Evropský parlament
2019-2024

Dokument ze zasedání

A9-0341/2021

7.12.2021

***I
ZPRÁVA

o návrhu 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Hospodářský a měnový výbor

Zpravodaj: Billy Kelleher

Vysvětlivky

*	Postup konzultace
***	Postup souhlasu
***I	Řádný legislativní postup (první čtení)
***II	Řádný legislativní postup (druhé čtení)
***III	Řádný legislativní postup (třetí čtení)

(Druh postupu závisí na právním základu navrženém v návrhu aktu.)

Pozměňovací návrhy k návrhu aktu

Pozměňovacích návrhy Parlamentu předložené ve dvou sloupcích

Vypuštění textu je označeno ***tučnou kurzivou*** v levém sloupci. Nahrazení je označeno ***tučnou kurzivou*** v obou sloupcích. Nový text je označen ***tučnou kurzivou*** v pravém sloupci.

První a druhý řádek záhlaví každého pozměňovacího návrhu označují příslušnou část projednávaného návrhu aktu. Pokud se pozměňovací návrh týká existujícího aktu, který má být návrhem aktu pozměněn, je v záhlaví mimo to na třetím řádku uveden existující akt a na čtvrtém řádku ustanovení existujícího aktu, kterého se pozměňovací návrh týká.

Pozměňovací návrhy Parlamentu v podobě konsolidovaného textu

Nové části textu jsou označeny ***tučnou kurzivou***. Vypuštěné části textu jsou označeny symbolem ▌ nebo přeškrtnuty. Nahrazení se vyznačují tak, že nový text se označí ***tučnou kurzivou*** a nahrazený text se vymaže nebo přeškrtne. Výjimečně se neoznačují změny výlučně technické povahy, které provedly příslušné útvary za účelem vypracování konečného znění.

OBSAH

Strana

NÁVRH LEGISLATIVNÍHO USNESENÍ EVROPSKÉHO PARLAMENTU 5

POSTUP V PŘÍSLUŠNÉM VÝBORU 91

JMENOVITÉ KONEČNÉ HLASOVÁNÍ V PŘÍSLUŠNÉM VÝBORU 92

NÁVRH LEGISLATIVNÍHO USNESENÍ EVROPSKÉHO PARLAMENTU

o návrhu 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
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Řádný legislativní postup: první čtení)

Evropský parlament,

– s ohledem na návrh Komise předložený Evropskému parlamentu a Radě (COM(2020)0595),

– s ohledem na čl. 294 odst. 2 a článek 114 Smlouvy o fungování Evropské unie, v souladu s nimiž Komise předložila svůj návrh Parlamentu (C9-0304/2020),

– s ohledem na čl. 294 odst. 3 Smlouvy o fungování Evropské unie,

– s ohledem na stanovisko Evropského hospodářského a sociálního výboru...[1],

– s ohledem na článek 59 jednacího řádu,

– s ohledem na zprávu Hospodářského a měnového výboru (A9-0341/2021),

1. přijímá níže uvedený postoj v prvním čtení;

2. vyzývá Komisi, aby věc znovu postoupila Parlamentu, jestliže svůj návrh nahradí jiným textem, podstatně jej změní nebo má v úmyslu jej podstatně změnit;

3. pověřuje svého předsedu, aby předal postoj Parlamentu Radě a Komisi, jakož i vnitrostátním parlamentům.

[1] Úř. věst. C 155,.30.4.2021, s. 38.

Pozměňovací návrh 1

POZMĚŇOVACÍ NÁVRHY EVROPSKÉHO PARLAMENTU*

k návrhu Komise

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[2],

s ohledem na stanovisko Evropského hospodářského a sociálního výboru,[3]

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. Základní charakteristiku veškeré činnosti finančních subjektů Unie tvoří všudypřítomné používání systémů IKT a vysoká míra digitalizace a propojení, avšak dostatečnou digitální odolnost jejich provozních rámců ***je nutné*** teprve vytvořit.

(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.

