančnímu subjektu poskytovat všechny nezbytné zpětné vazby nebo pokyny a evropské orgány dohledu by měly sdílet anonymizované údaje o hrozbách a zranitelných místech týkající se dané události, aby pomohly širší společné obraně.

(43) Je třeba předpokládat další reflexi možné centralizace zpráv o incidentech souvisejících s IKT prostřednictvím jednotného centra EU, které bude buď přímo

přijímat taková hlášení a automaticky informovat příslušné vnitrostátní orgány, nebo bude soustřeďovat hlášení zasílaná příslušnými vnitrostátními orgány a plnit úlohu koordinátora. Evropské orgány dohledu by měly být požádány, aby společně s ECB a ENISA vypracovaly do určitého data společnou zprávu zabývající se proveditelností vytvoření tohoto jednotného centra EU.

(44) Aby finanční subjekty dosáhly silné digitální provozní odolnosti a fungovaly v souladu s mezinárodními normami (např. Základní prvky G7 pro penetrační testování na základě hrozeb), měly by pravidelně testovat své systémy a personál IKT na efektivitu jejich prostředků prevence, detekce, reakce a obnovy, aby byla zjištěna a odstraněna potenciální zranitelná místa IKT. V reakci na rozdíly napříč finančními pododvětvími a v jejich rámci, pokud jde o připravenost finančních subjektů v oblasti kybernetické bezpečnosti, by mělo testování zahrnovat širokou škálu nástrojů a opatření od posouzení základních požadavků (např. posouzení a zjišťování zranitelnosti, analýzy otevřených zdrojů, vyhodnocení síťového zabezpečení, analýzy nedostatků, přezkumy fyzické bezpečnosti, dotazníky a antivirová softwarová řešení, v případě proveditelnosti přezkumy zdrojových kódů, testy založené na scénářích, testování kompatibility, testování výkonu nebo testování mezi koncovými body) až po pokročilejší testování (např. penetrační testy na základě hrozeb pro finanční subjekty z perspektivy IKT dostatečně vyspělé na to, aby tyto testy dokázaly provádět). Testování digitální provozní odolnosti by tedy mělo být pro některé významné finanční subjekty náročnější (např. pro velké úvěrové instituce, burzy, centrální depozitáře cenných papírů, ústřední protistrany atd.). Současně by testování digitální provozní odolnosti mělo být vhodnější pro některá pododvětví hrající klíčovou systémovou roli (např. platby, bankovnictví, clearing a vypořádání) a méně vhodné pro jiná pododvětví (např. správci aktiv, ratingové agentury atd.). Přeshraniční finanční subjekty vykonávající své právo usazování nebo poskytování služeb v rámci Unie by měly ve svém domovském členském státě splňovat jednotný soubor požadavků na pokročilé testování (např. penetrační testy na základě hrozeb) a příslušné testování by mělo zahrnovat infrastruktury IKT ve všech jurisdikcích, kde přeshraniční skupina působí v rámci Unie, což přeshraničním skupinám umožní, aby náklady na testování vznikly pouze v jedné jurisdikci.

(45) Za účelem zajištění řádného sledování rizik v oblasti IKT spojených s třetími stranami je nutné stanovit soubor pravidel založených na zásadách jako vodítko pro finanční subjekty sledující rizika, která vznikají v souvislosti s funkcemi externě zajišťovanými poskytovateli služeb IKT z řad třetích stran a obecněji v souvislosti se závislostí na třetích stranách v oblasti IKT.

(46) Za dodržování povinností podle tohoto nařízení by měl vždy zůstat odpovědný finanční subjekt. Proporcionální sledování rizik vznikajících na úrovni poskytovatelů služeb IKT z řad třetích stran by mělo být organizováno s řádným přihlédnutím k rozsahu, složitosti a významu závislosti související s IKT, významu či důležitosti služeb, procesů nebo funkcí regulovaných smluvními ujednáními a nakonec na základě pečlivého posouzení všech potenciálních dopadů na kontinuitu a kvalitu finančních služeb na individuální úrovni a případně na úrovni skupiny.

(47) Toto sledování by se mělo řídit strategickým přístupem k rizikům v oblasti IKT spojeným s třetími stranami formalizovaným prostřednictvím specializované strategie přijaté vedoucím orgánem finančního subjektu, která bude založena na nepřetržité kontrole všech takových závislostí na třetích stranách v oblasti IKT. Aby se zvýšilo povědomí dohledu o závislosti na třetích stranách v oblasti IKT a s ohledem na další podporu rámce dohledu zřizovaného tímto nařízením, měly by orgány finančního

dohledu pravidelně dostávat zásadní informace z registrů a měly by mít možnost jednorázově žádat o výpisy z nich.

(48) Formální uzavření smluvních ujednání by mělo být založeno na předchozí důkladné předsmluvní analýze, zatímco k vypovídání smluv by mělo docházet na základě minimálního souboru skutečností dokládajících nedostatky vzniklé u poskytovatele služeb IKT z řad třetích stran.

(49) Za účelem řešení systémového dopadu rizika koncentrace třetích stran v oblasti IKT by mělo být podporováno vyvážené řešení prostřednictvím pružného a postupného přístupu, protože pevné mezní hodnoty nebo přísná omezení mohou omezovat podnikání a smluvní svobodu. Finanční subjekty by měly důkladně vyhodnocovat svá smluvní ujednání, aby identifikovaly pravděpodobnost vzniku tohoto rizika, včetně využití hloubkových analýz smluv s externími poskytovateli, zejména budou-li uzavírány s poskytovateli služeb IKT z řad třetích stran usazenými ve třetí zemi. V této fázi a s ohledem na dosažení spravedlivé rovnováhy mezi nutným zachováním smluvní svobody a nutným zajištěním finanční stability není považováno za vhodné stanovit pro expozici třetím stranám v oblasti IKT striktní mezní hodnoty a omezení. Evropský orgán dohledu pověřený dohledem nad jednotlivými kritickými poskytovateli služeb IKT z řad třetích stran („hlavní orgán dohledu“), by měl vykonávat své dohledové úkoly se zvláštní pozorností věnovanou úplnému pochopení rozsahu vzájemných závislostí a objevení konkrétních míst, kde je pravděpodobné, že vysoká koncentrace kritických poskytovatelů služeb IKT z řad třetích stran v Unii může ohrozit stabilitu a integritu jejího finančního systému, a místo toho by měl v případech, kdy bude toto riziko zjištěno, nabídnout dialog s kritickými poskytovateli služeb IKT z řad třetích stran[38].

(50) Aby bylo možné pravidelně vyhodnocovat a sledovat schopnost poskytovatele služeb IKT z řad třetích stran bezpečně poskytovat služby finančnímu subjektu bez nepříznivých dopadů na jeho odolnost, měly by být klíčové smluvní prvky harmonizovány v celém plnění smluv s poskytovateli služeb IKT z řad třetích stran. Tyto prvky by se měly týkat minimálních smluvních aspektů považovaných za zásadní pro umožnění úplného sledování finančním subjektem z hlediska zajištění jeho digitální odolnosti založené na stabilitě a bezpečnosti služeb IKT.

(51) Smluvní ujednání by měla zejména obsahovat specifikace úplných popisů funkcí a služeb, míst, kde jsou dotčené funkce poskytovány a údaje zpracovávány, a rovněž popisy úrovní úplné služby doplněné kvantitativními i kvalitativními výkonnostními cíli v rámci sjednaných úrovní služeb, aby mohl finanční subjekt provádět efektivní sledování. Současně je třeba, aby byla za zásadní prvky schopnosti finančního subjektu zajistit sledování rizik spojených s třetími stranami považována ustanovení o přístupnosti, dostupnosti, integritě, bezpečnosti a ochraně osobních údajů, jakož i záruky přístupu, obnovy a návratu v případě insolvence, řešení krize nebo ukončení obchodní činnosti poskytovatele služeb IKT z řad třetích stran.

(52) Aby bylo zajištěno, že si finanční subjekty zachovají úplnou kontrolu nad veškerým vývojem, který může narušit jejich bezpečnost v oblasti IKT, měly by být lhůty pro oznámení a povinnosti hlášení poskytovatelů služeb IKT z řad třetích stran v případě vývoje s potenciálním vážným dopadem na schopnost poskytovatelů služeb IKT z řad

[38] Dále, vznikne-li riziko zneužití poskytovatelem služeb IKT z řad třetích stran považovaným za dominantního, měly by mít finanční subjekty rovněž možnost předložit Evropské komisi nebo vnitrostátním úřadům pro ochranu hospodářské soutěže formální či neformální stížnost.

třetích stran zajišťovat zásadní nebo důležité funkce, včetně poskytování pomoci touto stranou v případě incidentu souvisejícího s IKT zdarma nebo za předem stanovenou cenu.

(53) Práva na přístup, kontrolu a audit finančním subjektem nebo určenou třetí stranou jsou společně s úplnou spoluprací poskytovatele služeb IKT z řad třetích stran klíčovými nástroji průběžného sledování plnění těchto poskytovatelů služeb. Podobně by měl příslušný orgán finančního subjektu disponovat týmiž právy provést po předchozím oznámení kontrolu a audit poskytovatele služeb IKT z řad třetích stran při zachování mlčenlivosti.

(54) Smluvní ujednání by měla stanovit jasná práva týkající se vypovězení smlouvy a souvisejících minimálních výpovědních lhůt a rovněž specializované strategie ukončení smluvního vztahu umožňující zejména povinná přechodná období, během nichž by měli poskytovatelé služeb IKT z řad třetích stran nadále plnit příslušné funkce s cílem snížit riziko narušení na úrovni finančního subjektu nebo mu podle složitosti poskytované služby umožnit přechod k jinému poskytovateli služeb IKT z řad třetích stran, případně začít využívat vlastní řešení.

(55) Kromě toho může dobrovolné použití standardních smluvních doložek vypracovaných Komisí pro cloudové výpočetní služby dále zjednodušit situaci finančních subjektů a jejich poskytovatelů služeb IKT z řad třetích stran, protože se zvýší úroveň právní jistoty ohledně využívání cloudových výpočetních služeb finančním sektorem v úplném souladu s požadavky a předpoklady stanovenými v nařízení o finančních službách. Tato práce vychází z opatření již předjímaných v akčním plánu pro finanční technologie z roku 2018, kde byl oznámen záměr Komise podporovat a usnadňovat vypracovávání standardních smluvních doložek pro používání externích cloudových služeb finančními subjekty, přičemž čerpá z práce meziodvětvových zúčastněných subjektů cloudových služeb, kterou Komise umožnila za přispění finančního sektoru.

(56) S cílem podpořit konvergenci a účinnost v souvislosti s přístupy k dohledu nad riziky pro finanční sektor v oblasti IKT spojenými s třetími stranami, posílit digitální provozní odolnosti finančních subjektů spoléhajících se při plnění provozních funkcí na kritické poskytovatele služeb IKT z řad třetích stran, a pomoci tak zachovat stabilitu finančního systému Unie a integritu jednotného trhu s finančními službami by se na kritické poskytovatele služeb IKT z řad třetích stran měl vztahovat unijní rámec dohledu.

(57) Protože zvláštní zacházení je odůvodněné pouze u kritických poskytovatelů služeb z řad třetích stran, je nutné pro účely uplatňování unijního rámce dohledu vytvořit mechanismus klasifikace, který zohlední rozsah a povahu závislosti finančního sektoru na těchto poskytovatelích služeb IKT z řad třetích stran, což se promítne do souboru kvantitativních a kvalitativních kritérií stanovujících parametry kritičnosti, na jejichž základě se bude na poskytovatele vztahovat dohled. Kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří nebudou automaticky určeni na základě použití výše uvedených kritérií, by měli mít možnost dobrovolného vstupu do rámce dohledu, zatímco poskytovatelé služeb IKT z řad třetích stran, na něž se již vztahují rámce mechanismů dohledu na úrovni Eurosystému s cílem podpořit úkoly uvedené v čl. 127 odst. 2 Smlouvy o fungování Evropské unie, by měli být následně vyňati.

(58) Požadavek, aby byli poskytovatelé služeb IKT z řad třetích stran, kteří byli označeni za kritické, usazeni v Unii, se nevztahuje na lokalizaci údajů, protože toto nařízení nezahrnuje žádný další požadavek, aby ukládání nebo zpracování dat probíhalo v Unii.

(59) Tento rámec se netýká pravomoci členských států provádět vlastní úkoly dohledu nad poskytovateli služeb IKT z řad třetích stran, kteří se podle tohoto nařízení neřadí mezi kritické, ovšem mohou být považováni za významné na vnitrostátní úrovni.

(60) Aby se využilo současné vícevrstvé institucionální architektury v oblasti finančních služeb, měl by společný výbor evropských orgánů dohledu nadále zajišťovat v souladu se svými úkoly v oblasti kybernetické bezpečnosti meziodvětvovou koordinaci ohledně všech záležitostí týkajících se rizik v oblasti IKT, přičemž mu bude pomáhat nový podvýbor (Fórum dohledu) provádějící přípravné práce jak pro individuální rozhodnutí určená kritickým poskytovatelům služeb IKT z řad třetích stran, tak pro kolektivní doporučení, zejména ohledně porovnávání testování programů dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran, a současně identifikovat osvědčené postupy pro řešení otázek rizika koncentrace IKT.

(61) Aby se zajistilo, že bude na poskytovatele služeb IKT z řad třetích stran hrající kritickou úlohu při fungování finančního sektoru na úrovni Unie dohlíženo srovnatelně, měl by být jeden evropský orgán dohledu určen pro každého poskytovatele služeb IKT z řad třetích stran jako hlavní orgán dohledu.

(62) Hlavním orgánům by měly být přiznány nezbytné pravomoci k provádění šetření, kontrol u kritických poskytovatelů služeb IKT z řad třetích stran na místě i dálkově, k přístupu do všech příslušných areálů a na všechna příslušná místa a k získávání úplných a aktualizovaných informací, jež jim umožní reálně pochopit druh, rozměr i dopad rizik v oblasti IKT spojených s třetími stranami pro finanční subjekty a konečně i pro finanční systém Unie.

Pověření evropských orgánů dohledu hlavním dohledem je nutným předpokladem k pochopení a řešení systémového rozměru rizik v oblasti IKT ve finančním sektoru. Stopa kritických poskytovatelů služeb IKT z řad třetích stran v Unii a s nimi související riziko koncentrace IKT si žádají přijetí kolektivního přístupu realizovaného na úrovni Unie. Výkon práv na provádění auditů a přístup ze strany početných příslušných orgánů samostatně nebo nekoordinovaně by nevedl k úplnému přehledu o rizicích oblasti IKT spojených s třetími stranami a současně by vytvářel zbytečnou redundantnost, zatížení a složitost pro kritické poskytovatele služeb IKT z řad třetích stran, na které by se tyto různé požadavky vztahovaly.

(63) Kromě toho by hlavní orgány dohledu měly mít možnost předkládat doporučení ohledně rizik v oblasti IKT a vhodných nápravných prostředků, včetně oponování některým smluvním ujednáním, které v posledku dopadají na stabilitu finančního subjektu či finančního systému. Vnitrostátní příslušné orgány by měly v rámci své funkce související s obezřetnostním dohledem nad finančními subjekty řádně přihlížet k dodržování shody s těmito základními doporučeními stanovenými hlavními orgány dohledu.

(64) Rámec dohledu nenahrazuje ani žádným způsobem či podílem nezastupuje řízení rizik spojených s poskytovateli služeb IKT z řad třetích stran, které musí zajišťovat finanční subjekty, včetně povinnosti průběžného sledování smluvních ujednání uzavřených s kritickými poskytovateli služeb IKT z řad třetích stran, a neovlivňuje úplnou odpovědnost finančních subjektů za provedení a splnění všech požadavků tohoto nařízení a příslušných právních předpisů o finančních službách. Aby se předešlo zdvojením a přesahům, neměly by příslušné orgány samostatně přijímat žádná opatření zaměřená na sledování rizik poskytovatelů služeb ICT z řad třetích stran. Všechna tato opatření je třeba předem koordinovat a schválit v souvislosti s rámcem dohledu.

(65) Za účelem podpory mezinárodního sbližování osvědčených postupů, které budou používány při přezkumu řízení digitálních rizik prováděného poskytovateli služeb IKT z řad třetích stran, by měly být evropské orgány dohledu vyzývány k tomu, aby s příslušnými orgány dohledu a regulatorními orgány třetích zemí uzavíraly smlouvy o spolupráci, které usnadní vypracování osvědčených postupů pro řešení rizik v oblasti IKT spojených s třetími stranami.

(66) Aby se využilo technických odborných znalostí odborníků na řízení provozních rizik a rizik v oblasti IKT z příslušných orgánů, měly by hlavní orgány dohledu čerpat z vnitrostátních dohledových zkušeností a vytvořit specializované týmy prošetřující jednotlivé kritické poskytovatele služeb IKT z řad třetích stran, jejichž seskupením vzniknou meziodvětvové týmy za účelem podpory příprav i skutečného provádění dohledových činností, včetně kontrol kritických poskytovatelů služeb IKT z řad třetích stran na místě, jakož i nezbytných následných opatření.

(67) Příslušné orgány by měly disponovat všemi kontrolními, vyšetřovacími a sankčními pravomocemi nezbytnými k zajištění uplatňování tohoto nařízení. Správní sankce by v zásadě měly být zveřejňovány. Finanční subjekty a poskytovatelé služeb IKT z řad třetích stran mohou být usazeni v různých členských státech a podléhat dohledu různých odvětvových příslušných orgánů, a proto by měla být zajištěna úzká spolupráce mezi relevantními příslušnými orgány, včetně ECB, pokud jde o zvláštní úkoly, které jí svěřuje nařízení Rady (EU) č. 1024/2013[39], a konzultace s evropskými orgány dohledu prostřednictvím vzájemné výměny informací a poskytování pomoci v souvislosti s činnostmi dohledu.

(68) Aby bylo možné dále kvantifikovat a kvalifikovat kritéria pro označení poskytovatelů služeb IKT z řad třetích stran a harmonizovat poplatky související s dohledem, měla by být pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování Evropské unie přenesena na Komisi, a to s ohledem na: další specifikování systémového dopadu, kterou by mělo selhání poskytovatele služeb IKT z řad třetích stran na finanční subjekty, pro které pracuje, počet globálních systémových významných institucí (G-SVI) nebo jiných systémových významných institucí (O-SVI), jež využívají daného poskytovatele služeb IKT z řad třetích stran, počet poskytovatelů služeb IKT z řad třetích stran působících na konkrétním trhu, náklady na přechod k jinému poskytovateli služeb IKT z řad třetích stran, počet členských států, kde daná třetí strana poskytuje služby IKT a kde působí funkční subjekty využívající daného poskytovatele služeb IKT z řad třetích stran a rovněž na výši poplatků souvisejících s dohledem a způsob jejich platby.

Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů[40]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

---

39 Nařízení Rady (EU) č. 1024/2013 ze dne 15. října 2013, kterým se Evropské centrální bance svěřují zvláštní úkoly týkající se politik, které se vztahují k obezřetnostnímu dohledu nad úvěrovými institucemi (Úř. věst. L 287, 29.10.2013, s. 63).

40 Úř. věst. L 123, 12.5.2016, s. 1.

(69) Protože toto nařízení, společně se směrnicí Evropského parlamentu a Rady (EU) 20xx/xx,[41] obsahuje konsolidaci ustanovení o řízení rizik v oblasti IKT, jež tvoří několik nařízení a směrnic unijního práva o finančních službách, včetně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014, je třeba za účelem zajištění úplné konzistentnosti tato nařízení změnit tak, aby uváděla, že jsou příslušná ustanovení o rizicích souvisejících s IKT uvedena v tomto nařízení.

Konzistentní harmonizaci požadavků stanovených tímto nařízením by měly zajišťovat technické normy. Vzhledem k vysoce odborným znalostem, jimiž evropské orgány dohledu disponují, by měly být tyto orgány pověřeny vypracováním návrhů regulačních technických norem, které nezahrnují volby politiky, a jejich předložením Komisi. Regulační technické normy by měly být vypracovány v oblastech řízení rizik v oblasti IKT, hlášení, testování a klíčových požadavků na řádné sledování rizik v oblasti IKT spojených s třetími stranami.

(70) Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni. Komise a evropské orgány dohledu by měly zajistit, aby tyto normy a požadavky mohly všechny finanční subjekty uplatňovat způsobem, který je přiměřený povaze, rozsahu a složitosti těchto subjektů a jejich činností.

(71) Aby se usnadnila srovnatelnost zpráv o závažných incidentech souvisejících s IKT a zajistila transparentnost smluvních ujednání pro používání služeb IKT poskytovaných třetími stranami, měly by být evropským orgánům dohledu dány pravomoci vypracovat návrhy prováděcích technických norem stanovících standardizované vzory, formuláře a postupy, které budou finanční subjekty používat pro hlášení závažných incidentů souvisejících s IKT, a rovněž vzory pro registr informací. Při vypracovávání těchto norem by měly evropské orgány dohledu zohlednit velikost a složitost finančních subjektů, jakož i povahu a úroveň rizika jejich činností. Komisi by měla být svěřena pravomoc přijímat tyto prováděcí technické normy postupem podle článku 291 SFEU a článku 15 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010. Protože již byly další požadavky specifikovány akty v přenesené pravomoci a prováděcími akty vycházejícími z technických regulačních a prováděcích technických norem v nařízeních (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a případně (EU) č. 909/2014, je vhodné pověřit evropské orgány dohledu, buď samostatně, nebo společně prostřednictvím společného výboru, předložením regulačních a prováděcích technických norem Komisi za účelem přijetí aktů v přenesené pravomoci a prováděcích aktů, jež provádějí a aktualizují stávající pravidla pro řízení rizik v oblasti IKT.

(72) Tato činnost bude zahrnovat následnou změnu stávajících aktů v přenesené pravomoci a prováděcích aktů přijatých v různých oblastech právních předpisů pro finanční služby. Je třeba upravit oblast působnosti článků o operačních rizicích, na jejichž základě zmocnění v těchto aktech nařídilo přijetí aktů v přenesené pravomoci a prováděcích aktů, tak aby byla do tohoto nařízení převzata všechna ustanovení týkající se digitální provozní odolnosti, jež jsou nyní součástí uvedených nařízení.

(73) Jelikož cíle tohoto nařízení, totiž dosažení digitální provozní odolnosti u všech finančních subjektů, nemůže být uspokojivě dosaženo na úrovni členských států, jelikož k tomu potřebují harmonizaci celé řady různých pravidel, která v současnosti existují v rámci některých aktů Unie, právních systémů jednotlivých členských států,

[41] [*vložte úplný odkaz*].

ale spíše jej z důvodu rozsahu a účinků této směrnice může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle.

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět

1. Toto nařízení stanoví jednotné požadavky týkající se bezpečnosti sítí a informačních systémů využívaných finančními subjekty při provozování jejich činnosti, nezbytné k dosažení vysoké obecné úrovně digitální provozní odolnosti, a to:

   (a) požadavky vztahující se na finanční subjekty týkající se:

   – řízení rizik v oblasti informačních a komunikačních technologií (IKT),

   – hlášení závažných incidentů souvisejících s IKT příslušným orgánům,

   – testování digitální provozní odolnosti,

   – sdílení operativních a jiných informací souvisejících s kybernetickými hrozbami a zranitelnými místy,

   – opatření pro řádné řízení rizik v oblasti IKT spojených s třetími stranami finančními subjekty;

   (b) požadavky týkající se smluvních ujednání uzavřených mezi poskytovateli služeb IKT z řad třetích stran a finančními subjekty;

   (c) rámec dohledu pro kritické poskytovatele služeb IKT z řad třetích stran při poskytování služeb finančním subjektům;

   (d) pravidla spolupráce mezi příslušnými orgány a pravidla pro dohled a vymáhání ze strany příslušných orgánů v souvislosti se všemi otázkami upravenými tímto nařízením.

2. Ve vztahu k finančním subjektům určeným jako provozovatelé základních služeb podle vnitrostátních právních předpisů provádějících článek 5 směrnice (EU) 2016/1148 se toto nařízení pro účely čl. 1 odst. 7 uvedené směrnice považuje za odvětvový právní akt Unie.

Článek 2

Osobní působnost

1. Toto nařízení se vztahuje na tyto subjekty:

   (a) úvěrové instituce;

   (b) platební instituce;

   (c) instituce elektronických peněz;

(d) investiční podniky;

(e) poskytovatele služeb souvisejících s kryptoaktivy, vydavatele kryptoaktiv, vydavatele tokenů vázaných na aktiva a vydavatele významných tokenů vázaných na aktiva;

(f) centrální depozitáře cenných papírů;

(g) ústřední protistrany;

(h) obchodní systémy;

(i) registry obchodních údajů;

(j) správce alternativních investičních fondů;

(k) správcovské společnosti;

(l) poskytovatele služeb hlášení údajů;

(m) pojišťovny a zajišťovny;

(n) zprostředkovatele pojištění, zprostředkovatele zajištění a zprostředkovatele doplňkového pojištění;

(o) instituce zaměstnaneckého penzijního pojištění;

(p) ratingové agentury;

(q) statutární auditory a auditorské společnosti;

(r) správce kritických referenčních hodnot;

(s) poskytovatele služeb skupinového financování;

(t) registry sekuritizací;

(u) poskytovatele služeb IKT z řad třetích stran.

2. Subjekty uvedené v písmenech a) až t) jsou pro účely tohoto nařízení souhrnně nazývány „finančními subjekty“.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

(1) „digitální provozní odolností“ schopnost finančního subjektu budovat, zajišťovat a revidovat svoji provozní integritu z technologického hlediska prostřednictvím zajištění, ať již přímo, či nepřímo s využitím služeb IKT poskytovaných třetími stranami, veškerých prostředků souvisejících s IKT nezbytných k řešení otázek bezpečnosti sítí a informačních systémů, které finanční subjekt používá a které přispívají k nepřetržitému poskytování finančních služeb a k jejich kvalitě;

(2) „sítí a informačním systémem“ síť a informační systém dle vymezení v čl. 4 bodě 1 směrnice (EU) 2016/1148;

(3) „bezpečností sítí a informačních systémů“ bezpečnost sítí a informačních systémů dle vymezení čl. 4 bodě 2 směrnice (EU) 2016/1148;

(4) „riziky v oblasti IKT“ veškeré rozumně rozpoznatelné skutečnosti související s používáním sítě a informačních systémů – včetně poruchy, překročení kapacity, selhání, narušení, poškození, zneužití, ztráty či jiného druhu úmyslných či

neúmyslných událostí – které mohou narušit bezpečnost sítě a informačních systémů, jakýchkoli na technologiích závislých nástrojů nebo procesů, provozu a fungování procesů nebo poskytování služeb, a tím narušit integritu nebo dostupnost dat, softwaru nebo jakéhokoli jiného prvku služeb a infrastruktur IKT nebo způsobit porušení důvěrnosti, poškození fyzické infrastruktury IKT či mít jiné škodlivé dopady;

(5) „informačními aktivy“ soubor informací, v hmotné i nehmotné formě, které je potřeba chránit;

(6) „incidentem souvisejícím s IKT“ nepředvídaná zjištěná událost v síti a informačních systémech způsobená úmyslnou činností či nikoli, která ohrožuje bezpečnost sítí a informačních systémů, informací zpracovávaných, uchovávaných nebo přenášených těmito systémy nebo která nepříznivě dopadá na dostupnost, důvěrnost, kontinuitu či autenticitu finančních služeb poskytovaných finančním subjektem;

(7) „závažným incidentem souvisejícím s IKT“ incident související s IKT s potenciálně rozsáhlými nepříznivými dopady na síť a informační systémy využívané k zajištění zásadních funkcí finančního subjektu;

(8) „kybernetickou hrozbou“ kybernetická hrozba dle vymezení v čl. 2 bodě 8 nařízení Evropského parlamentu a Rady (EU) 2019/881[42];

(9) „kybernetickým útokem“ zlovolný incident související s IKT s cílem zničit, odhalit, pozměnit, deaktivovat či odcizit aktivum nebo k němu získat neoprávněný přístup či ho neoprávněně využívat spáchaný jakýmkoliv aktérem hrozby;

(10) „operativními informacemi o hrozbách“ informace, které byly shromážděny, zpracovány, analyzovány interpretovány nebo rozšířeny tak, aby poskytovaly nezbytné souvislosti pro rozhodování, a které přinášejí relevantní a dostatečné poznatky ke zmírnění dopadu incidentu souvisejícího s IKT nebo kybernetické hrozby, včetně technických údajů o kybernetickém útoku, osobách odpovědných za útok a jejich *modu operandi* a motivaci;

(11) „ochranou do hloubky“ strategie v oblasti IKT, zahrnující osoby, procesy a technologie, pro vytvoření škály bariér napříč různými vrstvami a dimenzemi subjektu;

(12) „zranitelností“ slabina, citlivost nebo chyba aktiva, systému, procesu nebo kontroly, jichž může využít případná hrozba;

(13) „penetračním testováním na základě hrozeb“ rámec napodobující taktiku, techniky a postupy skutečných aktérů hrozeb vnímaných jako skutečná kybernetická hrozba, který poskytuje řízené, individualizované a na operativních informacích založené (metoda „červeného týmu“) testování kritických systémů subjektu za provozu;

(14) „riziky v oblasti IKT spojenými s třetí stranou“ rizika pro finanční subjekt v oblasti IKT, která mohou vzniknout v souvislosti s jeho využíváním služeb IKT poskytovaných třetími stranami nebo jejich dalšími subdodavateli;

[42] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

(15) „poskytovatelem služeb IKT z řad třetích stran“, „poskytovatelem služeb IKT, který je třetí stranou“ nebo „třetí stranou poskytující služby IKT“ podnik poskytující digitální a datové služby, včetně poskytovatelů cloudových služeb, softwaru, služeb analýzy dat, datových center, avšak s výjimkou poskytovatelů hardwarových komponentů a podniků oprávněných podle práva Unie, jež zajišťují služby elektronických komunikací dle vymezení v čl. 2 bodě 4 směrnice Evropského parlamentu a Rady (EU) 2018/1972[43];

(16) „službami IKT“ digitální a datové služby poskytované prostřednictvím systémů IKT jednomu či více interním nebo externím uživatelům, včetně poskytování dat, služeb vkládání dat, uchovávání dat, zpracování a hlášení dat, sledování dat a rovněž na datech založených služeb na podporu činnosti a rozhodování;

(17) „zásadní nebo důležitou funkcí“ funkce, jejíž přerušení či chybný nebo neúspěšný průběh by významně narušily dodržování podmínek a povinností finančního subjektu vyplývajících z jeho povolení nebo jeho dalších povinností na základě příslušných právních předpisů o finančních službách nebo jeho finanční výkonnost či řádný průběh nebo kontinuitu jeho služeb a činností;

(18) „kritickým poskytovatelem služeb IKT z řad třetích stran“ poskytovatel služeb IKT z řad třetích stran určený v souladu s článkem 29 a podléhající rámci dohledu uvedenému v článcích 30 až 37;

(19) „poskytovatelem služeb IKT z řad třetích stran usazeným ve třetí zemi“ poskytovatel služeb IKT z řad třetích stran, který je právnickou osobou usazenou ve třetí zemi, nepodniká/nenachází se v Unii a uzavřel smluvní ujednání s finančním subjektem na poskytování služeb IKT;

(20) „subdodavatelem IKT usazeným ve třetí zemi“ subdodavatel IKT, který je právnickou osobou usazenou ve třetí zemi, nepodniká/nenachází se v Unii a uzavřel smluvní ujednání buď s poskytovatelem služeb IKT z řad třetích stran, nebo s poskytovatelem služeb IKT z řad třetích stran usazeným ve třetí zemi;

(21) „rizikem koncentrace IKT“ expozice jednotlivým či více spřízněným poskytovatelům služeb IKT z řad třetích stran vytvářející takovou míru závislosti na těchto poskytovatelích, že jejich nedostupnost, selhání nebo jiná nedostatečnost mohou potenciálně ohrozit schopnost finančního subjektu, a v konečném důsledku i celého finančního systému Unie poskytovat zásadní funkce nebo způsobit, že utrpí jinou újmu, včetně vysokých ztrát;

(22) „vedoucím orgánem“ vedoucí orgán dle vymezení v čl. 4 odst. 1 bodě 36 směrnice 2014/65/EU, čl. 3 odst. 1 bodě 7 směrnice 2013/36/EU, čl. 2 odst. 1 písm. s) směrnice 2009/65/ES, čl. 2 odst. 1 bodě 45 nařízení (EU) č. 909/2014, čl. 3 odst. 1 bodě 20 nařízení Evropského parlamentu a Rady (EU) 2016/1011[44], čl. 3 odst. 1 písm. u) nařízení Evropského parlamentu a Rady (EU) 20xx/xx[45] [MICA] nebo

---

[43] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (přepracované znění), (Úř. věst. L 321, 17.12.2018, s. 36).

[44] Nařízení Evropského parlamentu a Rady (EU) 2016/1011 ze dne 8. června 2016 o indexech, které jsou používány jako referenční hodnoty ve finančních nástrojích a finančních smlouvách nebo k měření výkonnosti investičních fondů, a o změně směrnic 2008/48/ES a 2014/17/EU a nařízení (EU) č. 596/2014 (Úř. věst. L 171, 29.6.2016, s. 1).

[45] [*Prosím vložte celý název a informace o Úř. věst.*]

rovnocenné osoby, které skutečně řídí subjekt nebo zastávají klíčové funkce podle příslušných unijních nebo vnitrostátních právních předpisů;

(23) „úvěrovou institucí“ úvěrová instituce dle vymezení v čl. 4 odst. 1 bodě 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013[46];

(24) „investičním podnikem“ investiční podnik dle vymezení v čl. 4 odst. 1 bodě 1 směrnice 2014/65/EU;

(25) „platební institucí“ platební instituce ve smyslu čl. 1 odst. 1 písm. d) směrnice (EU) 2015/2366;

(26) „institucí elektronických peněz“ instituce elektronických peněz dle vymezení v čl. 2 bodě 1 směrnice Evropského parlamentu a Rady 2009/110/ES[47];

(27) „ústřední protistranou“ ústřední protistrana dle vymezení v čl. 2 bodě 1 nařízení (EU) č. 648/2012;

(28) „registrem obchodních údajů“ registr obchodních údajů dle vymezení v čl. 2 bodě 2 nařízení (EU) č. 648/2012;

(29) „centrálním depozitářem cenných papírů“ centrální depozitář cenných papírů dle vymezení v čl. 2 odst. 1 bodě 1 nařízení č. 909/2014;

(30) „obchodním systémem“ obchodní systém dle vymezení v čl. 4 odst. 1 bodě 24 směrnice 2014/65/EU;

(31) „správcem alternativních investičních fondů“ správce alternativních investičních fondů dle vymezení v čl. 4 odst. 1 písm. b) směrnice 2011/61/EU;

(32) „správcovskou společností“ správcovská společnost dle vymezení v čl. 2 odst. 1 písm. b) směrnice 2009/65/ES;

(33) „poskytovatelem služeb hlášení údajů“ poskytovatel služeb hlášení údajů dle vymezení v čl. 4 odst. 1 bodě 63 směrnice 2014/65/ES;

(34) „pojišťovnou“ pojišťovna dle vymezení v čl. 13 bodě 1 směrnice 2009/138/ES;

(35) „zajišťovnou“ zajišťovna dle vymezení v čl. 13 bodě 4 směrnice 2009/138/ES;

(36) „zprostředkovatelem pojištění“ zprostředkovatel pojištění dle vymezení v čl. 2 bodě 3 směrnice (EU) 2016/97;

(37) „zprostředkovatelem doplňkového pojištění“ zprostředkovatel pojištění dle vymezení v čl. 2 bodě 4 směrnice (EU) 2016/97;

(38) „zprostředkovatelem zajištění“ zprostředkovatel zajištění dle vymezení v čl. 2 bodě 5 směrnice (EU) 2016/97;

(39) „institucí zaměstnaneckého penzijního pojištění“ instituce zaměstnaneckého penzijního pojištění dle vymezení v čl. 1 bodě 6 směrnice 2016/2341;

(40) „ratingovou agenturou“ ratingová agentura dle vymezení v čl. 3 odst. 1 písm. a) nařízení (ES) č. 1060/2009;

---

[46] Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

[47] Směrnice Evropského parlamentu a Rady 2009/110/ES ze dne 16. září 2009 o přístupu k činnosti institucí elektronických peněz, o jejím výkonu a o obezřetnostním dohledu nad touto činností, o změně směrnic 2005/60/ES a 2006/48/ES a o zrušení směrnice 2000/46/ES (Úř. věst. L 267, 10.10.2009, s. 7).

(41) „statutárním auditorem“ statutární auditor dle vymezení v čl. 2 bodě 2 směrnice 2006/43/ES;

(42) „auditorskou společností“ auditorská společnost dle vymezení v čl. 2 bodě 3 směrnice 2006/43/ES;

(43) „poskytovatelem služeb souvisejících s kryptoaktivy“ poskytovatel služeb souvisejících s kryptoaktivy dle vymezení v čl. 3 odst. 1 písm. n) nařízení (EU) 202x/xx [*OP: vložte odkaz na nařízení MICA*];

(44) „vydavatelem kryptoaktiv“ vydavatel kryptoaktiv dle vymezení v čl. 3 odst. 1 písm. h) [*Úř. věst: vložte odkaz na nařízení MICA*];

(45) „vydavatelem tokenů vázaných na aktiva“ vydavatel tokenů vázaných na aktiva dle vymezení v čl. 3 odst. 1 písm. i) [*Úř. věst: vložte odkaz na nařízení MICA*];

(46) „vydavatelem významných tokenů vázaných na aktiva“ vydavatel významných tokenů vázaných na aktiva dle vymezení v čl. 3 odst. 1 písm. j) [*Úř. věst: vložte odkaz na nařízení MICA*];

(47) „správcem kritických referenčních hodnot“ správce kritických referenčních hodnot dle vymezení v čl. x bodě x nařízení xx/202x [*Úř. věst: vložte odkaz na nařízení o referenčních hodnotách*];

(48) „poskytovatelem služeb skupinového financování“ poskytovatel služeb skupinového financování dle vymezení v čl. x bodě x nařízení (EU) 202x/xx [*OP: vložte odkaz na nařízení o skupinovém financování*];

(49) „registrem sekuritizací“ registr sekuritizací dle vymezení v čl. 2 bodě 23 nařízení (EU) 2017/2402;

(50) „mikropodnikem“ mikropodnik dle vymezení v čl. 2 odst. 3 přílohy doporučení 2003/361/ES.

KAPITOLA II

ŘÍZENÍ RIZIK V OBLASTI IKT

ODDÍL I

Článek 4

Řízení a organizace

1. Finanční subjekty disponují interními řídicími a kontrolními rámci, které zajistí účinné a obezřetné řízení všech rizik v oblasti IKT.

2. Vedoucí orgán finančního subjektu stanoví a schvaluje veškerá opatření související s rámcem řízení rizik v oblasti IKT zmíněným v čl. 5 odst. 1, dohlíží na jejich provádění a odpovídá za něj.

   Pro účely prvního pododstavce vedoucí orgán:

   (a) nese konečnou odpovědnost za řízení rizik finančního subjektu v oblasti IKT;

   (b) stanoví jasné úlohy a odpovědnosti pro všechny funkce související s IKT;

(c) stanoví odpovídající míru tolerance pro rizika finančního subjektu v oblasti IKT, jak je uvedeno v čl. 5 odst. 9 písm. b);

(d) schvaluje strategii finančního subjektu pro zachování provozu IKT a jeho plán obnovy provozu po havárii IKT uvedené v čl. 10 odst. 1 a 3, dohlíží na jejich provádění a pravidelně toto provádění přezkoumává;

(e) schvaluje a pravidelně přezkoumává plány auditů IKT a audity IKT a jejich podstatné změny;

(f) přiděluje a pravidelně přezkoumává odpovídající rozpočtové prostředky na pokrytí potřeb finančního subjektu v oblasti digitální provozní odolnosti s ohledem na všechny typy zdrojů, včetně školení o rizicích v oblasti IKT a zajištění odpovídajících dovedností všech příslušných pracovníků;

(g) schvaluje a pravidelně přezkoumává strategii finančního subjektu pro režimy využívání služeb IKT poskytovaných třetími stranami;

(h) je řádně informován o ujednáních o využívání služeb IKT uzavřených s poskytovateli z řad třetích stran, o jakýchkoli příslušných plánovaných významných změnách týkajících se poskytovatelů služeb IKT z řad třetích stran a o možných dopadech těchto změn na zásadní nebo důležité funkce, jichž se týkají zmíněná ujednání, včetně toho, že obdrží souhrn analýzy rizik za účelem posouzení dopadů těchto změn;

(i) je řádně informován o incidentech souvisejících s IKT a jejich dopadech a opatřeních v rámci reakce, obnovy provozu a nápravy.

3. Finanční subjekty jiné než mikropodniky vytvoří funkci sledování ujednání o využívání služeb IKT uzavřených s poskytovateli z řad třetích stran, nebo pověří člena vyššího vedení jako osobu odpovědnou za dohled nad expozicí souvisejícím rizikům a příslušnou dokumentací.

4. Členové vedoucího orgánu pravidelně absolvují zvláštní školení, aby měli dostatečné a aktuální znalosti a dovednosti k pochopení a hodnocení rizik v oblasti IKT a jejich dopadů na fungování finančního subjektu.

ODDÍL II

Článek 5

Rámec pro řízení rizik v oblasti IKT

1. Finanční subjekty musí mít solidní, ucelený a dobře zdokumentovaný rámec pro řízení rizik v oblasti IKT, který jim umožní řešit tato rizika rychle, účinně a komplexně a zajistit vysokou míru digitální provozní odolnosti odpovídající potřebám jejich provozu, jejich velikosti a složitosti jejich struktury

2. Rámec pro řízení rizik v oblasti IKT podle odstavce 1 obsahuje strategie, politiky, postupy, protokoly a nástroje IKT, jež jsou nezbytné pro řádnou a účinnou ochranu všech příslušných fyzických komponentů a infrastruktur, včetně počítačového hardwaru, serverů a rovněž příslušných areálů, datových center a citlivých specializovaných prostor, aby byla zajištěna vhodná ochrana všech těchto fyzických prvků před riziky, včetně poškození a neoprávněného přístupu nebo použití.

3. Finanční subjekty minimalizují dopad rizik v oblasti IKT zavedením vhodných strategií, politik, postupů, protokolů a nástrojů podle rámce pro řízení rizik v oblasti

IKT. Poskytují úplné a aktualizované informace o rizicích v oblasti IKT podle požadavků příslušných orgánů.

4. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v odstavci 1 finanční subjekty jiné než mikropodniky zavedou systém řízení bezpečnosti informací, vycházející z uznávaných mezinárodních norem a odpovídající pokynům dohledu a pravidelně jej revidují.

5. Finanční subjekty jiné než mikropodniky zajistí náležité oddělení vedoucích funkcí, kontrolních funkcí a interních auditních funkcí v oblasti IKT podle modelu tří linií obrany nebo interního modelu řízení a kontroly rizik.

6. Rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 se zdokumentuje a reviduje alespoň jednou ročně a rovněž po výskytu závažného incidentu souvisejícího s IKT a na základě pokynů dohledu nebo závěrů vyvozených na základě příslušných testů či auditů digitální provozní odolnosti. Je průběžně zdokonalován na základě zkušeností z jeho provádění a monitorování.

7. Rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 podléhá pravidelnému auditu auditory IKT s dostatečnými znalostmi, dovednostmi a odbornými zkušenostmi v oblasti rizik IKT. Četnost a zaměření auditů IKT odpovídají rizikům finančního subjektu v oblasti IKT.

8. Zavede se formální následný postup zahrnující pravidla pro včasné ověření a nápravu kritických zjištění auditu IKT, s přihlédnutím k závěrům z auditního přezkumu a se současným náležitým zohledněním povahy, rozsahu a komplexnosti služeb a činností finančních subjektů.

9. Rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 zahrnuje strategii digitální odolnosti, v níž se stanoví způsob jeho uplatňování. Za tím účelem zahrnuje metody řešení rizik v oblasti IKT a plnění specifických cílů v oblasti IKT, a to formou:

   (a) vysvětlení, jak rámec pro řízení rizik v oblasti IKT podporuje obchodní strategii a cíle finančního subjektu;

   (b) stanovení úrovně tolerance rizik v oblasti IKT podle ochoty finančního subjektu podstupovat riziko a analýzy tolerance dopadů výpadků v oblasti IKT;

   (c) stanovení jasných cílů v oblasti bezpečnosti informací;

   (d) vysvětlení referenční architektury IKT a veškerých změn potřebných k dosažení specifických obchodních cílů;

   (e) uvedení různých mechanismů zavedených za účelem odhalování incidentů souvisejících s IKT, ochraně před nimi a prevenci jejich dopadů;

   (f) evidování počtu nahlášených závažných incidentů souvisejících s IKT a účinnosti preventivních opatření;

   (g) definování holistické strategie s více dodavateli v oblasti IKT na úrovni subjektu s uvedením klíčových závislostí na poskytovatelích služeb IKT z řad třetích stran a s vysvětlením důvodů využívání služeb příslušného souboru třetích stran;

   (h) zavedení testování digitální provozní odolnosti;

   (i) popisu komunikační strategie v případě incidentů souvisejících s IKT.

10. Finanční subjekty mohou po schválení příslušnými orgány delegovat úkoly ověřování shody s požadavky řízení rizik v oblasti IKT na podniky v rámci skupiny či externí podniky.