---

* Pozměňovací návrhy: nový text či text nahrazující původní znění je označen tučně a kurzivou; vypuštění textu je označeno symbolem ▌.

[2][doplňte odkaz] Úř. věst C , , s. .

[3]Úř. věst. L 155, 30.4.2021, s. 38.

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, ▌správy pohledávek a činnosti provozních útvarů. ***Díky používání IKT došlo také k transformaci pojišťovnictví, od vzniku zprostředkovatelů digitálního pojištění, kteří využívají technologie v oblasti pojišťovnictví, přes upisování pojištění až po distribuci smluv.*** 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[4] potvrdila, jak stávající vysoká míra vzájemného 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[5] 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. ***V důsledku toho je nutné pohlížet na riziko v oblasti IKT v kontextu výrazně propojeného celosvětového finančního systému, v jehož rámci je nutné dávat přednost jednotnosti mezinárodní regulace a spolupráci mezi příslušnými orgány na celém světě.***

(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

[4] Zpráva ESRB – Systémová kybernetická rizika, únor 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[5] 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.

strategického a regulatorního rámce finančních služeb Unie nebo jen v několika málo členských státech.

(6) Akční plán Komise pro finanční technologie z roku 2018[6] 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 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 posílení mandátů orgánů finančního dohledu k ***řízení rizik souvisejících s IKT*** ve finančnictví ***s cílem zajistit integritu a účinnost jednotného trhu a jeho řádné fungování***.

(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

[6] 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.

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.

(10a) Základním předpokladem účinného sběru údajů o rizicích a vykazování rizik, jež jsou nezbytné pro řádné a udržitelné řízení rizik a rozhodovací procesy úvěrových institucí, je také vytvoření odpovídající infrastruktury sítí a informačních systémů a jejich udržování. V roce 2013 zveřejnil Basilejský výbor pro bankovní dohled (BCBS) na základě dvou zastřešujících principů správy a infrastruktury IT soubor zásad týkajících se účinného sběru údajů o rizicích a vykazování rizik (BCBS 239), který měl být zaveden začátkem roku 2016. Podle zprávy Evropské centrální banky (ECB) z května 2018 o tematickém přezkumu účinného sběru údajů o rizicích a vykazování rizik a zprávy o pokroku Basilejského výboru pro bankovní dohled z dubna 2020 byl pokrok při provádění dosažený globálními systémově významnými bankami neuspokojivý a vyvolával znepokojení. S cílem usnadnit dodržování těchto zásad a zajistit jejich soulad s mezinárodními normami by měla Komise v úzké spolupráci s ECB a po konzultaci s orgánem EBA a ESRB vypracovat hodnotící zprávu, v níž by posoudila, jak jsou zásady BCBS 239 propojeny s ustanoveními tohoto nařízení, a případně jak by tyto zásady měly být začleněny do právních předpisů Unie.

(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. ***Záměrem této iniciativy je také zvýšit povědomí o rizicích v oblasti IKT a uvědomit si, že incidenty týkající se IKT a nedostatečná provozní odolnost mohou ohrozit finanční stabilitu finančních subjektů.***

(13) Finanční subjekty by měly při řešení rizik v oblasti IKT postupovat stejně a dodržovat stejná pravidla založená na zásadách***, a to v závislosti na své velikosti, povaze, komplexnosti a na svém rizikovém profilu***. Konzistentnost přispívá ke zvýšení důvěry ve finanční systém a zachování jeho stability, zejména v době***, kdy se velmi spoléháme na*** IKT systémy, platformy a infrastrukturu s vyšším digitálním rizikem.

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.

(14a) Provádění tohoto nařízení by však nemělo bránit inovacím, pokud jde o způsob, jak finanční subjekty řeší otázky digitální provozní odolnosti při dodržování jeho ustanovení, ani pokud jde o služby, které nabízejí, nebo služby IKT poskytované třetími stranami.

(15) Kromě právních předpisů o finančních službách je současným hlavním rámcem kybernetické bezpečnosti na úrovni Unie směrnice Evropského parlamentu a Rady (EU) 2016/1148[7]. 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.