Článek 6

Systémy, protokoly a nástroje IKT

1. Finanční subjekty využívají a udržují aktualizované systémy, protokoly a nástroje IKT, které splňují následující podmínky:

   (a) systémy a nástroje jsou přiměřené povaze, škále, komplexnosti a rozsahu operací podporujících provádění jejich činností;

   (b) jsou spolehlivé;

   (c) mají dostatečnou kapacitu ke správnému zpracování dat potřebných k včasnému výkonu činností a poskytování služeb a k realizaci vysokých objemů objednávek, zpráv nebo transakcí podle potřeby, a to i v případě zavádění nových technologií;

   (d) jsou technologicky odolné, aby podle potřeby adekvátně zvládaly další požadavky na zpracování informací za napjatých tržních podmínek či v jiných nepříznivých situacích.

2. Používají-li finanční subjekty mezinárodně uznávané technické normy a nejlepší odvětvové postupy v oblasti bezpečnosti informací a interních kontrol IKT, používají tyto normy a postupy v souladu s veškerými příslušnými doporučeními orgánů dohledu pro jejich začlenění.

Článek 7

Identifikace

1. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty identifikují, klasifikují a náležitě zdokumentují veškeré funkce související s IKT v rámci činnosti organizace, informační aktiva podporující tyto funkce a konfigurace systémů IKT a jejich propojení s interními a externími systémy IKT. Finanční subjekty podle potřeby a alespoň jednou ročně přezkoumají přiměřenost klasifikace informačních aktiv a veškeré příslušné dokumentace.

2. Finanční subjekty nepřetržitě identifikují všechny zdroje rizik v oblasti IKT, zejména rizika vzájemné expozice s jinými finančními subjekty, a vyhodnocují kybernetické hrozby a zranitelná místa IKT relevantní pro funkce v rámci činnosti organizace související s IKT a informační aktiva. Finanční subjekty pravidelně, přinejmenším však jednou ročně, revidují scénáře rizik, které jsou pro ně relevantní.

3. Finanční subjekty jiné než mikropodniky vyhodnocují rizika po každé velké změně v infrastruktuře sítě a informačního systému a v procesech nebo postupech ovlivňujících funkce v rámci jejich činnosti, podpůrné procesy nebo informační aktiva.

4. Finanční subjekty identifikují všechny účty systémů IKT, včetně účtů na vzdálených pracovištích, síťové zdroje a hardwarové vybavení a evidují fyzické vybavení považované za kritické. Evidují konfiguraci aktiv IKT a propojení a vzájemné závislosti různých prostředků IKT.

5. Finanční subjekty identifikují a dokumentují veškeré procesy závislé na poskytovatelích služeb IKT z řad třetích stran a identifikují vzájemná propojení s poskytovateli služeb IKT z řad třetích stran.

6. Finanční subjekty pro účely odstavců 1, 4 a 5 vedou a pravidelně aktualizují příslušné soupisy.

7. Finanční subjekty jiné než mikropodniky pravidelně, přinejmenším však jednou ročně, provádějí zvláštní posouzení rizik v oblasti IKT u všech stávajících systémů IKT, zejména před propojením a po propojení starých a nových technologií, aplikací nebo systémů.

Článek 8

Ochrana a prevence

1. Pro účely odpovídající ochrany systémů IKT a organizace odezvy finanční subjekty nepřetržitě sledují a kontrolují fungování systémů a nástrojů IKT a minimalizují dopad takových rizik prostřednictvím zavedení vhodných nástrojů, strategií a postupů v oblasti IKT.

2. Finanční subjekty navrhují, opatřují a uplatňují strategie, politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, jejichž účelem je zejména zajištění odolnosti, kontinuity provozu a dostupnosti systémů IKT a udržování vysokých standardů bezpečnosti, důvěrnosti a integrity dat během jejich uchovávání, používání i přenosu.

3. Za účelem dosažení cílů uvedených v odstavci 2 finanční subjekty využívají nejmodernější technologie a procesy IKT, které:

   (a) zajišťují bezpečnost prostředků pro přenos informací;

   (b) minimalizují riziko poškození nebo ztráty dat, neoprávněného přístupu a technických závad, jež mohou narušovat výkon jejich činnosti;

   (c) zamezují úniku informací;

   (d) zajišťují ochranu dat před riziky souvisejícími se špatnou správou nebo zpracováním, včetně neodpovídajícího vedení záznamů.

4. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty:

   (a) vypracují a zdokumentují politiku zabezpečení informací s vymezením pravidel ochrany důvěrnosti, integrity a dostupnosti svých prostředků IKT, dat a informačních aktiv a prostředků IKT, dat a informačních aktiv svých klientů;

   (b) zavedou vhodné řízení sítí a infrastruktury na základě rizik využívající odpovídajících technik, metod a protokolů, včetně zavedení automatizovaných mechanismů pro izolaci dotčených informačních aktiv v případě kybernetických útoků;

   (c) uplatňují politiky omezující fyzický a virtuální přístup k prostředkům systémů IKT a k datům na minimum nezbytné pro výkon oprávněných a schválených funkcí a činností a za tím účelem vytvoří soubor zásad, postupů a kontrol pro přístupová práva a jejich řádnou správu;

   (d) zavedou postupy a protokoly pro silné ověřovací mechanismy založené na příslušných normách a systémech speciálních kontrol s cílem zabránit přístupu

ke kryptografickým klíčům, jimiž jsou zašifrována data, na základě výsledků schválené klasifikace dat a procesů posuzování rizik;

(e) zavedou politiky, postupy a kontroly pro řízení změn IKT, včetně změn softwarových, hardwarových a firmwarových komponentů, změn systému nebo změn zabezpečení, vycházející z posouzení rizik a tvořící nedílnou součást celkových postupů finančního subjektu pro řízení změn, s cílem zajistit, aby všechny změny systémů IKT byly řízeně zaznamenány, otestovány, vyhodnoceny, schváleny, zavedeny a ověřeny;

(f) mají odpovídající a ucelené zásady pro dočasné opravy a aktualizace.

Pro účely písmene b) finanční subjekty navrhnou infrastrukturu připojení k síti umožňující jeho okamžité přerušení a zajistí její rozčlenění a segmentaci s cílem minimalizovat šíření krize a zabránit jeho vzniku, zejména u vzájemně propojených finančních procesů.

Pro účely písmene e) jsou postupy řízení změn v oblasti IKT schvalovány příslušnými liniemi vedení a jejich součástí jsou specifické protokoly pro případ naléhavých změn.

Článek 9

Odhalování

1. Finanční subjekty mají zavedeny mechanismy včasného odhalování neobvyklých aktivit podle článku 15, včetně problémů s fungováním sítě IKT a incidentů souvisejících s IKT, a mechanismy identifikace jakýchkoli potenciálních významných kritických míst.

   Všechny detekční mechanismy uvedené v prvním pododstavci se pravidelně testují v souladu s článkem 22.

2. Detekční mechanismy uvedené v odstavci 1 umožňují vícestupňovou kontrolu, stanoví mezní hodnoty a kritéria výstrah pro spuštění detekce incidentů souvisejících s IKT a procesů reakce na ně a zavedou automatické výstražné mechanismy pro příslušné pracovníky odpovědné za reakce na incidenty související s IKT.

3. Finanční subjekty věnují s přihlédnutím ke své velikosti, činnosti a rizikových profilů dostatečné zdroje a prostředky na sledování aktivity uživatelů a výskytu anomálií IKT a incidentů souvisejících s IKT, zejména kybernetických útoků.

4. Finanční subjekty uvedené v čl. 2 odst. 1 písm. l) kromě toho zavedou systémy umožňující účinně kontrolovat úplnost obchodních zpráv, zjišťovat chybějící údaje a zjevné chyby a požadovat nové zaslání takovýchto chybných zpráv.

Článek 10

Reakce a obnova

1. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 a na základě požadavků na identifikaci uvedených v článku 7 finanční subjekty zavedou specializovanou a ucelenou strategii zachování provozu IKT jakožto nedílnou součást operační strategie zachování provozu finančního subjektu.

2. Finanční subjekty uplatňují strategii zachování provozu IKT uvedenou v odstavci 1 prostřednictvím specializovaných, vhodných a zdokumentovaných ujednání, plánů, postupů a mechanismů zaměřených na:

   (a) zaznamenávání všech incidentů souvisejících s IKT;

(b) zajištění kontinuity zásadních funkcí finančního subjektu;

(c) rychlou, vhodnou a účinnou reakci na všechny incidenty související s IKT a jejich vyřešení, zejména, avšak nejen kybernetické útoky, a to tak, aby byly omezeny škody a byla prioritně obnovena činnost a aktivována opatření na obnovu;

(d) neprodlenou aktivaci specializovaných plánů uvádějících do chodu izolační opatření, procesy a technologie odpovídající různým typům incidentů souvisejících s IKT a zamezující dalším škodám, jakož i přizpůsobené postupy reakce a obnovy v souladu s článkem 11;

(e) odhad předběžných dopadů, škod a ztrát;

(f) zavedení opatření v oblasti komunikace a krizového řízení, která zajistí předání aktualizovaných informací všem příslušným interním pracovníkům a externím zainteresovaným stranám podle článku 13 a jejich nahlášení příslušným orgánům v souladu s článkem 17.

3. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty uplatňují související plán obnovy provozu po havárii IKT, který u finančních subjektů jiných než mikropodniky podléhá nezávislým auditním přezkumům.

4. Finanční subjekty zavedou, udržují a pravidelně testují odpovídající plány zachování provozu IKT, zejména s ohledem na zásadní nebo důležité funkce zajišťované externě nebo nasmlouvané prostřednictvím ujednání s poskytovateli služeb IKT z řad třetích stran.

5. V rámci svého komplexního řízení rizik v oblasti IKT finanční subjekty:

(a) alespoň jednou ročně a po podstatných změnách systému IKT testují strategii zachování provozu IKT a plán obnovy provozu po havárii IKT;

(b) testují plány krizové komunikace zavedené podle článku 13.

Pro účely písmene a) finanční subjekty jiné než mikropodniky zahrnou do plánů testování scénáře kybernetických útoků a přechodu z primární infrastruktury IKT na rezervní kapacitu, záložní a rezervní zařízení nutná ke splnění povinností stanovených v článku 11.

Finanční subjekty pravidelně přezkoumávají svoji strategii zachování provozu IKT a plán obnovy provozu po havárii IKT, přičemž zohlední výsledky testů provedených v souladu s prvním pododstavcem a doporučeními vyplývajícími z auditních kontrol nebo přezkumů provedených orgány dohledu.

6. Finanční subjekty jiné než mikropodniky zavedou funkci řízení krizí, jež v případě aktivace strategie zachování provozu IKT nebo plánu obnovy provozu po havárii IKT stanoví jednoznačné postupy pro řízení interní a externí krizové komunikace podle článku 13.

7. Finanční subjekty zaznamenávají činnosti před výpadky a během výpadků po aktivaci strategie zachování provozu IKT nebo plánu obnovy provozu po havárii IKT. Tyto záznamy musí být ihned k dispozici.

8. Finanční subjekty uvedené v čl. 2 odst. 1 písm. f) poskytnou příslušným orgánům kopie výsledků testů zachování provozu IKT nebo podobných zkoušek provedených během přezkoumávaného období.

9. Finanční subjekty jiné než mikropodniky nahlásí příslušným orgánům veškeré náklady a ztráty způsobené výpadky IKT a incidenty souvisejícími s IKT.

Článek 11

Zásady zálohování a postupy obnovy

1. Pro účely zajištění obnovy provozu systémů IKT s minimální odstávkou a omezenými výpadky fungování finanční subjekty jako součást svého rámce pro řízení rizik v oblasti IKT vypracují:

   (a) zásady zálohování uvádějící rozsah dat, která se zálohují, a minimální frekvenci zálohování, a to na základě významu informací nebo citlivosti dat;

   (b) postupy obnovy.

2. Záložní systémy se spustí bez zbytečného prodlení, ledaže by takové spuštění ohrozilo bezpečnost sítí a informačních systémů nebo integritu a důvěrnost dat.

3. Při obnově zálohovaných dat pomocí vlastních systémů finanční subjekty použijí systémy IKT s operačním prostředím, jež je odlišné od hlavního, není k němu připojeno a je zabezpečeno před jakýmkoliv neoprávněným přístupem nebo narušením IKT.

   U finančních subjektů uvedených v čl. 2 odst. 1 písm. g) plány obnovy provozu umožňují obnovit všechny obchody k okamžiku přerušení, aby ústřední protistrana mohla nadále s jistotou fungovat a dokončit vypořádání ve stanovený den.

4. Finanční subjekty udržují rezervní kapacity IKT vybavené zdroji, prostředky a funkcemi, jež jsou dostatečné a vhodné pro zajištění potřeb jejich činnosti.

5. Finanční subjekty uvedené v čl. 2 odst. 1 písm. f) provozují alespoň jedno sekundární místo zpracování vybavené zdroji, prostředky, funkcemi a personálem dostatečnými a vhodnými pro zajištění potřeb jejich činnosti, nebo zajistí, aby takové sekundární místo provozovaly třetí strany, které jim poskytují služby IKT.

   Sekundární místo zpracování:

   (a) se nachází v takové geografické vzdálenosti od primárního místa zpracování, aby bylo zajištěno, že má odlišný profil a aby se zabránilo, že se jej dotkne událost, která zasáhla primární místo;

   (b) dokáže zajistit kontinuitu zásadních služeb stejně jako primární místo, nebo poskytovat úroveň služeb nezbytnou k zajištění provádění zásadních operací finančního subjektu v rámci cílů pro obnovu;

   (c) je ihned přístupné pro personál finančního subjektu zajišťující kontinuitu zásadních služeb v případě, že primární místo zpracování přestane být dostupné.

6. Při stanovení cílové doby a okamžiku obnovy provozu jednotlivých funkcí finanční subjekty zohlední potenciální celkový dopad na tržní efektivitu. Tyto časové cíle zajistí dodržení sjednaných úrovní služeb při extrémních scénářích.

7. Při obnově provozu po incidentu souvisejícím s IKT finanční subjekty provedou různé kontroly, včetně porovnání dat, aby byla zajištěna nejvyšší možná úroveň integrity dat. Tyto kontroly se provádějí rovněž při obnově dat od externích zainteresovaných stran, aby byla zajištěna konzistentnost všech dat v obou systémech.

Článek 12

Poučení a rozvoj

1. Finanční subjekty disponují prostředky a personálem odpovídajícími jejich velikosti, činnosti a rizikovým profilům, aby mohly shromažďovat informace o zranitelných místech a kybernetických hrozbách a o incidentech souvisejících s IKT, zejména kybernetických útocích, a analyzovat jejich pravděpodobný dopad na svoji digitální provozní odolnost.

2. Finanční subjekty zavedou přezkumy po závažných výpadcích IKT u svých hlavních činností zahrnující analýzu příčin výpadku a určení potřebných zlepšení operací IKT nebo v rámci strategie zachování provozu IKT uvedené v článku 10.

   Finanční subjekty jiné než mikropodniky při zavádění změn nahlásí tyto změny příslušným orgánům.

   Přezkumy po incidentech souvisejících s IKT podle prvního pododstavce stanoví, zda byly dodrženy zavedené postupy a zda byla přijatá opatření účinná, včetně:

   (a) rychlosti reakce na bezpečnostní výstrahy a stanovení dopadu incidentů souvisejících s IKT a jejich závažnosti;

   (b) kvality a rychlosti provádění forenzních analýz;

   (c) efektivity eskalace incidentů v rámci finančního subjektu;

   (d) efektivity interní a externí komunikace.

3. Poučení vyvozená z testování digitální provozní odolnosti provedeného v souladu s články 23 a 24 a ze skutečných incidentů souvisejících s IKT, zejména kybernetických útoků, a dále z problémů v souvislosti s aktivací plánu zachování provozu nebo plánu obnovy a relevantních informací vyměňovaných s protistranami a vyhodnocovaných během přezkumů orgány dohledu se začlení do postupů posuzování rizik IKT. Na základě těchto zjištění se provedou odpovídající přezkumy příslušných složek rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1.

4. Finanční subjekty sledují účinnost uplatňování své strategie digitální odolnosti podle čl. 5 odst. 9. Evidují vývoj rizik v oblasti IKT v čase, analyzují četnost, druhy, rozsah a vývoj incidentů souvisejících s IKT, zejména kybernetických útoků a jejich vzorců, aby bylo možné pochopit míru expozice rizikům v oblasti IKT a zvýšit kybernetickou vyspělost a připravenost finančního subjektu.

5. Vedoucí pracovníci odpovídající za IKT minimálně jednou ročně hlásí vedoucímu orgánu zjištění podle odstavce 3 a předloží doporučení.

6. Finanční subjekty vypracují jako povinné moduly svých osnov pro školení pracovníků programy zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti. Tato školení platí pro všechny zaměstnance a vyšší vedoucí pracovníky.

   Finanční subjekty průběžně sledují relevantní technologický vývoj, mimo jiné s cílem pochopit možné dopady zavádění nových technologií na požadavky na zabezpečení IKT a digitální provozní odolnost. Drží krok s nejnovějšími postupy řízení rizik v oblasti IKT a současně účinně čelí stávajícím či novým formám kybernetických útoků.

Článek 13

Komunikace

1. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty zavedou komunikační plány umožňující odpovědné informování klientů, protistran a případně veřejnosti o incidentech souvisejících s IKT nebo hlavních slabých místech.

2. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty uplatňují komunikační strategie pro pracovníky a externí zainteresované strany. Komunikační strategie pro pracovníky zohledňují nutnost rozlišovat mezi pracovníky podílejícími se na řízení rizik v oblasti IKT, zejména na reakci a na obnově provozu, a pracovníky, které je nutné informovat.

3. Uplatňováním komunikační strategie pro incidenty související s IKT a plněním role mluvčího pro styk s veřejností a médii pro tyto účely je pověřena alespoň jedna osoba v rámci subjektu.

Článek 14

Další harmonizace nástrojů, metod, postupů a strategií řízení rizik v oblasti IKT

Evropský orgán pro bankovnictví (EBA), Evropský orgán pro cenné papíry a trhy (ESMA) a Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění (EIOPA) po konzultaci s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) vypracují návrh regulačních technických norem pro následující účely:

(a) specifikace dalších prvků, které mají být začleněny do strategií, postupů, protokolů a nástrojů zabezpečení IKT uvedených v čl. 8 odst. 2 s cílem zajištění bezpečnosti sítí, zavedení vhodných ochranných opatření proti vniknutí a zneužití dat, zachování autenticity a integrity dat, včetně kryptografických technik, a zajištění přesného a rychlého přenosu dat bez vážných narušení;

(b) stanovení jak mají strategie, postupy a nástroje pro zabezpečení IKT uvedené v čl. 8 odst. 2 začleňovat bezpečnostní kontroly do systémů již od počátku (bezpečnost již od fáze návrhu), umožňovat přizpůsobení se vyvíjejícím se hrozbám a zajistit využívání technologií pro ochranu do hloubky;

(c) specifikace vhodných technik, postupů a protokolů uvedených v čl. 8 odst. 4 písm. b);

(d) další vývoj prvků kontrol řízení přístupových práv uvedených v čl. 8 odst. 4 písm. c) a vypracování související strategie v oblasti lidských zdrojů stanovící přístupová práva, postupy udělování a odebírání těchto práv, sledování neobvyklého chování v souvislosti s riziky v oblasti IKT pomocí vhodných ukazatelů, včetně ukazatelů vzorců, doby, aktivit IT a neznámých zařízení při používání sítě;

(e) další vývoj prvků uvedených v čl. 9 odst. 1 umožňujících rychle odhalit neobvyklé aktivity a kritérií uvedených v čl. 9 odst. 2 pro spuštění procesů detekce a reakce v případě incidentů souvisejících s IKT;

(f) specifikace složek strategie zachování provozu IKT uvedené v čl. 10 odst. 1;

(g) specifikace testování plánů zachování provozu IKT podle čl. 10 odst. 5, aby se zajistilo řádné zohlednění scénářů, za nichž se kvalita poskytování zásadních

nebo důležitých funkcí zhoršuje na nepřijatelnou úroveň nebo toto poskytování selhává, a potenciálního dopadu platební neschopnosti či jiných selhání jakéhokoli poskytovatele služeb IKT z řad třetích stran a v příslušných případech politická rizika v jurisdikcích příslušných poskytovatelů;

(h) specifikace složek plánu obnovy provozu po havárii IKT uvedeného v čl. 10 odst. 3.

EBA, ESMA a EIOPA předloží tyto návrhy regulačních technických norem Komisi do [*OJ: vložte datum 1 rok od data vstupu v platnost*].

Na Komisi je přenesena pravomoc přijímat regulační technické normy uvedené v prvním pododstavci v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

KAPITOLA III

ŘÍZENÍ, KLASIFIKACE a HLÁŠENÍ INCIDENTŮ SOUVISEJÍCÍCH S IKT

Článek 15

Proces řízení incidentů souvisejících s IKT

1. Finanční subjekty zavedou a uplatňují proces řízení incidentů souvisejících s IKT za účelem zjišťování, řízení a hlášení incidentů souvisejících s IKT, a zavedou výstražné ukazatele včasného varování.

2. Finanční subjekty zavedou vhodné procesy zajišťující konzistentní a integrované sledování, řešení a následná opatření pro incidenty související s IKT, aby byla zajištěna identifikace a odstranění jejich hlavních příčin, a zabránilo se tak výskytu těchto incidentů.

3. Proces řízení incidentů souvisejících s IKT uvedený v odstavci 1:

   (a) stanoví postupy k identifikaci, sledování, evidenci, kategorizaci a klasifikaci incidentů souvisejících s IKT podle jejich priority a závažnosti a podle významu zasažených služeb v souladu s kritérii uvedenými v čl. 16 odst. 1;

   (b) přiřadí úlohy a odpovědnosti, které je třeba aktivovat u různých typů a scénářů incidentů souvisejících s IKT;

   (c) stanoví plány komunikace pro pracovníky, externí zainteresované strany a média podle článku 13 a pro informování klientů, postupy interní eskalace, včetně stížností klientů souvisejících s IKT, a případně rovněž pro poskytování informací finančním subjektům jednajícím jako protistrany;

   (d) zajistí, aby byly závažné incidenty související s IKT hlášeny příslušným vyšším vedoucím pracovníkům, a o závažných incidentech souvisejících s IKT informuje vedoucí orgán s vysvětlením dopadů, reakce a dalších kontrol, jež budou zavedeny v důsledku incidentů souvisejících s IKT;

   (e) zavede postupy reakce na incidenty související s IKT ke zmírnění dopadů a zajistí, aby služby byly včas a bezpečně obnoveny.

Článek 16

Klasifikace incidentů souvisejících s IKT

1. Finanční subjekty klasifikují incidenty související s IKT a stanoví jejich dopad podle následujících kritérií:

   (a) počet uživatelů nebo finančních protistran dotčených výpadkem způsobeným incidentem souvisejícím s IKT, a zda incident související s IKT poškodil dobrou pověst;

   (b) doba trvání incidentu souvisejícího s IKT, včetně doby odstávky služby;

   (c) geografické rozšíření s ohledem na oblasti dotčené incidentem souvisejícím s IKT, zejména dopadne-li na více než dva členské státy;

   (d) ztráta dat v důsledku incidentu souvisejícího s IKT, například ztráta integrity, důvěrnosti nebo nedostupnost;

   (e) závažnost dopadu incidentu souvisejícího s IKT na systémy IKT finančního subjektu;

   (f) význam dotčených služeb, včetně transakcí a operací finančního subjektu;

   (g) absolutní i relativní ekonomický dopad incidentu souvisejícího s IKT.

2. Evropské orgány dohledu prostřednictvím svého společného výboru („společný výbor“) a po konzultaci s Evropskou centrální bankou (ECB) a ENISA vypracují společný návrh regulačních technických norem specifikujících:

   (a) kritéria stanovená v odstavci 1, včetně mezních hodnot závažnosti pro stanovení závažných incidentů souvisejících s IKT, na něž se vztahuje povinnost hlášení podle čl. 17 odst. 1;

   (b) kritéria, která příslušné orgány použijí pro účely posouzení relevantnosti závažných incidentů souvisejících s IKT pro jurisdikce jiných členských států, a údaje v hlášeních incidentů souvisejících s IKT, které budou sdíleny s dalšími příslušnými orgány podle čl. 17 bodů 5 a 6.

3. Evropské orgány dohledu při vypracování společného návrhu regulačních technických norem podle odstavce 2 přihlédnou k mezinárodním normám a rovněž ke specifikacím vypracovaným a zveřejněným ENISA, včetně případných specifikací pro jiná ekonomická odvětví.

   Evropské orgány dohledu předloží tento společný návrh regulačních technických norem Komisi do [*OP: vložte datum 1 rok od data vstupu v platnost*].

   Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených v odstavci 2 v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

Článek 17

Hlášení závažných incidentů souvisejících s IKT

1. Finanční subjekty hlásí závažné incidenty související s IKT příslušným orgánům uvedeným v článku 41 ve lhůtách stanovených v odstavci 3.

Pro účely prvního pododstavce finanční subjekty vypracují pomocí vzoru uvedeného v článku 18 na základě shromáždění a analýzy všech relevantních informací hlášení o incidentu a předloží je příslušnému orgánu.

Zpráva obsahuje veškeré informace nezbytné k tomu, aby příslušný orgán stanovil významnost závažného incidentu souvisejícího s IKT a posoudil možné přeshraniční dopady.

2. Má-li, nebo může-li mít závažný incident související s IKT dopad na finanční zájmy uživatelů služeb a klientů, finanční subjekty bez zbytečného prodlení uživatele svých služeb a klienty o tomto závažném incidentu souvisejícím s IKT informují a co nejdříve je informují o veškerých opatřeních přijetých ke zmírnění nepříznivých dopadů tohoto incidentu.

3. Finanční subjekty předloží příslušnému orgánu podle článku 41:

   (a) prvotní oznámení neprodleně, nejpozději však do konce obchodního dne, nebo v případě závažného incidentu souvisejícího s IKT, k němuž dojde později než dvě hodiny před koncem obchodního dne, nejpozději čtyři hodiny po začátku následujícího obchodního dne, nebo nejsou-li k dispozici kanály pro oznámení, jakmile budou dostupné;

   (b) průběžnou zprávu nejpozději jeden týden po prvotním oznámení podle písmene a), po níž případně následují aktualizovaná oznámení, jakmile jsou k dispozici aktualizované informace, a rovněž na základě výslovné žádosti příslušného orgánu;

   (c) závěrečnou zprávu po dokončení analýzy hlavní příčiny bez ohledu na to, zda již byla uplatněna zmírňující opatření, a poté, co jsou k dispozici skutečné číselné údaje o dopadech, které nahradí odhady, nejpozději však jeden měsíc od okamžiku odeslání prvotní zprávy

4. Finanční subjekty mohou delegovat své povinnosti hlášení podle tohoto článku na poskytovatele služeb, kteří jsou třetími stranami, pouze po schválení takového delegování příslušným orgánem uvedeným v článku 41.

5. Po obdržení hlášení podle odstavce 1 poskytne příslušný orgán bez zbytečného prodlení podrobné informace o incidentu:

   (a) EBA, ESMA či EIOPA, podle okolností;

   (b) případně ECB, jedná-li se o finanční subjekty uvedené v čl. 2 odst. 1 písm. a), b) a c); a

   (c) jednotnému kontaktnímu místu stanovenému podle článku 8 směrnice (EU) 2016/1148.

6. EBA, ESMA nebo EIOPA a ECB posoudí relevantnost závažného incidentu souvisejícího s IKT pro ostatní příslušné veřejné orgány a podle toho je co nejdříve vyrozumí. ECB informuje o veškerých záležitostech významných pro platební systém členy Evropského systému centrálních bank. Na základě oznámení přijmou příslušné orgány podle potřeby veškerá opatření nezbytná k ochraně bezprostřední stability finančního systému.

Článek 18

Harmonizace obsahu a vzory hlášení

1. Evropské orgány dohledu prostřednictvím společného výboru a po konzultaci s ENISA a ECB vypracují:

   (a) společný návrh regulačních technických norem pro:

      (1) stanovení obsahu hlášení u závažných incidentů souvisejících s IKT;

      (2) specifikaci podmínek, za nichž mohou finanční subjekty delegovat na základě předchozího schválení příslušným orgánem povinnost hlášení uvedenou v této kapitole na poskytovatele služeb, kteří jsou třetími stranami;

   (b) společný návrh prováděcích technických norem za účelem vytvoření standardních formulářů, vzorů a postupů, které finanční subjekty používají k hlášení závažných incidentů souvisejících s IKT.

   Evropské orgány dohledu předloží společný návrh regulačních technických norem podle odst. 1 písm. a) a společný návrh prováděcích technických norem podle odst. 1 písm. b) Komisi do xx 202x [*OP: vložte datum 1 rok od data vstupu v platnost*].

   Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím společných regulačních technických norem uvedených v odst. 1 písm. a) v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010 a (EU) č. 1094/2010.

   Na Komisi je přenesena pravomoc přijímat prováděcí technické normy uvedené v odst. 1 písm. b) postupem podle článku 15 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010, respektive (EU) č. 1094/2010.

Článek 19

Centralizace hlášení závažných incidentů souvisejících s IKT

1. Evropské orgány dohledu prostřednictvím společného výboru a po konzultacích s ECB a ENISA připraví společnou zprávu hodnotící proveditelnost další centralizace hlášení incidentů prostřednictvím vytvoření jednotného centra EU pro hlášení závažných incidentů souvisejících s IKT finančními subjekty. Zpráva přezkoumá možnosti usnadnění toku hlášení incidentů souvisejících s IKT, snížení nákladů a podpory tematických analýz s cílem zlepšení sbližování dohledu.

2. Zpráva uvedená v odstavci 1 obsahuje alespoň tyto prvky:

   (a) předpoklady pro vytvoření takového centra EU;

   (b) přínosy, omezení a případná rizika;

   (c) prvky provozního řízení;

   (d) podmínky členství;

   (e) způsoby přístupu finančních subjektů a vnitrostátních příslušných orgánů k centru EU;

   (f) předběžné posouzení finančních nákladů vytvoření provozní platformy podporující centrum EU, včetně nezbytného know-how.

3. Evropské orgány dohledu předloží zprávu uvedenou v odstavci 1 Komisi, Evropskému parlamentu a Radě do xx 202x [*Úř. věst.: vložte datum 3 roky po datu vstupu v platnost*].

Článek 20

Zpětná vazba orgánu dohledu

1. Příslušný orgán po obdržení zprávy podle čl. 17 odst. 1 potvrdí její přijetí a co nejrychleji finančnímu subjektu poskytne nezbytnou zpětnou vazbu nebo pokyny, zejména pojednávající o nápravě na úrovni daného subjektu nebo o způsobech minimalizace nepříznivého dopadu napříč odvětvími.

2. Evropské orgány dohledu každoročně anonymizovaně a souhrnně informují prostřednictvím společného výboru o hlášeních incidentů souvisejících s IKT obdržených od příslušných orgánů, přičemž uvedou alespoň počet závažných incidentů souvisejících s IKT, jejich povahu, dopad na provoz finančních subjektů nebo klientů, náklady a přijatá nápravná opatření.

   Evropské orgány dohledu vydávají varování a vysoce kvalitní statistiky na podporu posuzování hrozeb a zranitelných míst v oblasti IKT.

KAPITOLA IV

TESTOVÁNÍ DIGITÁLNÍ PROVOZNÍ ODOLNOSTI

Článek 21

Obecné požadavky na provádění testování digitální provozní odolnosti

1. Pro účely posuzování připravenosti na incidenty související s IKT, identifikace slabých míst, vad a nedostatků v digitální provozní odolnosti a rychlého zavedení nápravných opatření finanční subjekty s řádným přihlédnutím ke své velikosti, obchodní činnosti a rizikovým profilům vytvoří, udržují a aktualizují důkladný a ucelený program testování digitální provozní odolnosti jakožto nedílnou součást rámce pro řízení rizik v oblasti IKT uvedeného v článku 5.

2. Tento program testování digitální provozní odolnosti obsahuje celou řadu hodnocení, testů, metodik, postupů a nástrojů, které se použijí v souladu s ustanoveními článků 22 a 23.

3. Finanční subjekty při provádění programu testování digitální provozní odolnosti uvedeného v odstavci 1 postupují podle přístupu založeného na rizicích, přičemž zohlední vývoj rizik v oblasti IKT, jakákoli specifická rizika, jimž jsou, nebo mohou být vystaveny, význam informačních aktiv a poskytovaných služeb a rovněž jakékoliv jiné faktory, které finanční subjekt považuje za vhodné.

4. Finanční subjekty zajistí, aby testy prováděly interní či externí nezávislé subjekty.

5. Finanční subjekty vytvoří postupy a strategie pro stanovení priorit, klasifikaci a nápravu všech problémů zjištěných při provádění testů a vytvoří interní metodiky ověřování, jejichž prostřednictvím kontrolují, že všechny zjištěné slabiny, nedostatky či vady byly odstraněny.

6. Finanční subjekty alespoň jednou ročně otestují všechny své kritické systémy a aplikace IKT.

Článek 22

Testování nástrojů a systémů IKT

1. Program testování digitální provozní odolnosti uvedený v článku 21 stanoví provedení úplné škály vhodných testů, včetně hodnocení a zkoumání zranitelnosti, analýz otevřených zdrojů, posouzení zabezpečení sítě, analýz nedostatků, přezkumů fyzického zabezpečení, dotazníků a antivirových softwarových řešení, v proveditelných případech přezkumů zdrojových kódů, testů na základě scénářů, testování kompatibility, testování výkonnosti testování mezi koncovými body nebo penetračního testování.

2. Finanční subjekty uvedené v čl. 2 odst. 1 písm. f) a g) provádějí testování zranitelnosti před každým použitím či opakovaným použitím nových nebo stávajících služeb podporujících zásadní funkce, aplikací nebo prvků infrastruktury.

Článek 23

Pokročilé testování nástrojů, systémů a procesů IKT s využitím penetračního testování na základě hrozeb

1. Finanční subjekty určené podle odstavce 4 provádějí alespoň jednou za tři roky pokročilé testování s využitím penetračního testování na základě hrozeb.

2. Penetrační testování na základě hrozeb pokrývá alespoň zásadní funkce a služby finančního subjektu a provádí se za provozu na systémech skutečně využívaných k zajištění těchto funkcí. Přesný rozsah penetračního testování na základě hrozeb vycházející z posouzení zásadních funkcí a služeb stanoví finanční subjekty a potvrdí příslušné orgány.

   Pro účely prvního pododstavce finanční subjekty identifikují všechny základní procesy, systémy a technologie IKT podporující zásadní funkce a služby, včetně funkcí a služeb dodávaných externě či nasmlouvaných s poskytovateli služeb IKT z řad třetích stran.

   Jsou-li poskytovatelé služeb IKT z řad třetích stran zařazeni do penetračního testování na základě hrozeb, přijme finanční subjekt nezbytná opatření pro zjištění účasti těchto poskytovatelů.

   Finanční subjekty použijí účinné kontroly v rámci řízení rizik, aby omezily rizika jakéhokoliv případného dopadu na data, poškození aktiv a narušení zásadních služeb nebo operací u vlastního finančního subjektu, jeho protistran nebo celého finančního sektoru.

   Finanční subjekt a externí subjekty provádějící testování na konci testu a po odsouhlasení zpráv a plánů nápravy předloží příslušnému orgánu dokumentaci potvrzující, že bylo penetrační testování na základě hrozeb provedeno v souladu s požadavky. Příslušné orgány dokumentaci validují a vydají osvědčení.

3. Finanční subjekty pro účely provedení penetračních testů na základě hrozeb uzavřou smlouvy s testery v souladu s článkem 24.

   Příslušné orgány určí finanční subjekty, které provádějí penetrační testování na základě hrozeb, podle velikosti, významu, činnosti a celkového rizikového profilu finančního subjektu, přičemž posuzují:

   (a) faktory související s dopady, zejména význam poskytovaných služeb a činností prováděných finančním subjektem;

(b) případná hlediska finanční stability, včetně systémové povahy finančního subjektu na vnitrostátní nebo případně unijní úrovni;

(c) konkrétní profil rizika v oblasti IKT, úroveň vyspělosti finančního subjektu v oblasti IKT nebo dotčené technologické prvky.

4. EBA, ESMA a EIOPA po konzultaci s ECB a s přihlédnutím k příslušným rámcům Unie platným pro penetrační testy na základě operativních informací vypracují návrh regulačních technických norem, který bude specifikovat:

(a) kritéria použitá pro účely uplatňování odstavce 6 tohoto článku;

(b) požadavky týkající se:

(a) rozsahu penetračního testování na základě hrozeb uvedeného v odstavci 2 tohoto článku;

(b) metodiky a postupů testování pro jednotlivé fáze procesu testování;

(c) výsledků a fáze ukončení testování a nápravy;

(c) druh spolupráce v oblasti dohledu potřebný k provádění penetračního testování na základě hrozeb, pokud jde o finanční subjekty působící ve více než jednom členském státě, aby byla umožněna náležitá úroveň zapojení orgánů dohledu a pružné uplatňování, které zohlední specifičnosti finančních pododvětví nebo místních finančních trhů.

Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do [*Úř. věst.: vložte datum 2 měsíce po datu vstupu v platnost*].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených ve druhém pododstavci v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010 a (EU) č. 1094/2010.

Článek 24

Požadavky na subjekty provádějící testování

1. Finanční subjekty použijí k penetračnímu testování na základě hrozeb pouze testery, kteří:

(a) jsou nejvhodnější a mají nejlepší pověst;

(b) disponují technickými a organizačními prostředky a specifickým know-how v oblasti hrozeb, penetračního testování nebo testování metodou „červeného týmu“;

(c) jsou certifikováni akreditačním orgánem v členském státě, nebo dodržují formální kodexy chování či etické rámce;

(d) v případě externích testerů předloží nezávislé potvrzení nebo auditní zprávu týkající se řádného řízení rizik v souvislosti s prováděním penetračního testování na základě hrozeb, včetně náležitého zabezpečení důvěrných informací finančního subjektu a prostředků nápravy rizik pro činnost finančního subjektu;

(e) v případě externích testerů jsou řádně a plně kryti příslušným pojištěním odpovědnosti za škody při výkonu povolání, včetně rizik pochybení a nedbalosti.

2. Finanční subjekty zajistí, aby ve smlouvách uzavřených s externími testery byla požadována řádná správa výsledků penetračního testování na základě hrozeb a aby jakékoliv jejich zpracování, včetně jakéhokoliv vypracování, návrhu, uložení, agregace, hlášení, sdělení nebo zničení neohrozilo finanční subjekt.

KAPITOLA V

ŘÍZENÍ RIZIK V OBLASTI IKT SPOJENÝCH S TŘETÍMI STRANAMI

ODDÍL I

HLAVNÍ ZÁSADY SPRÁVNÉHO ŘÍZENÍ RIZIK V OBLASTI IKT SPOJENÝCH S TŘETÍMI STRANAMI

Článek 25

Obecné zásady

Finanční subjekty řídí rizika v oblasti IKT spojená s třetími stranami jako nedílnou součást rizik v oblasti IKT ve svém rámci pro řízení rizik v oblasti IKT podle následujících zásad:

1. Finanční subjekty, které uzavřely smluvní ujednání na využívání služeb IKT za účelem provádění svých obchodních operací, jsou vždy plně odpovědné za dodržení a splnění všech povinností vyplývajících z tohoto nařízení a platných právních předpisů o finančních službách.

2. Řízení rizik v oblasti IKT spojených s třetími stranami musí být finančními subjekty uplatňováno s ohledem na zásadu proporcionality a na:

   (a) rozsah, složitost a význam závislostí v oblasti IKT;

   (b) rizika vyplývající ze smluvních ujednání o využívání služeb IKT uzavřených s poskytovateli z řad třetích stran se zohledněním významu či důležitosti příslušné služby, procesu nebo funkce a potenciálního dopadu na kontinuitu a kvalitu finančních služeb a činností na individuální úrovni i na úrovni skupiny.

3. Finanční subjekty jako součást svého rámce pro řízení rizik v oblasti IKT přijmou a pravidelně revidují strategii pro rizika v oblasti IKT spojená s třetími stranami, přičemž zohlední strategii více dodavatelů podle čl. 5 odst. 9 písm. g). Uvedená strategie obsahuje zásady využívání služeb IKT poskytovaných třetími stranami a uplatňuje se na individuálním a případně subkonsolidovaném či konsolidovaném základě. Vedoucí orgán pravidelně přezkoumává zjištěná rizika týkající se externího poskytování zásadních nebo důležitých funkcí.

4. Jako součást svého rámce pro řízení rizik IKT finanční subjekty na úrovni subjektu a na subkonsolidované a konsolidované úrovni vedou a aktualizují registr informací s ohledem na všechna smluvní ujednání o využívání služeb IKT poskytovaných třetími stranami.

   Smluvní ujednání uvedená v prvním pododstavci se řádně zdokumentují, přičemž se rozlišuje mezi těmi, která se týkají zásadních nebo důležitých funkcí a těmi, která se jich netýkají.

Finanční subjekty alespoň jednou ročně nahlásí příslušným orgánům informace o počtu nových ujednání o využívání služeb IKT, kategoriích poskytovatelů služeb IKT z řad třetích stran, druhu smluvních ujednání a poskytovaných službách a funkcích.

Finanční subjekt na požádání zpřístupní příslušným orgánům úplný registr informací, nebo jeho konkrétní části, dle příslušného požadavku, a rovněž jakékoli informace považované za nezbytné k účinnému dohledu nad finančním subjektem.

Finanční subjekty včas informují příslušný orgán o plánovaném nasmlouvání zásadních nebo důležitých funkcí a v případě, že se funkce stane zásadní nebo důležitou.

5. Finanční subjekty před uzavřením smluvního ujednání o využívání služeb IKT:

(a) posoudí, zda se smluvní ujednání týká zásadní nebo důležité funkce;

(b) posoudí, zda jsou splněny podmínky dohledu pro uzavření smlouvy;

(c) identifikují a posoudí všechna relevantní rizika týkající se smluvního ujednání, včetně možnosti, kdy tato smluvní ujednání mohou přispívat k zesílení rizika koncentrace IKT;

(d) s náležitou péčí přezkoumají potenciální poskytovatele služeb IKT z řad třetích stran a pomocí procesů výběru a vyhodnocení zajistí vhodnost poskytovatele služeb IKT z řad třetích stran;

(e) identifikují a posoudí střety zájmů, které mohou smluvní ujednání způsobit.

6. Finanční subjekty smí uzavírat smluvní ujednání pouze s poskytovateli služeb IKT z řad třetích stran, kteří splňují přísné, náležité a nejnovější normy v oblasti bezpečnosti informací.

7. Finanční subjekty při výkonu práv na přístup, kontrolu a audit u poskytovatele služeb IKT z řad třetích stran předem na základě rizik stanoví četnost auditů a kontrol a oblasti, které budou auditovány s využitím obecně uznávaných auditních standardů a v souladu se všemi pokyny orgánů dohledu pro využití a začlenění těchto auditních standardů.

U technicky velmi složitých smluvních ujednání finanční subjekt ověří, že interní, skupinoví nebo externí auditoři disponují příslušnými dovednostmi a znalostmi pro účinné provedení relevantních auditů a posouzení.

8. Finanční subjekty zajistí, že budou smluvní ujednání o využívání služeb IKT ukončena alespoň za podmínek:

(a) třetí strana poskytující služby IKT poruší platné zákony, předpisy nebo smluvní podmínky;

(b) sledováním rizik v oblasti IKT spojených s třetími stranami se zjistí okolnosti, u nichž se má za to, že mohou změnit plnění funkcí poskytovaných prostřednictvím smluvního ujednání, včetně podstatných změn ovlivňujících dané ujednání nebo situaci poskytovatele služeb IKT z řad třetích stran;

(c) u celkového řízení rizik v oblasti IKT poskytovatele služeb IKT z řad třetích stran jsou zjištěna slabá místa, a to zejména ve způsobu, jakým zajišťuje bezpečnost důvěrných, osobních nebo jiných citlivých dat nebo jiných než osobních informací;

(d) okolnosti, za nichž již příslušný orgán nedokáže dále efektivně dohlížet na finanční subjekt, které vzniknou v důsledku příslušného smluvního ujednání.

9. Finanční subjekty zavedou strategie ukončení smluvního vztahu, aby zohlednily rizika, jež mohou vzniknout na úrovni třetí strany poskytující služby IKT, zejména její případný úpadek, snížení kvality poskytovaných funkcí, jakékoliv narušení činnosti v důsledku nevhodného či chybného poskytování služeb nebo vážného rizika vznikajícího v souvislosti s řádným a nepřetržitým vykonáváním funkce.

Finanční subjekty zajistí, aby byly schopny ukončit smluvní ujednání, aniž by došlo k:

(a) narušení jejich činností,

(b) narušení dodržování regulatorních požadavků,

(c) zhoršení kontinuity a kvality služeb, které poskytují klientům.

Plány ukončení smluvního vztahu musí být komplexní, zdokumentované a v případě potřeby dostatečně otestované.

Finanční subjekty identifikují alternativní řešení a vypracují plány přechodu, které jim umožní odebrání nasmlouvaných funkcí a příslušných dat od třetí strany poskytující služby IKT a jejich bezpečný a integrovaný přenos k alternativnímu poskytovateli, nebo jejich začlenění v rámci vlastní organizace.

Finanční subjekty přijmou vhodná opatření pro nepředvídané události, aby byla za všech okolností uvedených v prvním pododstavci zachována kontinuita provozu.

10. Evropské orgány dohledu vypracují prostřednictvím společného výboru návrh prováděcích technických norem, které stanoví standardní vzory pro účely registru informací uvedeného v odstavci 4.

Evropské orgány dohledu předloží tyto návrhy prováděcích technických norem Komisi do [*Úř. věst.: vložte datum 1 roku od data vstupu tohoto nařízení* v platnost].

Na Komisi je přenesena pravomoc přijímat prováděcí technické normy uvedené v prvním pododstavci postupem podle článku 15 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010, respektive (EU) č. 1094/2010.