(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 ***v případě finančních subjektů*** *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

[7] 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).

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. ***Společný orgán dohledu, hlavní orgány dohledu a*** příslušné orgány podle tohoto nařízení by rovněž měly konzultovat a spolupracovat s vnitrostátními skupinami CSIRT uvedenými v článku 9 směrnice (EU) 2016/1148.

Toto nařízení by navíc mělo zajistit, aby byly síti CSIRT zřízené směrnicí (EU) 2016/1148 poskytnuty podrobné informace o závažných incidentech souvisejících s IKT.

(18) Je rovněž důležité zajistit soulad ***jak*** 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, ***tak i se směrnicí týkající se odolnosti kritických subjektů***, které mají možný dopad na finanční sektor[8].

(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***, přičemž jak hmotněprávní, tak i procesní požadavky, které se podle tohoto nařízení vztahují na kritické poskytovatele služeb IKT z řad třetích stran, by měly být v souladu s požadavky platnými v rámci uvedené směrnice***. 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 ***i v rámci jedné skupiny***. Je třeba zvýšit práh digitální provozní odolnosti finančního systému a současně umožnit proporcionální uplatňování požadavků***, a to s přihlédnutím k jejich povaze, velikosti, komplexnosti a celkovému rizikovému profilu***.

[8] 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).

(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)[9] 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.

(21a) Za účelem omezení administrativní zátěže, složitosti a duplicitních ohlašovacích povinností u poskytovatelů platebních služeb, kteří spadají do působnosti tohoto nařízení, by měly přestat platit požadavky týkající se hlášení incidentů uvedené ve směrnici (EU) 2015/2366. Úvěrové instituce, instituce elektronických peněz a platební instituce by tak podle tohoto nařízení měly hlásit veškeré provozní nebo bezpečnostní incidenty spojené s platbami i ty, které s platbami spojeny nejsou, jež se dříve hlásily podle směrnice (EU) 2015/2366, nehledě na to, zda mají tyto incidenty spojitost s IKT.

(22) Aby mohly příslušné orgány plnit své dohledové funkce získáním úplného přehledu o povaze, četnosti, významu a dopadu incidentů souvisejících s IKT a aby se zlepšila výměna informací mezi relevantními veřejnými orgány, včetně donucovacích orgánů a orgánů příslušných k řešení krize, je nutné stanovit pravidla, která by umožnila ***vybudovat propracovaný*** režim hlášení incidentů souvisejících s IKT s požadavky, jež ***by zaplnily mezery v odvětvových*** právních předpisech týkajících se finančních ***služeb***, 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 svým příslušným orgánům ***na základě jednotného účinného rámce stanoveného v tomto nařízení***. 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, ***a někdy*** nekoordinovaných, vnitrostátních rámcích, které řeší stejné otázky různým způsobem. To vede ke zdvojování nákladů pro přeshraniční finanční subjekty a ***mohlo by bránit*** vzájemnému 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

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

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.

(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[10], 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

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

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 činností poskytovatelů služeb IKT z řad třetích stran, kteří ***poskytují*** kritické ***služby*** finančním subjektům. ***Vzhledem k tomu, že poskytování služeb v oblasti IKT v rámci skupiny nepředstavuje stejné riziko, neměli by být poskytovatelé služeb IKT, kteří jsou součástí téže skupiny nebo téhož interinstitucionálního systému ochrany, definováni jako kritičtí poskytovatele služeb IKT z řad třetích stran.***

(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. ***S cílem vytvořit otevřený systém výměny operativních informací a zajistit přístup „bezpečnost již od fáze návrhu“, které jsou velmi důležité z hlediska zajištění větší operační odolnosti a připravenosti finančního odvětví, pokud jde o rizika spojená s IKT, je proto důležité upevnit dohody o spolupráci a podávání zpráv mezi finančními subjekty a příslušnými orgány a dále poskytování informací veřejnosti. Ujednání o sdílení informací by měla vždy náležitě zohledňovat potenciální rizika související s kybernetickou bezpečností, ochranou údajů nebo obchodním tajemstvím.***