11. Evropské orány dohledu prostřednictvím společného výboru vypracují návrh regulačních norem:

(a) pro další specifikaci podrobného obsahu zásad uvedených v odstavci 3 týkajících se smluvních ujednání o použití služeb IKT dodávaných třetími stranami poskytujícími služby IKT formou odkazu na hlavní fáze životního cyklu příslušných ujednání o použití služeb IKT;

(b) pro druh informací, které mají být uvedeny v registru informací podle odstavce 4.

Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do [*OP: vložte datum 1 rok od data vstupu v platnost*].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených ve druhém pododstavci v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010 a (EU) č. 1094/2010.

Článek 26

Předběžné posouzení rizika koncentrace IKT a dalších ujednání se subdodavateli

1. Finanční subjekty při identifikaci a posuzování rizika koncentrace IKT podle čl. 25 odst. 5 písm. c) zohlední, zda by uzavření smluvního ujednání souvisejícího se službami IKT způsobilo jakoukoli z následujících situací:

   (a) uzavření smlouvy se třetí stranou poskytující služby IKT, kterou není snadné nahradit; nebo

   (b) uzavření více smluvních ujednání týkajících se dodávky služeb IKT stejnou třetí stranou poskytující služby IKT nebo s úzce propojenými třetími stranami poskytujícími služby IKT.

   Finanční subjekty zváží přínosy a náklady alternativních řešení, například využití jiných třetích stran poskytujících služby IKT, přičemž zohlední, zda a jak předpokládaná řešení odpovídají požadavkům obchodní činnosti a cílům stanoveným v jejich strategii digitální odolnosti.

2. Obsahují-li smluvní ujednání o využívání služeb IKT možnost, aby třetí strana poskytující služby IKT zajišťovala zásadní nebo důležitou funkci prostřednictvím subdodávek od jiných třetích stran poskytujících služby IKT, finanční subjekty zváží výhody a rizika, jež mohou vzniknout v souvislosti s tímto využitím subdodavatele IKT, zejména je-li tento subdodavatel IKT usazen ve třetí zemi.

   Jsou-li smluvní ujednání o využívání služeb IKT uzavřena se třetí stranou poskytující služby IKT usazenou ve třetí zemi, finanční subjekty považují za relevantní alespoň následující faktory:

   (a) dodržování ochrany dat;

   (b) účinné prosazování právních předpisů;

   (c) ustanovení insolvenčních právních předpisů, která se uplatní v případě úpadku třetí strany poskytující služby IKT;

   (d) veškerá omezení, jež mohou vzniknout při naléhavé obnově dat finančního subjektu.

   Finanční subjekty posoudí, zda a jak mohou potenciální dlouhé nebo složité subdodavatelské řetězce ovlivnit jejich schopnost plně sledovat nasmlouvané funkce a schopnost příslušných orgánů provádět v tomto ohledu účinný dohled nad finančním subjektem.

Článek 27

Hlavní smluvní ustanovení

1. Práva a povinnosti finančního subjektu a třetí strany poskytující služby IKT jsou jasně rozděleny a stanoveny písemně. Úplná smlouva, která zahrnuje dohody o úrovni služeb, je vyhotovena v jednom písemném dokumentu dostupném stranám ve fyzické formě, nebo ve formátu, který lze stáhnout a je přístupný.

2. Smluvní ujednání o využívání služeb IKT minimálně obsahují:

   (a) srozumitelný a úplný popis všech funkcí a služeb dodávaných třetí stranou poskytující služby IKT s uvedením, zda je povoleno zajišťování zásadní nebo

důležité funkce nebo jejich podstatných součástí subdodavatelem, a v kladném případě podmínky, kterými se toto využití subdodavatele řídí;

(b) místa, kde budou nasmlouvané nebo subdodavatelem zajišťované funkce a služby poskytovány a kde budou zpracovávána data, včetně místa jejich uchovávání, a povinnost třetí strany poskytující služby IKT oznámit finančnímu subjektu, plánuje-li změnu těchto míst;

(c) ustanovení o přístupnosti, dostupnosti, integritě, bezpečnosti a ochraně osobních údajů a o zajištění přístupu, obnovy a vrácení ve snadno přístupném formátu osobních a jiných než osobních údajů zpracovávaných finančním subjektem v případě platební neschopnosti, řešení krize nebo přerušení činností třetí strany poskytující služby IKT;

(d) úplný popis úrovně služeb, včetně jejich aktualizací a revizí, a přesné kvalitativní i kvantitativní výkonnostní cíle v rámci sjednaných úrovní služeb umožňující účinné sledování finančním subjektem a neprodlená vhodná nápravná opatření, nejsou-li sjednané úrovně služeb splněny;

(e) výpovědní doby a povinnosti hlášení třetí strany poskytující služby IKT finančnímu subjektu, včetně oznámení jakéhokoliv vývoje, který by mohl mít významný dopad na schopnost třetí strany poskytující služby IKT účinně provádět zásadní nebo důležité funkce v souladu se sjednanými úrovněmi služeb;

(f) povinnost třetí strany poskytující služby IKT poskytnout v případě incidentu souvisejícího s IKT pomoc bezplatně, nebo za předem stanovenou cenu;

(g) povinnosti třetí strany poskytující služby IKT uplatňovat a testovat plány pro nepředvídané události a disponovat bezpečnostními opatřeními, nástroji a strategiemi v oblasti IKT, jež vhodně zajistí bezpečné poskytování služeb finančním subjektem v souladu s jeho regulačním rámcem;

(h) právo nepřetržitě sledovat výsledky třetí strany poskytující služby IKT, které zahrnuje:

  i) právo na přístup, kontrolu a audit vykonávané finančním subjektem nebo určeným třetím subjektem a právo pořizovat kopie příslušné dokumentace, přičemž jeho výkon nesmí být znemožňován či omezován jinými smluvními ujednáními nebo prováděcími strategiemi;

  ii) právo sjednat alternativní úroveň záruky, budou-li dotčena práva jiných klientů;

  iii) závazek úplné spolupráce při kontrolách na místě prováděných finančním subjektem a podrobnosti o rozsahu, způsobech a četnosti dálkových auditů;

(i) povinnost třetí strany poskytující služby IKT plně spolupracovat s příslušnými orgány a orgány příslušnými k řešení krize finančního subjektu, včetně jimi jmenovaných osob;

(j) práva na ukončení smlouvy a související minimální výpovědní doby pro ukončení smlouvy v souladu s očekáváními příslušných orgánů;

(k) strategie ukončení smluvního vztahu, zejména stanovení povinného vhodného přechodného období:

(a) během kterého bude třetí strana poskytující služby IKT s ohledem na snížení rizika výpadků u finančního subjektu nadále poskytovat příslušné funkce nebo služby;

(b) které umožní finančnímu subjektu podle složitosti poskytované služby změnit třetí stranu poskytující služby IKT, nebo přejít na vlastní řešení.

3. Finanční subjekty a třetí strany poskytující služby IKT při vyjednávání o smluvních ujednáních zváží použití standardních smluvních doložek vypracovaných pro konkrétní služby.

4. Evropské orgány dohledu vypracují prostřednictvím společného výboru návrh regulačních technických norem, jež podrobněji stanoví prvky, které musí finanční subjekt určit a posoudit při zajišťování zásadních nebo důležitých funkcí prostřednictvím subdodavatelů, aby byla řádně uplatněna ustanovení odst. 2 písm. a).

Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do [*Úř. věst.: vložte datum 1 rok od data vstupu v platnost*].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených v prvním pododstavci v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010 a (EU) č. 1094/2010.

ODDÍL II

RÁMEC DOHLEDU NAD KRITICKÝMI TŘETÍMI STRANAMI POSKYTUJÍCÍMI SLUŽBY IKT

Článek 28

Určení kritických třetích stran poskytujících služby IKT

1. Evropské orgány dohledu prostřednictvím společného výboru a na základě doporučení fóra dohledu zřízeného podle čl. 29 odst. 1:

(a) určí třetí strany poskytující služby IKT, které jsou kritické pro finanční subjekty, přičemž zohlední kritéria podle odstavce 2;

(b) jmenují buď EBA, ESMA, nebo EIOPA hlavním orgánem dohledu pro jednotlivé kritické třetí strany poskytující služby IKT, a to podle toho a, zda celková hodnota aktiv finančních subjektů, jež využívají služeb této kritické třetí strany poskytující služby IKT a na něž se vztahuje některé z nařízení (EU) č. 1093/2010 (EU), č. 1094/2010, respektive (EU) č. 1095/2010, představuje více než polovinu celkových aktiv všech finančních subjektů využívajících služeb dané kritické třetí strany poskytující služby IKT, což bude doloženo konsolidovanými účetními závěrkami finančních subjektů, nebo jejich jednotlivými účetními závěrkami, pokud účetní závěrky nejsou konsolidovány.

2. Určení podle odst. 1 písm. a) vychází ze všech následujících kritérií:

(a) systémový dopad na stabilitu, kontinuitu nebo kvalitu poskytování finančních služeb v případě, že bude příslušná třetí strana poskytující služby IKT čelit rozsáhlému provoznímu výpadku poskytování svých služeb, přičemž se zohlední počet finančních subjektů, kterým daná třetí strana poskytující služby IKT dodává své služby;

(b) systémová povaha či význam finančních subjektů, které spoléhají na danou třetí stranu poskytující služby IKT, na základě posouzení podle následujících parametrů:

i) počet globálních systémově významných institucí (G-SVI) nebo jiných systémově významných institucí (O-SVI), které spoléhají na danou třetí stranu poskytující služby IKT;

ii) vzájemná závislost mezi G-SVI nebo O-SVI uvedenými v bodě i) a dalšími finančními subjekty, včetně situací, kdy G-SVI nebo O-SVI poskytují služby finanční infrastruktury dalším finančním subjektům;

(c) spoléhání finančních subjektů na služby dodávané příslušnou třetí stranou poskytující služby IKT v souvislosti se zásadními nebo důležitými funkcemi finančních subjektů, které v konečném důsledku zahrnují zapojení stejné třetí strany poskytující služby IKT bez ohledu na to, zda finanční subjekty využívají tyto služby přímo či nepřímo prostřednictvím subdodavatelských ujednání;

(d) míra nahraditelnosti třetí strany poskytující služby IKT s přihlédnutím k těmto parametrům:

i) nedostatek, i částečný, reálných alternativ vzhledem k omezenému počtu třetích stran poskytujících služby IKT aktivně působících na konkrétním trhu, podíl příslušné třetí strany poskytující služby IKT na trhu, nebo technická složitost či sofistikovanost služeb, též v souvislosti s jakoukoli chráněnou technologií, nebo specifické vlastnosti organizace či činnosti třetí strany poskytující služby IKT;

ii) potíže s částečnou či úplnou migrací relevantních dat a pracovních úkolů při přechodu k jiné třetí straně poskytující služby IKT buď kvůli vysokým finančním nákladům, času nebo zdrojům, jež může proces migrace vyžadovat, nebo kvůli zvýšeným rizikům v oblasti IKT či jiným operačním rizikům, jimž může být finanční subjekt během této migrace vystaven;

(e) počet členských států, kde příslušná třetí strana poskytující služby IKT dodává své služby;

(f) počet členských států, kde působí finanční subjekty využívající příslušnou třetí stranu poskytující služby IKT.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 50 k doplnění kritérií uvedených v odstavci 2.

4. Mechanismus určování podle odst. 1 písm. a) se nepoužije, dokud Komise nepřijme akt v přenesené pravomoci podle odstavce 3.

5. Mechanismus určování podle odst. 1 písm. a) se nevztahuje na třetí strany poskytující služby IKT, které podléhají rámci dohledu stanovenému pro účely podpory úkolů uvedených v čl. 127 odst. 2 Smlouvy o fungování Evropské unie.

6. Evropské orgány dohledu prostřednictvím společného výboru vypracují, zveřejní a každoročně aktualizují seznam kritických třetích stran poskytujících služby IKT na úrovni Unie.

7. Příslušné orgány pro účely odst. 1 písm. a) každoročně a na agregovaném základě zašlou zprávy podle čl. 25 odst. 4 fóru dohledu vytvořenému v souladu s článkem 29.

Fórum dohledu posoudí na základě informací obdržených od příslušných orgánů závislost finančních subjektů na třetích stran IKT.

8. Třetí strany poskytující služby IKT, které nejsou uvedeny v seznamu podle odstavce 6, mohou požádat o zápis do tohoto seznamu.

Třetí strana poskytující služby IKT pro účely prvního pododstavce předloží odůvodněnou žádost EBA, ESMA nebo EIOPA, které prostřednictvím společného výboru rozhodnou, zda tuto třetí stranu poskytující služby IKT zařadí do seznamu podle odst. 1 písm. a).

Rozhodnutí uvedená ve druhém pododstavci se přijmou a oznámí třetí straně poskytující služby IKT do šesti měsíců od přijetí žádosti.

9. Finanční subjekty nesmí využívat třetí stranu poskytující služby IKT usazenou ve třetí zemi, která by byla označena za kritickou podle odst. 1 písm. a), kdyby byla usazena v Unii.

Článek 29

Struktura rámce dohledu

1. Společný výbor v souladu s článkem 57 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 vytvoří fórum dohledu jako podvýbor pro účely podpory pracovních úkolů společného výboru a hlavního orgánu dohledu podle čl. 28 odst. 1 písm. b), co se týče rizik v oblasti IKT spojenými s třetími stranami ve všech finančních odvětvích. Fórum dohledu připravuje návrhy společných stanovisek a společných aktů společného výboru v této oblasti.

Fórum dohledu pravidelně jedná o relevantním vývoji v oblasti rizik a zranitelných míst IKT a podporuje konzistentní přístup ke sledování rizik v oblasti IKT spojených s třetími stranami na úrovni Unie.

2. Fórum dohledu provede každý rok společné posouzení výsledků a zjištění dohledových činností prováděných pro všechny kritické třetí strany poskytující služby IKT a podporuje koordinační opatření ke zvýšení digitální provozní odolnosti finančních subjektů a osvědčené postupy pro řešení rizika koncentrace IKT a zkoumá zmírňující opatření u šíření rizik mezi odvětvími.

3. Fórum dohledu předloží komplexní referenční hodnoty kritických třetích stran poskytujících služby IKT, které společný výbor schválí jako společná stanoviska evropských orgánů dohledu v souladu s čl. 56 odst. 1 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

4. Fórum dohledu se skládá z předsedů evropských orgánů dohledu a jednoho zástupce na vysoké úrovni z řad stávajících vedoucích pracovníků příslušného orgánu z každého členského státu. Fóra dohledu se jako pozorovatelé účastní rovněž výkonní ředitelé jednotlivých evropských orgánů dohledu a po jednom zástupci z Evropské komise, ESRB, ECB a ENISA.

5. V souladu s článkem 16 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 vydají evropské orgány dohledu pro účely tohoto oddílu pokyny pro spolupráci mezi evropskými orgány dohledu a příslušnými orgány týkající se podrobných postupů a podmínek souvisejících s výkonem úkolů příslušných orgánů a evropských orgánů dohledu a podrobností o výměně informací, jež příslušné orgány potřebují k zajištění dodržování doporučení vydaných hlavními orgány

dohledu podle čl. 31 odst. 1 písm. d) kritickým třetím stranám poskytujícím služby IKT.

6. Požadavky stanovenými v tomto oddíle není dotčeno uplatňování směrnice (EU) 2016/1148 ani dalších právních předpisů Unie týkajících se dohledu vztahujících se na poskytovatele cloudových služeb.

7. Evropské orgány dohledu prostřednictvím společného výboru a na základě přípravné práce provedené fórem dohledu každý rok předloží Evropskému parlamentu, Radě a Komisi zprávu o uplatňování tohoto oddílu.

Článek 30

Úkoly hlavního orgánu dohledu

1. Hlavní orgán dohledu posoudí, zda jednotlivé kritické třetí strany poskytující služby IKT disponují komplexními, jasnými a účinnými pravidly, postupy, mechanismy a ujednáními pro řízení rizik v oblasti IKT, jež mohou představovat pro finanční subjekty.

2. Posouzení uvedené v odstavci 1 zahrnuje:

(a) požadavky v oblasti IKT k zajištění zejména bezpečnosti, dostupnosti, kontinuity, škálovatelnosti a kvality služeb, které kritická třetí strana poskytující služby IKT dodává finančním subjektům, a rovněž schopnost nepřetržitého dodržování vysokých standardů pro bezpečnost, důvěrnost a integritu dat;

(b) fyzické zabezpečení přispívající k zajištění bezpečnosti v oblasti IKT, včetně zabezpečení areálů, zařízení a datových center;

(c) procesy řízení rizik, včetně strategií pro řízení rizik v oblasti IKT, plánů zachování provozu IKT a plánů obnovy provozu po havárii IKT;

(d) systém správy a řízení, včetně organizační struktury s jasným, transparentním a konzistentním rozdělením odpovědnosti a pravidly odpovědnosti umožňující účinné řízení rizik v oblasti IKT;

(e) identifikaci, sledování a rychlé hlášení incidentů souvisejících s IKT finančním subjektům a řízení a řešení těchto incidentů, zejména kybernetických útoků;

(f) mechanismus pro přenositelnost dat a přenositelnost a interoperabilitu aplikací, který zajistí účinný výkon práv finančních subjektů na vypovězení smlouvy;

(g) testování systémů, infrastruktury a kontrol v oblasti IKT;

(h) audity v oblasti IKT;

(i) použití příslušných vnitrostátních a mezinárodních norem vztahujících se na poskytování jeho služeb IKT finančním subjektům.

3. Hlavní orgán dohledu přijme na základě hodnocení uvedeného v odstavci 1 jasné, podrobné a odůvodněné individuální plány dohledu pro jednotlivé kritické třetí strany poskytující služby IKT. Tento plán je každoročně sdělen příslušné kritické třetí straně poskytující služby IKT.

4. Po schválení a oznámení plánů dohledu uvedených v odstavci 3 kritickým třetím stranám poskytujícím služby IKT mohou příslušné orgány přijímat opatření týkající

se třetích stran poskytujících služby IKT pouze po dohodě s hlavním orgánem dohledu.

Článek 31

Pravomoci hlavního orgánu dohledu

1. Pro účely provádění povinností stanovených v tomto oddíle disponuje hlavní orgán dohledu těmito pravomocemi:

   (a) požádat o všechny příslušné informace a dokumentaci podle článku 32;

   (b) provádět obecná šetření a kontroly podle článků 33 a 34;

   (c) požadovat zprávy po dokončení činností dohledu, kde jsou uvedena provedená opatření nebo nápravné prostředky uplatněné kritickými třetími stranami poskytujícími služby IKT v souvislosti s doporučeními uvedenými v písmenu d) tohoto odstavce;

   (d) vydávat doporučení v oblastech uvedených v čl. 30 odst. 2, zejména pokud jde o:

      i) použití specifických požadavků či procesů v oblasti bezpečnosti a kvality IKT, zejména s ohledem na provádění dočasných oprav, aktualizací, šifrování a dalších bezpečnostních opatření, která hlavní orgán dohledu považuje za relevantní pro zajištění bezpečnosti služeb poskytovaných finančním subjektům v oblasti IKT;

      ii) použití smluvních podmínek, včetně jejich technického provádění, za nichž kritické třetí strany poskytující služby IKT poskytují své služby finančním subjektům a které hlavní orgán dohledu považuje za relevantní pro prevenci vzniku selhání nebo jeho rozšíření nebo pro minimalizaci možného systémového dopadu na celý finanční sektor Unie v případě rizika koncentrace IKT;

      iii) po přezkoumání ujednání o zajišťování služeb subdodavatelem podle článků 32 a 33, včetně ujednání o externím zajištění subdodávek, které kritické třetí strany poskytující služby IKT plánují uzavřít s dalšími třetími stranami poskytujícími služby IKT nebo subdodavateli IKT usazenými ve třetí zemi, všechna plánovaná externí zajišťování služeb, včetně subdodávek, u nichž se hlavní orgán dohledu domnívá, že mohou představovat rizika pro poskytování služeb finančními subjekty nebo ohrozit finanční stabilitu;

      iv) neuzavírání dalších ujednání o subdodávkách, jsou-li splněny následující kumulativní podmínky:

         – plánovaný subdodavatel je třetí stranou poskytující služby IKT nebo subdodavatelem IKT usazeným ve třetí zemi;

         – subdodávky se týkají zásadní nebo důležité funkce finančního subjektu.

2. Hlavní orgán dohledu před výkonem svých pravomocí podle odstavce 1 konzultuje fórum dohledu.

3. Kritické třetí strany poskytující služby IKT v dobré víře spolupracují s hlavním orgánem dohledu a pomáhají mu při plnění jeho úkolů.

4. Hlavní orgán dohledu může ukládat opakované pokuty, aby přiměl kritickou třetí stranu poskytující služby IKT dodržovat ustanovení odst. 1 písm. a), b) a c).

5. Opakované pokuty uvedené v odstavci 4 se ukládají na denním základě, dokud není dosaženo dodržování uvedených ustanovení, avšak nejdéle po dobu šesti měsíců od vyrozumění kritické třetí strany poskytující služby IKT.

6. Výše opakovaných pokut vypočítaná od data uvedeného v rozhodnutí o uložení opakovaných pokut činí 1 % průměrného denního celosvětového obratu dané kritické třetí strany poskytující služby IKT v předcházejícím obchodním roce.

7. Pokuty mají správní povahu a jsou vymahatelné. Výkon rozhodnutí se řídí předpisy občanského procesního práva toho členského státu, na jehož území se mají uskutečnit kontroly a přístup. Ohledně stížností souvisejících s nesprávným výkonem rozhodnutí jsou příslušné soudy dotčeného členského státu. Částky pokut jsou příjmem souhrnného rozpočtu Evropské unie.

8. Evropské orgány dohledu zveřejní každou opakovanou uloženou pokutu s výjimkou případů, kdy by jejich zveřejnění vážně ohrozilo finanční trhy nebo způsobilo nepřiměřenou škodu zúčastněným subjektům.

9. Hlavní orgán dohledu před uložením opakované pokuty podle odstavce 4 umožní zástupcům kritické třetí strany poskytující služby IKT, jíž se řízení týká, slyšení ohledně zjištění a svá rozhodnutí založí pouze na zjištěních, k nimž měla třetí strana poskytující služby IKT, které se řízení týká, možnost se vyjádřit. V průběhu řízení musí být plně respektováno právo účastníků řízení na obhajobu. Mají právo nahlížet do spisů, s výhradou oprávněného zájmu jiných osob na ochraně jejich obchodního tajemství. Právo nahlížet do spisu se nevztahuje na důvěrné informace ani na interní přípravné dokumenty hlavního orgánu dohledu.

Článek 32
Žádost o informace

1. Hlavní orgán dohledu může prostou žádostí nebo rozhodnutím požádat kritické třetí strany poskytující služby IKT, aby poskytly všechny informace nezbytné pro výkon povinností hlavního orgánu dohledu podle tohoto nařízení, včetně všech relevantních obchodních nebo provozních dokumentů, smluv, dokumentaci o vnitřních politikách, zpráv z auditů bezpečnosti IKT, zpráv o hlášení incidentů souvisejících s IKT a rovněž všech informací týkajících se stran, jimž kritická třetí strana poskytující služby IKT externě zadala zajišťování provozních funkcí nebo činnosti.

2. V případě prosté žádosti o informace podle odstavce 1 hlavní orgán dohledu:

   (a) odkazuje na tento článek jako na právní základ žádosti;

   (b) uvede účel žádosti;

   (c) upřesní, jaké informace jsou požadovány;

   (d) stanoví lhůtu, v níž mají být informace poskytnuty;

   (e) upozorní zástupce kritické třetí strany poskytující služby IKT, od níž informace žádá, že nemá povinnost informace poskytnout, avšak rozhodne-li se na žádost dobrovolně odpovědět, nesmějí být poskytnuté informace nepravdivé nebo zavádějící.

3. V případě žádosti o poskytnutí informací podle odstavce 1 na základě rozhodnutí hlavní orgán dohledu:

(a) odkazuje na tento článek jako na právní základ žádosti;

(b) uvede účel žádosti;

(c) upřesní, jaké informace jsou požadovány;

(d) stanoví lhůtu, v níž mají být informace poskytnuty;

(e) upozorní na pokuty stanovené v čl. 31 odst. 4, pokud budou poskytnuté informace neúplné;

(f) upozorní na možnost odvolat se proti rozhodnutí k odvolacímu senátu ESA a nechat rozhodnutí přezkoumat Soudním dvorem Evropské unie (dále jen „Soudní dvůr“) v souladu s články 60 a 61 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010, respektive (EU) č. 1095/2010.

4. Zástupci kritických třetích stran poskytujících služby IKT jsou povinni požadované informace dodat. Informace za své klienty mohou sdělit řádně zmocnění právní zástupci. Kritická třetí strana poskytující služby IKT však nese i nadále plnou odpovědnost, jsou-li poskytnuté informace neúplné, nepravdivé či zavádějící.

5. Hlavní orgán dohledu neprodleně zašle kopii rozhodnutí o předložení informací příslušným orgánům finančních subjektů využívajících služeb dotčených kritických třetích stran poskytujících služby IKT.

Článek 33
Obecná šetření

1. Aby mohl provádět své povinnosti podle tohoto nařízení, může hlavní orgán dohledu s pomocí vyšetřovacího týmu podle čl. 34 odst. 1 provádět nezbytná šetření třetích stran poskytujících služby IKT:

2. Hlavní orgán dohledu je oprávněn:

(a) zkoumat záznamy, údaje, postupy a jakékoli jiné materiály, které mají význam pro plnění jeho úkolů, a to bez ohledu na nosič, na němž jsou uchovávány;

(b) pořizovat nebo získávat ověřené kopie takových záznamů, údajů, postupů a jiných materiálů nebo výpisy z nich;

(c) předvolat zástupce třetí strany poskytující služby IKT a požádat jej o ústní nebo písemné vysvětlení skutečností nebo o dokumenty, které se týkají předmětu a účelu šetření, a odpovědi zaznamenat;

(d) vyslechnout jakoukoli jinou fyzickou nebo právnickou osobu, která s tím souhlasí, za účelem získání informací souvisejících s předmětem šetření;

(e) požadovat výpisy telefonních hovorů a datových přenosů.

3. Úředníci hlavního orgánu dohledu a další osoby tímto orgánem pověřené pro účely šetření podle odstavce 1 vykonávají své pravomoci na základě vyhotovení písemného pověření, v němž je uveden předmět a účel šetření.

V tomto pověření se rovněž uvedou opakované pokuty podle čl. 31 odst. 4, nebudou-li předloženy požadované záznamy, údaje, postupy nebo jakékoliv jiné materiály nebo odpovědi na otázky položené zástupcům třetí strany poskytující služby IKT, nebo nebudou-li úplné.

4. Zástupci třetích stran poskytujících služby IKT se musí šetření nařízenému rozhodnutím hlavního orgánu dohledu podrobit. V rozhodnutí musí být uvedeny

předmět a účel šetření, pokuty stanovené v čl. 31 odst. 4, opravné prostředky, které jsou k dispozici podle nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010, a právo na přezkum rozhodnutí Soudním dvorem.

5. Hlavní orgán dohledu s dostatečným předstihem před šetřením informuje příslušné orgány finančních subjektů využívajících tuto třetí stranou poskytující služby IKT o šetření a o totožnosti pověřených osob.

Článek 34
Kontroly na místě

1. Aby mohl provádět své povinnosti podle tohoto nařízení, může hlavní orgán dohledu s pomocí vyšetřovacího týmu podle čl. 35 odst. 1 provádět všechny nezbytné kontroly na místě ve všech prostorách, na všech pozemcích nebo ve všech budovách využívaných k podnikatelské činnosti třetích stran poskytujících služby IKT, jako jsou jejich sídla, provozní střediska, druhotná pracoviště, a rovněž může provádět kontroly na dálku.

2. Úředníci a další osoby pověřené hlavním orgánem dohledu prováděním kontrol na místě mohou vstupovat do všech prostor, na všechny pozemky a do všech budov využívaných k podnikatelské činnosti a jsou oprávněni po dobu kontroly a v rozsahu pro kontrolu nezbytném zapečetit jakékoliv takové prostory a účetní knihy nebo záznamy.

   Své pravomoci vykonávají na základě vystaveného písemného pověření uvádějícího předmět a účel kontroly a opakované pokuty podle čl. 31 odst. 4, pokud se zástupci dotčených třetích stran poskytujících služby IKT kontrole nepodrobí.

3. Hlavní orgán dohledu informuje s dostatečným předstihem před kontrolou příslušné orgány finančních subjektů využívajících tuto třetí stranu poskytující služby IKT.

4. Kontroly se týkají všech relevantních systémů IKT, sítí, zařízení, informací a dat používaných nebo přispívajících k poskytování služeb finančním subjektům.

5. Hlavní orgán dohledu před jakoukoliv plánovanou návštěvou na místě zašle kritickým třetím stranám poskytujícím služby IKT oznámení v dostatečném předstihu, ledaže takové oznámení není možné v důsledku naléhavé nebo krizové situace, nebo pokud by způsobilo, že by již kontrola nebo audit nebyly účinné.

6. Kritická třetí strana poskytující služby IKT se podrobí kontrolám na místě nařízeným rozhodnutím hlavního orgánu dohledu. V rozhodnutí musí být uvedeny předmět a účel kontroly, datum, kdy má být kontrola zahájena, pokuty stanovené v čl. 31 odst. 4, opravné prostředky, které jsou k dispozici podle nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010, a dále právo na přezkum rozhodnutí Soudním dvorem.

7. Jestliže úředníci nebo jiné osoby pověřené hlavním orgánem dohledu zjistí, že kritická třetí strana poskytující služby IKT odmítá podrobit se kontrole nařízené podle tohoto článku, hlavní orgán dohledu informuje kritického poskytovatele IKT o důsledcích tohoto odporu, včetně možnosti, že příslušné orgány dotčených finančních subjektů ukončí smluvní ujednání uzavřená s touto kritickou třetí stranou poskytující služby IKT.

Článek 35

Průběžný dohled

1. Hlavnímu orgánu dohledu je při provádění obecných šetření nebo kontrol na místě nápomocen vyšetřovací tým vytvořený pro každou kritickou třetí stranu poskytující služby IKT.

2. Společný vyšetřovací tým uvedený v odstavci 1 bude tvořit maximálně 10 členů z řad pracovníků hlavního orgánu dohledu a příslušných orgánů dohledu nad finančními subjekty, jimž daná kritická třetí strana poskytující služby IKT dodává své služby, kteří se budou podílet na přípravách a provádění činností dohledu. Všichni členové společného vyšetřovacího týmu musí mít odborné znalosti v oboru rizik v oblasti IKT a operačních rizik. Práci společného vyšetřovacího týmu řídí určený pracovník evropského orgánu dohledu („koordinátor hlavního orgánu dohledu“).

3. Evropské orgány dohledu prostřednictvím společného výboru vypracují společný návrh regulačních technických norem, které se budou podrobněji zabývat jmenováním členů společného vyšetřovacího týmu z příslušných kompetentních orgánů a rovněž úkoly a organizací práce vyšetřovacího týmu. Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do [*Úř. věst.: vložte datum 1 rok od data vstupu v platnost*].

   Na Komisi je přenesena pravomoc přijímat regulační technické normy uvedené v prvním pododstavci v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

4. Hlavní orgán dohledu do 3 měsíců po dokončení šetření nebo kontroly na místě a po konzultaci s fórem dohledu přijme doporučení, která budou adresována kritické třetí straně poskytující služby IKT podle pravomocí uvedených v článku 31.

5. Doporučení uvedená v odstavci 4 budou neprodleně sdělena kritické třetí straně poskytující služby IKT a příslušným orgánům finančních subjektů, jimž dodává služby.

   Pro účely plnění činností dohledu může hlavní orgán dohledu přihlédnout ke všem relevantním osvědčením třetích stran a interním nebo externím auditním zprávám třetích stran v oblasti IKT předloženým kritickou třetí stranou poskytující služby IKT.

Článek 36

Harmonizace podmínek umožňujících provádění dohledu

1. Evropské orány dohledu prostřednictvím společného výboru vypracují návrh regulačních technických norem, které stanoví:

   (a) informace, jež mají být předloženy kritickou třetí stranou poskytující služby IKT v žádosti o dobrovolnou účast podle čl. 28 odst. 8;

   (b) obsah a formát zpráv, které mohou být vyžádány pro účely čl. 31 odst. 1 písm. c);

(c) podmínky pro předkládání informací, včetně struktury, formátů a postupů, které bude muset kritická třetí strana poskytující služby IKT předložit, zveřejnit nebo nahlásit podle čl. 31 odst. 1;

(d) podrobnosti o vyhodnocení opatření přijatých kritickými třetími stranami poskytujícími služby IKT na základě doporučení hlavního orgánu dohledu podle čl. 37 odst. 2 příslušnými orgány.

2. Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do 1. ledna 20xx [*Úř. věst.: vložte datum 1 rok od data vstupu v platnost*].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených v prvním pododstavci v souladu s postupem podle článků 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

Článek 37

Následná opatření příslušných orgánů

1. Kritické třetí strany poskytující služby IKT do 30 kalendářních dnů od přijetí doporučení vydaných hlavním orgánem dohledu podle čl. 31 odst. 1 písm. d) oznámí hlavnímu orgánu dohledu, zda mají v úmyslu se těmito doporučeními řídit. Hlavní orgány dohledu tuto informaci neprodleně předají příslušným orgánům.

2. Příslušné orgány sledují, zda finanční subjekty zohledňují rizika uvedená v doporučeních adresovaných hlavním orgánem dohledu kritickým třetím stranám poskytujícím služby IKT podle čl. 31 odst. 1 písm. d).

3. Příslušné orgány mohou v souladu s článkem 44 požádat finanční subjekty, aby částečně či úplně přestaly využívat služby dodávané kritickou třetí stranou poskytující služby IKT, a to do doby, kdy kritické třetí strany poskytující služby IKT odstraní rizika uvedená v jim adresovaných doporučeních. Bude-li to nutné, mohou finanční subjekty požádat, aby zcela či zčásti ukončily příslušná smluvní ujednání uzavřená s dotčenými kritickými třetími stranami poskytujícími služby IKT.

4. Příslušné orgány při přijímání rozhodnutí podle odstavce 3 zohlední druh a rozsah rizik, která kritická třetí strana poskytující služby IKT neodstranila, a rovněž závažnost porušení předpisů, přičemž přihlédnou k těmto kritériím:

(a) závažnosti a délce trvání porušení předpisů;

(b) zda porušení předpisů odhalilo závažná slabá místa v postupech, řídicích systémech, řízení rizik a interních kontrolních prostředků kritické třetí strany poskytující služby IKT;

(c) zda porušení předpisů usnadnilo či umožnilo spáchání finančního trestného činu nebo zda lze takový trestný čin danému porušení jakýmkoliv jiným způsobem přičíst;

(d) zda k porušení předpisů došlo úmyslně nebo z nedbalosti.

5. Příslušné orgány pravidelně informují hlavní orgán dohledu o přístupech a opatřeních přijatých v rámci jejich pracovních úkolů týkajících se finančních subjektů a rovněž o jimi podniknutých smluvních opatřeních v případech, kdy kritická třetí strana poskytující služby IKT zcela či zčásti nepřistoupila k doporučením hlavních orgánů dohledu.

Článek 38

Poplatky za dohled

1. Evropské orgány dohledu naúčtují kritickým třetím stranám poskytujícím služby IKT poplatky, které budou plně pokrývat nezbytné výdaje těchto orgánů v souvislosti s prováděním pracovních úkolů dohledu podle tohoto nařízení, a to včetně uhrazení veškerých nákladů, jež mohou vzniknout v důsledku činnosti příslušných orgánů podílejících se na činnostech dohledu podle článku 35.

   Částka poplatku účtovaného kritické třetí straně poskytující služby IKT bude zahrnovat všechny administrativní výdaje a bude poměrná k obratu poskytovatele služeb IKT.

2. Komisi je svěřena pravomoc přijmout akt v přenesené pravomoci v souladu s článkem 50, kterým doplní toto nařízení stanovením výše poplatků a způsobu jejich placení.

Článek 39

Mezinárodní spolupráce

1. EBA, ESMA a EIOPA mohou v souladu s článkem 33 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010, respektive (EU) č. 1095/2010 pro účely posílení mezinárodní spolupráce ohledně rizik v oblasti IKT spojených s třetími stranami v různých finančních odvětvích uzavírat administrativní ujednání s regulačními orgány a orgány dohledu třetích zemí, a to zejména při práci na osvědčených postupech pro přezkum postupů, kontrolních prostředků, zmírňujících opatření a reakce na incidenty souvisejících s řízením rizik v oblasti IKT.

2. Evropské orgány dohledu každých pět let předloží prostřednictvím společného výboru Evropskému parlamentu, Radě a Komisi společnou důvěrnou zprávu shrnující závěry z relevantních jednání s orgány třetích zemí podle odstavce 1, které budou zaměřeny na vývoj rizik v oblasti IKT spojených s třetími stranami a dopady na finanční stabilitu, integritu trhu, ochranu investorů nebo fungování jednotného trhu.

KAPITOLA VI

UJEDNÁNÍ O SDÍLENÍ INFORMACÍ

Článek 40

Ujednání o sdílení operativních a jiných informací o kybernetických hrozbách

1. Finanční subjekty si mohou mezi sebou vyměňovat operativní a jiné informace o kybernetických hrozbách, včetně ukazatelů narušení, taktiky, technik a postupů, výstrah v oblasti kybernetické bezpečnosti a konfiguračních nástrojů, pokud se toto sdílení operativních a jiných informací:

   (a) zaměřuje na zlepšení digitální provozní odolnosti finančních subjektů, zejména zvyšováním povědomí o kybernetických hrozbách, omezení nebo zabránění možností šíření těchto hrozeb, podporu rozsahu obraných prostředků finančních subjektů, techniky detekce hrozeb, zmírňující strategie nebo fáze reakce a obnovy provozu;

   (b) odehrává v důvěryhodných komunitách finančních subjektů;

(c) provádí prostřednictvím ujednání o sdílení informací chránících potenciálně citlivou povahu sdílených informací, která se řídí pravidly chování plně respektujícími důvěrnou povahu obchodních informací, ochranu osobních údajů[48] a dodržování pokynů týkajících se hospodářské soutěže[49].

2. Ujednání o sdílení informací musí pro účely odst. 1 písm. c) stanovit podmínky spolupráce a případně podrobnosti o zapojení veřejných orgánů a jejich možné způsobilosti k účasti na ujednáních o sdílení informací a rovněž o provozních prvcích, včetně použití specializovaných IT platforem.

3. Finanční subjekty informují příslušné orgány o své účasti na ujednáních o sdílení informací uvedených v odstavci 1 po ověření jejich členství, nebo případně ukončení jejich členství, jakmile vstoupí v platnost.

KAPITOLA VII

PŘÍSLUŠNÉ ORGÁNY

Článek 41

Příslušné orgány

Aniž jsou dotčena ustanovení o rámci dohledu pro poskytovatele služeb IKT z řad třetích stran uvedená v kapitole V oddílu II tohoto nařízení, dodržování povinností stanovených tímto nařízením zajišťují v souladu se svými pravomocemi udělenými příslušnými právními akty tyto příslušné orgány:

(a) v případě úvěrových institucí příslušný orgán stanovený v souladu s článkem 4 směrnice 2013/36/EU, aniž jsou dotčeny zvláštní úkoly svěřené nařízením (EU) č. 1024/2013 ECB;

(b) v případě poskytovatelů platebních služeb příslušný orgán určený v souladu s článkem 22 směrnice (EU) 2015/2366;

(c) v případě institucí elektronických peněz příslušný orgán určený v souladu s článkem 37 směrnice 2009/110/ES;

(d) v případě investičních podniků příslušný orgán určený v souladu s článkem 4 směrnice (EU) 2019/2034;

(e) v případě poskytovatelů služeb souvisejících s kryptoaktivy, vydavatelů kryptoaktiv, vydavatelů tokenů vázaných k vlastnictví aktiv a vydavatelů významných tokenů vázaných k vlastnictví aktiv příslušný orgán určený podle čl. 3 odst. 1 písm. ee) první odrážky [*nařízení (EU) 20xx, nařízení MICA*];

(f) v případě centrálních depozitářů cenných papírů příslušný orgán určený v souladu s článkem 11 nařízení (EU) č. 909/2014;

(g) v případě ústředních protistran příslušný orgán určený v souladu s článkem 22 nařízení (EU) č. 648/2012;

---

[48] V souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

[49] Sdělení Komise – Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci, 2011/C 11/01.

(h) v případě obchodních systémů a poskytovatelů služeb hlášení údajů příslušný orgán určený v souladu s článkem 67 směrnice 2014/65/EU;

(i) v případě registrů obchodních údajů příslušný orgán určený v souladu s článkem 55 nařízení (EU) č. 648/2012;

(j) v případě správců alternativních investičních fondů příslušný orgán určený v souladu s článkem 44 směrnice 2011/61/ES;

(k) v případě správcovských společností příslušný orgán určený v souladu s článkem 97 směrnice 2009/65/ES;

(l) v případě pojišťoven a zajišťoven příslušný orgán určený v souladu s čl. 30 směrnice 2009/138/ES;

(m) v případě zprostředkovatelů pojištění, zprostředkovatelů zajištění a zprostředkovatelů doplňkového pojištění příslušný orgán určený v souladu s článkem 12 směrnice (EU) 2016/97;

(n) v případě institucí zaměstnaneckého penzijního pojištění příslušný orgán určený v souladu s článkem 47 směrnice 2016/2341;

(o) v případě ratingových agentur příslušný orgán určený v souladu s článkem 21 nařízení (ES) č. 1060/2009;

(p) v případě statutárních auditorů a auditorských společností příslušný orgán určený v souladu s čl. 3 odst. 2 a článkem 32 směrnice 2006/43/ES;

(q) v případě správců kritických referenčních hodnot příslušný orgán určený v souladu s články 40 a 41 *nařízení xx/202x;*

(r) v případě poskytovatelů služeb skupinového financování příslušný orgán určený v souladu s *článkem x nařízení xx/202x;*

(s) v případě registrů sekuritizací příslušný orgán určený v souladu s článkem 10 a čl. 14 odst. 1 nařízení (EU) č. 2017/2402.

Článek 42

Spolupráce se strukturami a orgány zřízenými směrnicí (EU) 2016/1148

1. Aby se usnadnila spolupráce a umožnila výměna v oblasti dohledu mezi příslušnými orgány stanovenými tímto nařízením a skupinou pro spolupráci vytvořenou podle článku 11 směrnice (EU) 2016/1148, mohou evropské orgány dohledu a příslušné orgány požádat o přizvání k činnostem skupiny pro spolupráci.

2. Příslušné orgány se mohou ve vhodných případech obrátit na jednotné kontaktní místo a vnitrostátní bezpečnostní týmy typu CSIRT uvedené v článcích 8 a 9 směrnice (EU) 2016/1148.

Článek 43

Cvičení, komunikace a spolupráce ve finančním sektoru

1. Evropské orgány dohledu mohou prostřednictvím společného výboru a ve spolupráci s příslušnými orgány, ECB a ESRB vytvářet mechanismy umožňující sdílení osvědčených postupů ve finančních odvětvích, které zlepší znalost situace a identifikují společná kybernetická zranitelná místa a rizika napříč odvětvími.

Mohou připravovat cvičení v oblastech krizového řízení a reakce na nepředvídané události zahrnující scénáře kybernetického útoku, jejichž cílem bude rozvoj komunikačních kanálů a postupné umožnění účinné koordinované reakce na úrovni EU v případě závažného přeshraničního incidentu souvisejícího s IKT nebo související hrozby se systémovým dopadem na celý finanční sektor Unie.

Tato cvičení mohou podle potřeby rovněž testovat závislosti finančního sektoru na dalších hospodářských odvětvích.

2. Příslušné orgány, EBA, ESMA nebo EIOPA a ECB při plnění svých povinností podle článků 42 až 48 vzájemně úzce spolupracují a vyměňují si informace. Úzce koordinují svůj dohled za účelem zjišťování případů porušení tohoto nařízení a jejich nápravy, rozvoje a prosazování osvědčených postupů, usnadňování spolupráce, prosazování jednotnosti výkladu a poskytování hodnocení napříč jurisdikcemi v případě jakékoli neshody.

Článek 44

Správní sankce a nápravná opatření

1. Příslušné orgány disponují všemi kontrolními, vyšetřovacími a sankčními pravomocemi nezbytnými k plnění svých povinností podle tohoto nařízení.

2. Pravomoci podle odstavce 1 zahrnují přinejmenším tyto pravomoci:

   (a) mít přístup k jakémukoli dokumentu nebo údajům uloženým v jakékoli formě, kterou příslušný orgán považuje za vhodnou pro výkon svých úkolů, a obdržet nebo pořídit jejich kopii;

   (b) provádět kontroly na místě nebo vyšetřování;

   (c) požadovat opravná a nápravná opatření v případě porušení požadavků tohoto nařízení.

3. Aniž je dotčeno jejich právo ukládat trestní sankce podle článku 46, členské státy přijmou pravidla stanovící vhodné správní sankce a nápravná opatření pro případy porušení tohoto nařízení a zajistí jejich účinné uplatňování.

   Tyto sankce nebo opatření musí být účinné, přiměřené a odrazující.