(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. ***Je proto důležité posílit tyto komunikační kanály a v nezbytných a relevantních případech získat informace od orgánů, které nejsou orgány dohledu, a to v průběhu celého cyklu dohledu.***

(32) Finanční subjekty by měly být ***rovněž*** 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[11] pro ochranu hospodářské soutěže a rovněž způsobem zaručujícím úplné dodržování předpisů Unie

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

pro ochranu osobních údajů, zejména nařízení Evropského parlamentu a Rady (EU) 2016/679[12], 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, ***včetně požadavků rámce pro řízení rizik***, zohledňovat výrazné rozdíly ve velikosti, ***povaze, komplexnosti a rizikovém profilu***. 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, ***povahy, komplexnosti,*** podnikatelského profilu ***a relativního rizikového profilu***, 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, 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 ***odhadovaných*** nákladů a ztrát způsobených ***závažným*** narušením IKT ***a závažnými incidenty souvisejícími s IKT*** a hlášení výsledků přezkumů po ***takových*** 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

[12] 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).

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[13], podporuje soubor funkcí usnadňujících celkovou strukturalizaci řízení rizik v oblasti IKT. Budou-li hlavní prostředky, kterými disponují 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***, přičemž by se mělo zohlednit, zda se jedná o zásadní nebo důležitou funkci***. 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.

---

[13] CPMI-IOSCO, *Pokyny ke kybernetické odolnosti infrastruktury finančních trhů*, https://www.bis.org/cpmi/publ/d146.pdf *G7 – Základní prvky kybernetické bezpečnosti pro finanční sektor,* 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

(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 pro hlášení závažných incidentů souvisejících s IKT***, 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***, kromě mikropodniků,*** 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. ***Za účelem prohloubení spolupráce s důvěryhodnými třetími zeměmi v oblasti odolnosti finančních subjektů by se měla Komise a příslušné orgány snažit o vytvoření rámce pro vzájemné uznávání výsledků penetračních testů na základě hrozeb.***

Členské státy by měly určit jeden veřejný orgán odpovědný za penetrační testy na základě hrozeb ve finančním sektoru na vnitrostátní úrovni. Tímto veřejným orgánem by mohl být například příslušný vnitrostátní orgán nebo veřejný orgán určený v souladu s článkem 8 směrnice (EU) 2016/1148 (směrnice o bezpečnosti sítí a informací). Tento veřejný orgán by měl být odpovědný za vydávání osvědčení, že byl penetrační test na základě hrozeb proveden v souladu s požadavky. Tato osvědčení by měla usnadnit vzájemné uznávání testů mezi příslušnými orgány.

Některé finanční subjekty jsou schopny provádět interní pokročilé testování, zatímco jiné budou uzavírat smlouvy s externími testery z Unie nebo ze třetí země. Je proto důležité, aby se na všechny testery vztahovaly stejné, jasné požadavky. Aby byla zajištěna nezávislost interních testerů, mělo by jejich využití podléhat schválení příslušným orgánem.

Metodika penetračních testů na základě hrozeb by neměla být povinná, ale mělo by se mít za to, že stávající rámec TIBER-EU vyhovuje požadavkům penetračních testů na základě hrozeb stanoveným v tomto nařízení.

Do vstupu tohoto nařízení v platnost a do vypracování povinných regulačních technických norem pro penetrační testy na základě hrozeb a jejich přijetí evropskými orgány dohledu by se finanční subjekty měly řídit příslušnými pokyny a rámci Unie, které se vztahují na penetrační testy prováděné na základě operativních informací, neboť tyto pokyny a rámce budou platit i po vstupu tohoto nařízení v platnost.

(44a) Odpovědnost za provádění penetračních testů na základě hrozeb – a za řízení kybernetické bezpečnosti obecně a prevenci kybernetických útoků – by měla zůstat plně na finančním subjektu a osvědčení vydávaná orgány by měla sloužit výhradně k účelům vzájemného uznávání a neměla by vylučovat žádná následná opatření na úrovni rizika souvisejícího s IKT, kterému je finanční subjekt vystaven, ani by neměla být vnímána jako potvrzení jeho schopností v oblasti řízení a zmírňování rizik souvisejících s IKT.