4. Členské státy delegují na příslušné orgány pravomoc k uplatňování alespoň následujících správních sankcí nebo nápravných opatření v případech porušení tohoto nařízení:

   (a) vydat příkaz požadující, aby fyzická nebo právnická osoba jednání ukončila nebo aby takové jednání neopakovala;

   (b) požadovat dočasné nebo trvalé ukončení veškeré praxe nebo všech jednání, jež příslušné orgány považují za odporující ustanovením tohoto nařízení, a zabránění opakování této praxe nebo tohoto jednání;

   (c) přijmout jakákoliv opatření, včetně pokut, zajišťujících, že budou finanční subjekty nadále dodržovat požadavky právních předpisů;

   (d) v rozsahu povoleném vnitrostátním právem vyžadovat existující záznamy o datovém provozu uchovávané telekomunikačním operátorem, jestliže existuje důvodné podezření na porušení tohoto nařízení a jestliže tyto záznamy mohou být relevantními podklady pro vyšetřování porušení tohoto nařízení; a

(e) vydávat veřejná oznámení, včetně veřejných oznámení uvádějících totožnost fyzických či právnických osob a povahu jejich porušení.

5. Pokud se ustanovení uvedená v odst. 2 písm. c) a v odstavci 4 použijí na právnické osoby, svěří členské státy příslušným orgánům pravomoc uplatňovat správní sankce a nápravná opatření, s výhradou podmínek stanovených ve vnitrostátním právu, na členy vedoucího orgánu a na další osoby, které nesou podle vnitrostátního práva odpovědnost za dané porušení.

6. Členské státy zajistí, aby veškerá rozhodnutí o uložení správních sankcí nebo nápravných opatření uvedených v odst. 2 písm. c) byla řádně odůvodněna a aby bylo možné podat proti nim opravný prostředek.

Článek 45

Výkon pravomoci ukládat správní sankce a jiná nápravná opatření

1. Příslušné orgány vykonávají pravomoc ukládat správní sankce a nápravná opatření podle článku 44 v souladu se svým vnitrostátním právním řádem:

(a) přímo;

(b) ve spolupráci s jinými orgány;

(c) na svou odpovědnost přenesením na jiné orgány;

(d) podáním návrhu příslušným soudním orgánům.

2. Příslušné orgány při stanovení druhu a míry správní sankce nebo nápravného opatření uloženého podle článku 44 zohledňují, do jaké míry bylo porušení předpisů způsobeno úmyslně nebo z nedbalosti, a všechny ostatní relevantní okolnosti, případně včetně:

(a) závažnosti, účinků a doby trvání porušení;

(b) stupně odpovědnosti fyzické nebo právnické osoby odpovědné za porušení;

(c) finanční síly odpovědné fyzické nebo právnické osoby;

(d) důležitosti zisků nebo ztrát, které odpovědná fyzická nebo právnická osoba získala nebo kterým předešla, pokud je možné je stanovit;

(e) ztrát třetích stran způsobených porušením, pokud je lze stanovit;

(f) míry spolupráce odpovědné fyzické nebo právnické osoby s příslušným orgánem, aniž je dotčena nutnost zajistit vydání zisku realizovaného touto osobou nebo ztrát, kterým se vyhnula;

(g) předchozích porušení ze strany odpovědné fyzické nebo právnické osoby.

Článek 46

Trestní sankce

1. Členské státy se mohou rozhodnout, že nestanoví pravidla pro správní sankce nebo nápravná opatření za ta porušení předpisů, na která se podle jejich vnitrostátního práva vztahují trestní sankce.

2. Pokud se členské státy rozhodly stanovit za porušení tohoto nařízení trestní sankce, zajistí, aby byla zavedena vhodná opatření k tomu, aby příslušné orgány měly veškeré pravomoci nezbytné ke spolupráci s orgány činnými v trestním řízení

v rámci své jurisdikce, aby mohly získat konkrétní informace týkající se trestního vyšetřování či řízení zahájeného pro porušení předpisů uvedená v tomto nařízení a předat tyto informace ostatním příslušným orgánům a rovněž orgánům EBA, ESMA nebo EIOPA, aby splnily svou povinnost spolupráce pro účely tohoto nařízení.

Článek 47

Oznamovací povinnosti

Členské státy oznámí právní a správní předpisy k provedení této kapitoly včetně všech relevantních trestněprávních ustanovení Komisi a orgánům ESMA, EBA a EIOPA do [*OJ: vložte datum 1 rok po datu vstupu v platnost*]. Dále Komisi a orgánům ESMA, EBA a EIOPA bez zbytečného odkladu oznámí veškeré následné změny těchto předpisů.

Článek 48

Zveřejňování správních sankcí

1. Příslušné orgány zveřejňují na svých oficiálních webových stránkách bez zbytečného prodlení všechna rozhodnutí, jimiž se ukládají správní sankce, proti nimž není možné odvolání, jakmile se subjekt, jemuž byla sankce uložena, dozví o tomto rozhodnutí.

2. Uveřejnění uvedené v odstavci 1 zahrnuje informace o druhu a povaze porušení předpisů, totožnosti odpovědných osob a uložených sankcích.

3. Bude-li se příslušný orgán na základě posouzení jednotlivých případů domnívat, že by zveřejnění totožnosti u právnických osob nebo totožnosti a osobních údajů u fyzických osob nebylo přiměřené, že by ohrožovalo stabilitu finančních trhů nebo vedení probíhajícího vyšetřování trestného činu, nebo způsobilo, pokud by bylo možné určit totožnost dotčených osob, těmto osobám nepřiměřené škody, přijme ohledně rozhodnutí o uložení správních sankcí některé z těchto řešení:

   (a) odloží jeho zveřejnění až do okamžiku, kdy pominou všechny důvody pro nezveřejnění;

   (b) zveřejní je anonymně v souladu s vnitrostátním právem; nebo

   (c) je nezveřejní, budou-li možnosti uvedené v písmenech a) a b) považovány za nedostatečné k zajištění, že nebude nijak ohrožena stabilita finančních trhů, nebo bude-li toto zveřejnění disproporční k mírné povaze ukládané sankce.

4. V případě rozhodnutí zveřejnit správní sankci anonymně podle odst. 3 písm. b) může být zveřejnění příslušných údajů odloženo.

5. Pokud příslušný orgán uveřejní rozhodnutí o uložení správní sankce, vůči němuž je podán opravný prostředek k příslušným soudním orgánům, příslušné orgány tuto informaci ihned uvedou na svých oficiálních webových stránkách spolu s případnými následnými informacemi o výsledku řízení o tomto opravném prostředku zjištěných v pozdějších fázích. Rovněž se uveřejní jakékoli soudní rozhodnutí, kterým se rozhodnutí o uložení správní sankce ruší.

6. Příslušné orgány zajistí, aby jakékoli zveřejnění podle odstavců 1 až 4 zůstalo na jejich oficiálních webových stránkách po dobu nejméně pěti let od zveřejnění. Osobní údaje, jež taková zveřejněná informace obsahuje, jsou na oficiálních webových stránkách uchovávány pouze po nezbytnou dobu, v souladu s platnými předpisy o ochraně údajů.

Článek 49

Služební tajemství

1. Na veškeré důvěrné informace obdržené, vyměněné nebo předané podle tohoto nařízení se vztahují podmínky služebního tajemství stanovené v odstavci 2.

2. Povinnost zachovávat služební tajemství se vztahuje na všechny osoby, které pracují nebo pracovaly pro příslušné orgány podle tohoto nařízení či jakýkoli orgán nebo podnik na trhu či pro fyzickou nebo právnickou osobu, na niž příslušné orgány přenesly své pravomoci, včetně auditorů a odborníků smluvně najatých těmito orgány.

3. Informace, na něž se vztahuje služební tajemství, nesmějí být sděleny žádné jiné osobě nebo orgánu, vyjma na základě ustanovení unijního či vnitrostátního práva.

4. Veškeré informace vyměněné mezi příslušnými orgány podle tohoto nařízení, které se týkají obchodních nebo provozních podmínek a jiných ekonomických či osobních záležitostí, jsou považovány za důvěrné a podléhají služebnímu tajemství s výjimkou případů, kdy příslušný orgán v okamžiku jejich sdělení uvede, že informace mohou být zpřístupněny, nebo kdy je takovéto zpřístupnění nutné pro účely soudního řízení.

KAPITOLA VIII

AKTY V PŘENESENÉ PRAVOMOCI

Článek 50

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v čl. 28 odst. 3 a čl. 38 odst. 2 je svěřena Komisi na dobu pěti let od [OP: vložte datum 5 let od data vstupu tohoto nařízení v platnost].

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 28 odst. 3 a čl. 38 odst. 2 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Před přijetím aktu v přenesené pravomoci Komise vede konzultace s odborníky jmenovanými jednotlivými členskými státy v souladu se zásadami stanovenými v interinstitucionální dohodě ze dne 13. dubna 2016 o zdokonalení tvorby právních předpisů.

5. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

6. Akt v přenesené pravomoci přijatý podle čl. 28 odst. 3 a čl. 38 odst. 2 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky

ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

KAPITOLA IX

PŘECHODNÁ A ZÁVĚREČNÁ USTANOVENÍ

ODDÍL I

Článek 51

Ustanovení o přezkumu

Do [*OP: vložte datum 5 let od data vstupu tohoto nařízení v platnost*] Komise po konzultaci s EBA, ESMA, EIOPA a ESRB, podle okolností, provede přezkum a předloží zprávu Evropskému parlamentu a Radě, k níž bude případně připojen legislativní návrh týkající se kritérií určování kritických poskytovatelů služeb IKT z řad třetích stran v čl. 28 odst. 2.

ODDÍL II

ZMĚNY

Článek 52

Změna nařízení (ES) č. 1060/2009

V příloze I nařízení (ES) č. 1060/2009 se v bodě 4 oddílu A první pododstavec nahrazuje tímto:

„Ratingová agentura používá řádné administrativní a účetní postupy, mechanismy vnitřní kontroly, účinné postupy hodnocení rizik a účinná kontrolní a ochranná opatření pro řízení systémů IKT v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/xx* [DORA].

* Nařízení Evropského parlamentu a Rady (EU) 2021/xx […] (Úř. věst. L XX, DD.MM.RRRR, s. X).“.

Článek 53

Změny nařízení (EU) č. 648/2012

Nařízení (EU) č. 648/2012 se mění takto:

(1) článek 26 se mění takto:

(a) odstavec 3 se nahrazuje tímto:

„3. Ústřední protistrana musí mít a provozovat organizační strukturu, která zajišťuje nepřetržitý a řádný výkon jejích služeb a činností. Musí využívat vhodné a přiměřené systémy, zdroje a postupy, včetně systémů

IKT řízených v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/xx* [DORA].

* Nařízení Evropského parlamentu a Rady (EU) 2021/xx […] (Úř. věst. L XX, DD.MM.RRRR, s. X).“;

(b) odstavec 6 se zrušuje;

(2) článek 34 se mění takto:

(a) odstavec 1 se nahrazuje tímto:

„1. Ústřední protistrana zavede, provádí a udržuje vhodnou politiku pro zachování provozu a plán obnovy činnosti po havárii, který zahrnuje plán zachování provozu IKT a plán obnovy činnosti po havárii IKT vypracované v souladu s nařízením (EU) 2021/xx [DORA], s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění povinností ústřední protistrany.“;

(b) v odstavci 3 se první pododstavec nahrazuje tímto:

„K zajištění jednotného uplatňování tohoto článku vypracuje ESMA po konzultaci s členy ESCB návrhy regulačních technických norem, které blíže určují minimální obsah politiky zachování provozu a plánu obnovy činnosti po havárii a požadavky na ně, vyjma plánu zachování provozu IKT a plánu obnovy činnosti po havárii IKT.“;

(3) v čl. 56 odst. 3 se první pododstavec nahrazuje tímto:

„3. Za účelem zajištění jednotného uplatňování tohoto článku vypracuje ESMA návrhy regulačních technických norem, které blíže určují náležitosti žádosti o registraci uvedené v odstavci 1 kromě požadavků týkajících se řízení rizik v oblasti IKT.“;

(4) v článku 79 se odstavce 1 a 2 nahrazují tímto:

„1. Registr obchodních údajů určí zdroje operačního rizika a minimalizuje je rovněž prostřednictvím rozvoje vhodných systémů, kontrol a postupů, včetně systémů IKT řízených v souladu s nařízením (EU) 2021/xx *[DORA*].

2. Registr obchodních údajů stanoví, provádí a dodržuje vhodnou politiku pro zachování provozu a plán obnovy činnosti po havárii, včetně plánu zachování provozu IKT a plánu obnovy činnosti po havárii IKT vypracovaných v souladu s nařízením (EU) 2021/xx*[DORA]*, s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění svých povinností.“;

(5) v článku 80 se zrušuje odstavec 1.

Článek 54

Změny nařízení (EU) č. 909/2014

Článek 45 nařízení (EU) č. 909/2014 se mění takto:

(1) odstavec 1 se nahrazuje tímto:

„1. Centrální depozitář určí vnitřní i vnější zdroje operačního rizika a minimalizuje jejich dopad rovněž prostřednictvím rozvoje vhodných nástrojů, procesů a strategií IKT zavedených a řízených v souladu s nařízením Evropského parlamentu a Rady (EU) 2021/xx*[*DORA*] a rovněž pomocí jakýchkoli jiných vhodných nástrojů, kontrol a postupů pro jiné druhy operačních rizik, mimo jiné pro všechny vypořádací systémy, které provozuje.

* Nařízení (EU) 2021/xx Evropského parlamentu a Rady […] (Úř. věst. L XX, DD.MM.RRRR, s. X).“;

(2) odstavec 2 se zrušuje;

(3) odstavce 3 a 4 se nahrazují tímto:

„3. Pro služby, které poskytuje, jakož i pro každý vypořádací systém, který provozuje, centrální depozitář vypracuje, zavede a udržuje odpovídající strategii zajištění kontinuity provozu a plán obnovy provozu po havárii, včetně plánu zajištění kontinuity provozu IKT a obnovy provozu po havárii IKT v souladu s nařízením (EU) 2021/xx [DORA], aby zajistil zachování služeb, včasnou obnovu provozu a plnění povinností centrálního depozitáře v případě událostí, které představují významné riziko narušení provozu.

4. Plán uvedený v odstavci 3 musí zajistit obnovení všech obchodů a pozic účastníků k okamžiku narušení provozu, aby mohli účastníci centrálního depozitáře s jistotou pokračovat v činnosti a dokončit vypořádání v plánovaný den, mimo jiné zajištěním toho, aby kritické systémy informačních technologií mohly obnovit provoz od okamžiku jeho narušení, jak je stanoveno v čl. 11 odst. 5 a 7 nařízení (EU) 2021/xx [DORA].“;

(4) v odstavci 6 se první pododstavec nahrazuje tímto:

„Centrální depozitář určí, sleduje a řídí rizika, která pro jeho provoz mohou představovat hlavní účastníci vypořádacích systémů, které provozuje, jakož i poskytovatelé služeb a technické infrastruktury, jiní centrální depozitáři nebo jiné subjekty tržní infrastruktury. Na žádost poskytne příslušným a dotčeným orgánům informace o každém takto určeném riziku. Centrální depozitář rovněž příslušný orgán a dotčené orgány neprodleně informuje o všech provozních incidentech z těchto rizik vyplývajících, kromě incidentů souvisejících s riziky v oblasti IKT.“;

(5) v odstavci 7 se první pododstavec nahrazuje tímto:

„Orgán ESMA vypracuje v úzké spolupráci s členy ESCB návrhy regulačních technických norem upřesňujících operační rizika uvedená v odstavcích 1 a 6, kromě rizik v oblasti IKT, metody testování, řešení nebo minimalizace těchto rizik, včetně strategie zajištění kontinuity provozu a plánu obnovy provozu po havárii uvedených v odstavcích 3 a 4, a metody jejich posuzování.“.

Článek 55

Změny nařízení (EU) č. 600/2014

Nařízení (EU) č. 600/2014 se mění takto:

(1) článek 27g se mění takto:

(a) odstavec 4 se zrušuje;

(b) v odstavci 8 se písmeno c) nahrazuje tímto:

(c) „c) konkrétní organizační požadavky stanovené v odstavcích 3 a 5.“;

(2) článek 27h se mění takto:

(a) odstavec 5 se zrušuje;

(b) v odstavci 8 se písmeno e) nahrazuje tímto:

„e) konkrétní organizační požadavky stanovené v odstavci 4.“;

(3) článek 27i se mění takto:

(a) odstavec 3 se zrušuje;

(b) v odstavci 5 se písmeno b) nahrazuje tímto:

„b) konkrétní organizační požadavky stanovené v odstavcích 2 a 4.“.

Článek 56

Vstup v platnost a použitelnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Použije se ode dne [*OP: vložte datum – 12 měsíců po datu vstupu v platnost*].

Články 23 a 24 se však použijí od [*OP: vložte datum – 36 měsíců od data vstupu tohoto nařízení v platnost*].

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda/předsedkyně	*předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Povaha návrhu/podnětu

1.4. Cíle

1.5. Odůvodnění návrhu/podnětu

1.6. Doba trvání a finanční dopad návrhu/podnětu

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systémy řízení a kontroly

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

3.2.2. Odhadovaný dopad na operační prostředky

3.2.3. Odhadovaný dopad na lidské zdroje

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

Příloha

Obecné předpoklady

Pravomoci dohledu

LEGISLATIVNÍ FINANČNÍ VÝKAZ „AGENTURY“

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru.

1.2. Příslušné oblasti politik

Oblast politiky: Finanční stabilita, finanční služby a unie kapitálových trhů

Činnost: Digitální provozní odolnost

1.3. Tento návrh se týká

☑ **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci**[50]

☐ **prodloužení stávající akce**

☐ sloučení **jedné či více akcí do jiné/nové akce**

1.4. Cíle

1.4.1. Obecné cíle

Obecným cílem tohoto podnětu je posílení digitální provozní odolnosti subjektů finančního sektoru EU pomocí harmonizace a aktualizace stávajících pravidel a předložení nových požadavků v případech nedostatků. Tím by se rovněž zlepšil jednotný soubor pravidel týkající se jeho digitálního rozměru.

Celkový cíl je možné rozdělit na tři obecné cíle: (1) snížení rizika finančního narušení a nestability, (2) snížení administrativního zatížení a zvýšení účinnosti dohledu a (3) zvýšení ochrany spotřebitelů a investorů.

1.4.2. Specifické cíle

Návrh má tyto specifické cíle:

komplexnější řešení rizik v oblasti informačních a komunikačních technologií („IKT“) a posílení celkové úrovně digitální odolnosti finančního sektoru;

harmonizace hlášení incidentů souvisejících s IKT a řešení požadavků na hlášení překrytí;

umožnění přístupu finančního dohledu k informacím o incidentech souvisejících s IKT;

zajištění, aby finanční subjekty, kterých se tento návrh týká, posoudily účinnost svých preventivních opatření a opatření v oblasti odolnosti a identifikovaly slabá místa související s IKT;

snížení roztříštěnosti jednotného trhu a umožnění přeshraničního schvalování výsledků testování;

[50] Uvedené v čl. 58 odst. 2 písm. a) nebo b) finančního nařízení.

posílení smluvních záruk pro finanční subjekty při využívání služeb IKT, včetně pravidel pro externí zajišťování (upravujících sledování třetích stran poskytujících služby IKT); umožnění dohledu nad činnostmi kritických třetích stran poskytujících služby IKT; motivace k výměně operativních informací o hrozbách ve finančním sektoru.

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Akt o digitální provozní odolnosti pro finanční sektor by zajistil komplexní rámec pokrývající všechny aspekty digitální provozní odolnosti a účinně by přispěl ke zlepšení celkové provozní odolnosti finančního sektoru. Zajistil by přehlednost a soudržnost v rámci jednotného souboru pravidel.

Rovněž by zajistil vyšší srozumitelnost a soudržnost vzájemné reakce se směrnicí o opatřeních k zajištění vysoké společné úrovně bezpečnosti (NIS) a jejími revizemi. Objasnil by finančním subjektům různá pravidla pro digitální provozní odolnost, která musí dodržovat, zejména v případě finančních subjektů s více oprávněními a působícími na různých trzích v rámci EU.

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele pro sledování pokroku a dosažených výsledků.

Možné ukazatele:

počet incidentů souvisejících s IKT ve finančním sektoru EU a jejich dopad

počet závažných incidentů souvisejících s IKT nahlášených orgánům obezřetnostního dohledu

počet finančních subjektů, jež budou vyžadovat provedení penetračních testů na základě hrozeb

počet finančních subjektů využívajících při uzavírání smluvních ujednání se třetími stranami poskytujícími služby IKT standardní smluvní doložky

počet kritických třetích stran poskytujících služby IKT, na něž dohlíží evropské orgány dohledu / orgány obezřetnostního dohledu

počet finančních subjektů podílejících se na sdílení řešení v oblasti operativních informací o hrozbách

počet orgánů dostávajících hlášení o stejném incidentu souvisejícím s IKT

počet přeshraničních penetračních testů na základě hrozeb

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Finanční sektor ve velké míře spoléhá na informační a komunikační technologie (IKT). Přes významný pokrok v důsledku cílené politiky a legislativní iniciativy na vnitrostátní i evropské úrovni představují rizika v oblasti IKT problém pro provozní odolnost, výkonnost a stabilitu finančního systému EU. Reforma, která následovala po finanční krizi z roku 2008, primárně posílila finanční odolnost finančního sektoru EU a zaměřovala se na zajištění konkurenceschopnosti EU a stability z hlediska ekonomiky, obezřetnosti a chování trhu. Zabezpečení IKT a digitální odolnost jsou součástí operačních rizik, ovšem regulatorní agenda po krizi se jim věnovala méně a rozvíjely se pouze v některých oblastech strategického a regulatorního rámce finančních služeb EU, nebo pouze v několika málo členských státech. To představuje následující výzvy, které by měl návrh řešit:

Právní rámec pro rizika v oblasti IKT a provozní odolnosti ve finančním sektoru je roztříštěný a není zcela soudržný.

Nedostatečně konzistentní požadavky na hlášení incidentů souvisejících s IKT způsobují, že mají orgány dohledu neúplný přehled o povaze, četnosti, významu a dopadu těchto incidentů.

Některé finanční subjekty se potýkají se složitými, překrývajícími se a potenciálně nekonzistentními požadavky na hlášení téhož incidentu souvisejícího s IKT.

Nedostatečné sdílení informací a spolupráce v oblasti operativních informací o kybernetických hrozbách na strategické, taktické a provozní úrovni brání jednotlivým finančním subjektům vhodně posuzovat, sledovat, bránit se a reagovat na kybernetické hrozby.

V některých finančních pododvětvích může existovat několik nekoordinovaných rámců pro penetrační testování a testování odolnosti, k nimž se přidává neuznávání výsledků v jiných státech, zatímco v jiných odvětvích tyto testovací rámce zcela chybí.

Nedostatečný přehled orgánů dohledu o činnostech finančních subjektů, které jsou zajišťovány třetími stranami poskytujícími služby IKT, vystavují jednotlivé finanční subjekty a celý finanční systém operačním rizikům.

Orgány finančního dohledu nedisponují dostatečnými pravomocemi ani nástroji ke sledování a řízení rizik koncentrace a systémových rizik vyplývajících z toho, že finanční subjekty spoléhají na třetí strany v oblasti IKT.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Důvody pro akci na evropské úrovni (ex ante):

Digitální provozní odolnost je otázkou společného zájmu finančních trhů EU. Akce na úrovni EU by přinesla více výhod a měla by větší smysl než samostatné akce na úrovni států. Jestliže by nebyla doplněna tato provozní ustanovení o rizicích v oblasti IKT, pak by jednotný soubor pravidel poskytoval nástroje k řešení všech dalších druhů rizik na evropské úrovni, ale netýkal by se aspektů digitální provozní odolnosti, nebo by se tyto aspekty řídily roztříštěnými a nekoordinovanými iniciativami na úrovni států. Tento návrh by zajistil právní srozumitelnost ohledně možností a způsobu uplatňování ustanovení o digitální provozní odolnosti, zejména v případě přeshraničních finančních subjektů, a členské státy by nemusely jednotlivě zlepšovat pravidla, normy a předpoklady týkající se provozní odolnosti a kybernetické bezpečnosti jako reakci na stávající omezenou platnost pravidel EU a obecnou povahu směrnice NIS.

Očekávaná vytvořená přidaná hodnota na úrovni Unie (ex post):

Zásah Unie by významně zvýšil účinnost této strategie a současně by omezil složitost a snížil finanční a administrativní zatížení všech finančních subjektů. Harmonizoval by hluboce propojenou a integrovanou oblast hospodářství, která již těží z jednotného souboru pravidel a dohledu. Pokud jde o hlášení incidentů souvisejících s IKT, návrh by omezil zatížení – a tedy i náklady – způsobené hlášeními téhož incidentu souvisejícího s IKT různým orgánům EU a/nebo členských států. Rovněž usnadní vzájemné uznávání/přijímání výsledků testování u přeshraničně působících subjektů, jež jsou regulovány několika testovacími rámci v různých členských státech.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Nová iniciativa

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

Cíl tohoto návrhu je v souladu s několika dalšími strategiemi a probíhajícími iniciativami EU, zejména směrnicí o opatřeních k zajištění vysoké společné úrovně bezpečnosti (NIS) a směrnicí o určování a označování evropských kritických infrastruktur (EKI). Tento návrh by zachoval výhody spojené s horizontálním rámcem pro kybernetickou bezpečnost, protože zachová tři finanční pododvětví v rámci platnosti směrnice NIS. Protože orgány finančního dohledu zůstanou v ekosystému NIS, budou moci si vyměňovat relevantní informace s orgány NIS a účastnit se jednání skupiny pro spolupráci NIS. Návrh nedopadá na směrnici NIS, spíše z ní vychází a řeší případná překrytí pomocí výjimky *lex specialis*. Interakce mezi nařízením o finančních službách a směrnicí NIS by se nadále řídila doložkou *lex specialis*, tedy vynětím finančních subjektů z podstatných požadavků směrnice NIS a zabráněním překrývání se těchto dvou aktů. Dále by měl být tento návrh v souladu se směrnicí o určování a označování evropských kritických infrastruktur (EKI), která je nyní revidována za účelem zlepšení ochrany a odolnosti kritických infrastruktur před jinými než kybernetickými hrozbami.

Tento návrh by neměl mít dopad na víceletý finanční rámec (VFR). Zaprvé, rámec dohledu nad kritickými třetími poskytovateli IKT bude plně financován poplatky vybíranými od těchto poskytovatelů; zadruhé, další regulační úkoly související s digitální provozní odolnosti delegované na evropské orgány dohledu zajistí interní přeložení stávajících pracovníků.

To se promítne do návrhu, který má zvýšit počet oprávněných pracovníků agentury během budoucího ročního rozpočtového procesu. Agentura bude pokračovat v práci směřující k maximalizaci součinnosti a efektivity (mimo jiné prostřednictvím informačních systémů) a úzce sledovat dodatečnou pracovní zátěž související s tímto návrhem, což se promítne do úrovně počtu oprávněných pracovníků požadovaných agenturou v rámci ročního rozpočtového procesu.

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Bylo zváženo několik možností financování:

Zaprvé, dodatečné náklady lze uhradit obvyklými finančními mechanismy evropských orgánů dohledu. To by ovšem znamenalo podstatné zvýšení příspěvku EU pro finanční prostředky evropských orgánů dohledu.

Tato možnost byla zvolena kvůli nákladům souvisejícím s regulačními úkoly souvisejícími s tímto návrhem. Fakticky budou evropské orgány dohledu požádány, aby přeřadily stávající pracovníky na vypracování množství technických norem. Ovšem vícenáklady související s dohledem nad kritickými třetími stranami poskytujícími služby nebude možné financovat přesunutím prostředků v rámci evropských orgánů dohledu, které mají i jiné úkoly než úkoly předpokládané podle tohoto návrhu a také dalších právních předpisů Unie. Kromě toho úkoly dohledu související s digitální provozní odolností vyžadují konkrétní technické a odborné znalosti. Protože je současná výše těchto prostředků v evropských orgánech dohledu nedostatečná, jsou nutné další prostředky.

Konečně budou podle tohoto návrhu od kritických třetích stran poskytujících služby IKT podléhajících dohledu vybírány poplatky. Ty budou určeny k pokrytí všech dodatečných zdrojů nutných k provádění nových úkolů a pravomocí evropských orgánů dohledu.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ **omezená doba trvání**

☐ Návrh/podnět s platností od [DD/MM]RRRR do [DD/MM]RRRR

☐ Finanční dopad od RRRR do RRRR

☑ **časově neomezená doba trvání**

Provádění s obdobím rozběhu od 2021

poté plné fungování.

1.7. Předpokládaný způsob řízení[51]

Přímé řízení Komisí prostřednictvím

☐ výkonných agentur.

☐ **Sdílené řízení** s členskými státy

☑ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

☐ mezinárodní organizace a jejich agentury (upřesněte);

☐EIB a Evropský investiční fond;

☐ subjekty uvedené v článcích 70 a 71;

☐ veřejnoprávní subjekty;

☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky;

☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky;

☐ osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

Poznámky

neuvedeno

[51] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

V souladu s již existujícími opatřeními zpracovávají evropské orgány dohledu pravidelné zprávy o své činnosti (včetně podávání interních zpráv vrcholnému vedení, podávání zpráv správním radám a zpracování výročních zpráv) a podrobují se auditům využívání zdrojů a výkonnosti, které vykonává Účetní dvůr a Útvar interního auditu Komise. Sledování a podávání zpráv o opatřeních uvedených v návrhu bude v souladu s již existujícími požadavky i s novými požadavky vyplývajícími z návrhu.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Řízení bude prováděno nepřímo prostřednictvím evropských orgánů dohledu. Mechanismus financování bude uplatňován prostřednictvím poplatků vybíraných od dotčených kritických třetích stran poskytujících služby IKT.

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Pokud jde o právní, ekonomické, efektivní a účinné využití prostředků na základě návrhu, očekává se, že návrh nepřinese nová vážná rizika, která by nebyla kryta stávajícím rámcem pro vnitřní kontrolu. Nový problém se ovšem může týkat zajišťování včasného výběru poplatků od dotčených kritických třetích stran poskytujících služby IKT.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Systémy řízení a kontroly stanovené v nařízení o evropských orgánech dohledu jsou již zavedeny. Evropské orgány dohledu úzce spolupracují s Útvarem interního auditu Komise, aby se zajistilo, že ve všech oblastech rámce vnitřní kontroly budou dodržovány vhodné standardy. Tyto požadavky se budou vztahovat i na roli evropských orgánů podle současného návrhu. Kromě toho Evropský parlament na doporučení Rady každý rozpočtový rok uděluje každému evropskému orgánu dohledu absolutorium za plnění jeho rozpočtu.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Pro účely boje proti podvodům, korupci a jiné protiprávní činnosti se na evropské orgány dohledu bez jakéhokoli omezení uplatňují ustanovení nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF).

Evropské orgány dohledu mají specializovanou strategii boje proti podvodům a z ní vycházející akční plán. Posílená činnost evropských orgánů dohledu v oblasti boje proti podvodům bude slučitelná s pravidly a pokyny stanovenými finančním nařízením (opatření pro boj proti podvodům jako součást řádného finančního řízení), s politikou boje proti podvodům úřadu OLAF, s ustanoveními strategie Komise proti podvodům (KOM(2011) 376), jakož i s ustanoveními společného přístupu k decentralizovaným subjektům EU (červenec 2012) a souvisejícího plánu.

Kromě toho nařízení, kterým jsou evropské orgány dohledu zřízeny, jakož i finanční nařízení týkající se evropských orgánů dohledu obsahují ustanovení o plnění a kontrole rozpočtů evropských orgánů dohledu a použitelná finanční pravidla včetně pravidel týkajících se zamezení podvodům a nesrovnalostem.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Počet	RP/NRP[52].	ze zemí ESVO[53]	z kandidátských zemí[54]	z třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení

Nové rozpočtové položky, jejichž vytvoření se požaduje

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Počet	RP/NRP	ze zemí ESVO	z kandidátských zemí	z třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení

[52] RP = rozlišené prostředky / NRP = nerozlišené prostředky.

[53] ESVO: Evropské sdružení volného obchodu.

[54] Kandidátské země a případně potenciální kandidáti ze západního Balkánu.

3.2. Odhadovaný dopad na výdaje

3.3. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	Počet	Kód

GŘ: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**CELKEM**
	Závazky	(1)									
	Platby	(2)									
Prostředky CELKEM pro GŘ <>	Závazky										
	Platby										

Okruh víceletého finančního rámce		

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2022	2023	2024	2025	2026	2027	**CELKEM**
GŘ pro								
• Lidské zdroje								
• Ostatní správní výdaje<>								
GŘ CELKEM	Prostředky							

Prostředky CELKEM v rámci OKRUHU víceletého finančního rámce	(Závazky celkem = platby celkem)							

v milionech EUR (zaokrouhleno na tři desetinná místa), stálé ceny

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**CELKEM**
Prostředky CELKEM v OKRUHU 1 víceletého finančního rámce	Závazky							
	Platby							

3.3.1. Odhadovaný dopad na operační prostředky

☑ Návrh/podnět nevyžaduje využití operačních prostředků.

☐ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa) stálé ceny

Uveďte cíle a výstupy ⇩			2022		2023		2024		2025		2026		2027		**CELKEM**	
	VÝSTUPY															
	Druh[55]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Celkové náklady
SPECIFICKÝ CÍL č. 1[56] …																
– Výsledek																
Mezisoučet za specifický cíl č. 1																
SPECIFICKÝ CÍL č. 2 …																
– Výsledek																
Mezisoučet za specifický cíl č. 2																
CELKOVÉ NÁKLADY																

[55] Výsledky jsou dodávané produkty a služby (např.: počet financovaných výměn studentů, počet postavených km silnic atd.).

[56] Popsaný v bodě 1.4.2. „Specifické cíle…“.

3.3.2. Odhadovaný dopad na lidské zdroje

3.3.2.1. Shrnutí

☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

☑ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa), stálé ceny

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**CELKEM**
Dočasní zaměstnanci (třídy AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Dočasní zaměstnanci (třídy AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Smluvní zaměstnanci							
Vyslaní národní odborníci							
CELKEM	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Požadavky na zaměstnance (FTE):

EBA, EIOPA, ESMA a EEA	2022	2023	2024	2025	2026	2027	**CELKEM**
Dočasní zaměstnanci (třídy AD) EBA = 5, EIOPA = 5, ESMA = 5	15	15	15	15	15	15	15
Dočasní zaměstnanci (třídy AST) EBA = 1, EIOPA = 1, ESMA = 1	3	3	3	3	3	3	3
Smluvní zaměstnanci							
Vyslaní národní odborníci							
CELKEM	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Odhadované potřeby lidských zdrojů pro (mateřské) GŘ

☑ Návrh/podnět nevyžaduje využití lidských zdrojů.

☐ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v celých číslech (nebo zaokrouhlete nejvýše na jedno desetinné místo)

		2022	2023	2024	2025	2026	2027
• **Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)**							
• **Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)**[57]							
XX 01 02 01 (SZ, VNO, ZAP z celkového rámce)							
XX 01 02 02 (SZ, MZ, VNO, ZAP a MOD při delegacích)							
XX 01 04 ***yy***[58]	– v ústředí[59]						
	– při delegacích						
XX 01 05 02 (AC, END, INT – v nepřímém výzkumu)							
10 01 05 02 (SZ, ZAP, VNO – v přímém výzkumu)							
Jiné rozpočtové položky (upřesněte)							
CELKEM							

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	
Externí zaměstnanci	

Popis výpočtu nákladů na jednotky FTE by měl být zahrnut v příloze V oddílu 3.

[57] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[58] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

[59] Zejména pro strukturální fondy, Evropský zemědělský fond pro rozvoj venkova (EZFRV) a Evropský rybářský fond (ERF).

3.3.3. Slučitelnost se stávajícím víceletým finančním rámcem

☑ Návrh/podnět je v souladu se stávajícím víceletým finančním rámcem.

☐ Návrh/podnět si vyžádá úpravu příslušného okruhu víceletého finančního rámce.

☐ Návrh/podnět vyžaduje použití nástroje pružnosti nebo změnu víceletého finančního rámce[60].

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky. […]

3.3.4. Příspěvky třetích stran

☐ Návrh/podnět nepočítá se spolufinancováním od třetích stran.

☑ Návrh/podnět počítá se spolufinancováním podle následujícího odhadu:

v milionech EUR (zaokrouhleno na tři desetinná místa)

EBA

	2022	2023	2024	2025	2026	2027	Celkem
Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Spolufinancované prostředky CELKEM	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Celkem
Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Spolufinancované prostředky CELKEM	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Celkem

[60] Viz články 11 a 17 nařízení Rady (EU, Euratom) č. 1311/2013, kterým se stanoví víceletý finanční rámec na období let 2014–2020.

[61] 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.

[62] 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.

Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Spolufinancované prostředky CELKEM	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Odhadovaný dopad na příjmy

☑ Návrh/podnět nemá žádný finanční dopad na příjmy.

☑ Návrh/podnět má tento finanční dopad:

☑ na vlastní zdroje

☐ na jiné příjmy

☑ uveďte, zda je příjem účelově vázán na výdajové položky

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[64]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek ……								

U účelově vázaných různých příjmů upřesněte dotčené výdajové rozpočtové položky.

[…]

Upřesněte způsob výpočtu dopadu na příjmy.

[…]

63 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.

64 Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.

PŘÍLOHA

Obecné předpoklady

Hlava I – Výdaje na zaměstnance

Při výpočtu výdajů na zaměstnance podle níže vysvětlených identifikovaných požadavků na zaměstnance byly použity tyto konkrétní předpoklady:

- Další zaměstnanci přijatí v roce 2022 jsou vzhledem k předpokládanému času nutnému na nábor dalších zaměstnanců v nákladech započítáni za 6 měsíců
- Průměrné roční náklady na dočasného zaměstnance činí 150 000 EUR, v nichž je zahrnuto 25 000 EUR nákladů na „zajištění prostředků“ (budovy, IT atd.)
- Opravné koeficienty platné pro mzdy zaměstnanců v Paříži (EBA a ESMA) a Frankfurtu (EIOPA) činí 117,7 a 99,4
- Příspěvky zaměstnavatele na důchodové pojištění dočasných zaměstnanců vychází ze standardních základních mezd zahrnutých ve standardních průměrných ročních nákladech, tj. 95 660 EUR
- Další dočasní zaměstnanci patří do tříd AD5 a AST.

Hlava II – Infrastruktura a provozní výdaje

Náklady vychází z vynásobení počtu zaměstnanců podle poměrné části roku v zaměstnání standardními náklady na „zajištění prostředků“, tj. 25 000 EUR.

Hlava III – Provozní výdaje

Náklady jsou odhadovány na základě těchto předpokladů:

- Náklady na překlady jsou u jednotlivých evropských orgánů dohledu stanoveny na 350 000 EUR
- Předpokládá se, že se ve dvou letech 2022 a 2023 uplatní v jednotlivých evropských orgánech dohledu jednorázové náklady na IT ve výši 500 000 EUR, které se rozdělí po 50 %. Roční náklady na údržbu se pro rok 2024 odhadují v jednotlivých evropských orgánech dohledu na 50 000 EUR
- Roční náklady na kontroly na místě se odhadují v jednotlivých evropských orgánech dohledu na 200 000 EUR

Výsledkem výše uvedených odhadů jsou tyto roční náklady:

Okruh víceletého finančního rámce	Počet	

Stálé ceny

EBA:			2022	2023	2024	2025	2026	2027	**CELKEM**
Hlava 1:	Závazky	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Platby	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Hlava 2:	Závazky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Závazky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Prostředky CELKEM pro EBA	Závazky	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Platby	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**CELKEM**
Hlava 1:	Závazky	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Platby	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Hlava 2:	Závazky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Závazky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

Prostředky CELKEM pro EIOPA	Závazky	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Platby	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**CELKEM**
Hlava 1:	Závazky	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Platby	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Hlava 2:	Závazky	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Platby	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Hlava 3:	Závazky	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Platby	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
Prostředky CELKEM pro ESMA	Závazky	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Platby	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Návrh vyžaduje využití operačních prostředků, jak je vysvětleno dále:

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa) stálé ceny

EBA

Uveďte cíle a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[65]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Celkové náklady
SPECIFICKÝ CÍL č. 1[66] Přímý dohled nad kritickými třetími stranami poskytujícími služby IKT																
– Výsledek				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Mezisoučet za specifický cíl č. 1																
SPECIFICKÝ CÍL č. 2 …																
– Výsledek																
Mezisoučet za specifický cíl č. 2																
CELKOVÉ NÁKLADY				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Uveďte cíle a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[67]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Celkové náklady
SPECIFICKÝ CÍL č. 1[68] Přímý dohled nad kritickými třetími stranami poskytujícími služby IKT																
– Výsledek				0,800		0,800		0,600		0,600		0,600		0,600		4,000

[65] Výsledky jsou dodávané produkty a služby (např.: počet financovaných výměn studentů, počet postavených km silnic atd.).

[66] Popsaný v bodě 1.4.2. „Specifické cíle…“.

[67] Výsledky jsou dodávané produkty a služby (např.: počet financovaných výměn studentů, počet postavených km silnic atd.).

[68] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Mezisoučet za specifický cíl č. 1														
SPECIFICKÝ CÍL č. 2 …														
– Výsledek														
Mezisoučet za specifický cíl č. 2														
CELKOVÉ NÁKLADY		**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Uveďte cíle a výstupy ⇩			2022		2023		2024		2025		2026		2027			
	VÝSTUPY															
	Druh[69]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Celkové náklady
SPECIFICKÝ CÍL č. 1[70] Přímý dohled nad kritickými třetími stranami poskytujícími služby IKT																
– Výsledek				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Mezisoučet za specifický cíl č. 1																
SPECIFICKÝ CÍL č. 2 …																
– Výsledek																
Mezisoučet za specifický cíl č. 2																
CELKOVÉ NÁKLADY				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Výsledky jsou dodávané produkty a služby (např.: počet financovaných výměn studentů, počet postavených km silnic atd.).

[70] Popsaný v bodě 1.4.2. „Specifické cíle…“.

Činnosti dohledu jsou plně financovány poplatky vybíranými od subjektů, nad nimiž je vykonáván dohled, a to následovně:

EBA

	2022	2023	2024	2025	2026	2027	Celkem
Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Spolufinancované prostředky CELKEM	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Celkem
Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Spolufinancované prostředky CELKEM	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Celkem
Tyto náklady budou ze 100 % financovány poplatky vybranými od subjektů, nad nimiž je vykonáván dohled[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Spolufinancované prostředky CELKEM	1,373	1,948	1,748	1,748	1,748	1,748	10,313

KONKRÉTNÍ INFORMACE

Přímé pravomoci dohledu

[71] 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.
[72] 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.
[73] 100 % celkových odhadovaných nákladů plus všechny penzijní příspěvky zaměstnavatelů.

Na úvod je třeba připomenout, že subjekty podléhající přímému dohledu ESMA budou platit poplatky orgánu ESMA (jednorázové náklady na registraci a opakované náklady za průběžný dohled). Platí to pro ratingové agentury (viz nařízení Komise v přenesené pravomoci (EU) č. 272/2012) a registry obchodních údajů (nařízení Komise v přenesené pravomoci (EU) č. 1003/2013).

Podle tohoto legislativního návrhu budou evropské orgány dohledu pověřeny novými úkoly zaměřenými na sbližování dohledových přístupů k rizikům v oblasti IKT spojeným s třetími stranami ve finančním sektoru tím, že se na kritické třetí strany poskytující služby IKT bude vztahovat rámec dohledu Unie.

Rámec dohledu podle tohoto návrhu vychází ze stávající institucionální architektury v oblasti finančních služeb, přičemž společný výbor evropských orgánů dohledu zajistí v souladu se svými úkoly v oblasti kybernetické bezpečnosti koordinaci ohledně všech záležitostí rizik v oblasti IKT, v tom mu pomůže příslušný podvýbor (Fórum dohledu) provádějící přípravné práce pro individuální rozhodnutí a kolektivní doporučení určená kritickým poskytovatelům služeb IKT, kteří jsou třetími stranami.

Prostřednictvím tohoto rámce získají evropské orgány dohledu stanovené jako hlavní orgány dohledu pro jednotlivé kritické třetí strany poskytující služby IKT pravomoci zajistit, aby byli poskytovatelé technologických služeb, kteří hrají kritickou úlohu ve fungování finančního sektoru, v celé Evropě příslušným způsobem sledováni. Povinnosti v oblasti dohledu jsou uvedeny v tomto návrhu a podrobně vysvětleny v důvodové zprávě. Zahrnují práva požadovat všechny relevantní informace a dokumentaci pro provádění šetření a kontrol, zasílat doporučení a následně předkládat zprávy o přijatých opatřeních nebo uplatněných nápravných opatřeních při realizaci těchto doporučení.

Aby bylo možné provádět nové úkoly předpokládané v tomto návrhu, evropské orgány dohledu přijmou další zaměstnance specializované na rizika v oblasti IKT a zaměřující se na posuzování závislostí na třetích stranách.

Nezbytné lidské zdroje je možné u jednotlivých orgánů odhadnout na 6 FTE (5AD a 1 AST podporující AD). Evropským orgánům dohledu rovněž vzniknou další náklady na IT, které se odhadují na 500 000 EUR (jednorázové náklady) a rovněž 50 000 EUR ročně pro každý ze tří evropských orgánů dohledu na náklady na údržbu. Jedním z důležitých prvků při plnění nových úkolů jsou cíle provádění kontrol a auditů na místě, jejichž náklady lze pro každý evropský orgán dohledu odhadnout na 200 000 EUR ročně. Do řádku provozních výdajů jsou zahrnuty také náklady na překlady různých dokumentů, které evropské orgány dohledu obdrží od kritických třetích stran poskytujících služby IKT, jež činí 350 000 EUR ročně.

Všechny výše uvedené administrativní náklady budou v plné výši financovány z ročních poplatků vybíraných evropskými orgány dohledu od kritických třetích stran poskytujících služby IKT, nad nimiž bude vykonáván dohled (bez dopadu na rozpočet EU).