(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***, zejména pokud jde o zajišťování zásadních nebo důležitých funkcí těmito poskytovateli,*** 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, ***povaze,*** 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***, jakož i na základě toho, zda jsou služby IKT zajišťovány v rámci skupiny, nebo třetí stranou***.

(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 v případě minimálního souboru skutečností dokládajících ***závažné*** nedostatky vzniklé u poskytovatele služeb IKT z řad třetích stran by měla být ***přijata nápravná opatření, mezi která může patřit částečné nebo úplné vypovězení*** smlouvy.

(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 ▌. 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. ***Společný orgán dohledu provádějící*** dohled nad jednotlivými kritickými poskytovateli služeb IKT z řad třetích stran ***a evropský orgán dohledu pověřený prováděním každodenního dohledu*** („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[14].

(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

[14] 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.

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, ukončení obchodní činnosti poskytovatele služeb IKT z řad třetích stran ***nebo ukončení smluvních ujednání***.

(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 třetích stran zajišťovat zásadní nebo důležité funkce, včetně poskytování pomoci touto stranou v případě incidentu souvisejícího s IKT***, který má význam z hlediska služeb poskytovaných touto třetí stranou finančnímu subjektu v rámci sjednaných úrovní služeb,*** zdarma nebo za předem stanovenou cenu. ***Na doplňkové služby IKT, na nichž nezávisí provoz finančních subjektů, se toto nařízení nevztahuje.***

Kromě toho by definice „zásadní nebo důležité funkce“ stanovená v tomto nařízení měla zahrnovat definici „zásadních funkcí“ uvedenou v čl. 2 odst. 1 bodě 35 směrnice Evropského parlamentu a Rady 2014/59/EU ze dne 15. května 2014[15]***. Funkce, které jsou považovány za zásadní podle směrnice (EU) 2014/59/EU, by se proto měly považovat za zásadní nebo důležité funkce i podle tohoto nařízení.***

(53) ***V případě smluvních ujednání týkajících se zásadních nebo důležitých funkcí*** jsou práva na přístup, kontrolu a audit finančním subjektem nebo určenou třetí stranou společně s úplnou spoluprací poskytovatele služeb IKT z řad třetích stran klíčovými nástroji průběžného sledování plnění těchto poskytovatelů služeb. Podobně by měl ***společný orgán dohledu a hlavní orgán dohledu*** finančního subjektu disponovat týmiž právy provést po předchozím oznámení kontrolu a audit poskytovatele služeb IKT z řad třetích stran při zachování mlčenlivosti***, přičemž musí dbát na to, aby nenarušily služby poskytované dalším zákazníkům tohoto poskytovatele služeb IKT z řad třetích stran***. ***Finanční subjekt a poskytovatel služeb IKT z řad třetích stran by měli mít možnost dohodnout se na tom, že práva na přístup, kontrolu a audit lze přenést na nezávislou třetí stranu.***

(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 ***interní*** řešení. ***Úvěrové instituce by měly zajistit, aby byly příslušné***

[15] ***Směrnice Evropského parlamentu a Rady 2014/59/EU ze dne 15. května 2014, kterou se stanoví rámec pro ozdravné postupy a řešení krize úvěrových institucí a investičních podniků a kterou se mění směrnice Rady 82/891/EHS, směrnice Evropského parlamentu a Rady 2001/24/ES, 2002/47/ES, 2004/25/ES, 2005/56/ES, 2007/36/ES, 2011/35/EU, 2012/30/EU a 2013/36/EU a nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 a (EU) č. 648/2012 (Úř. věst. L 173, 12.6.2014, s. 190).***

smlouvy v oblasti IKT robustní a aby je bylo možné v případě řešení krize určité úvěrové instituce vymáhat. Úvěrové instituce by měly v souladu s očekáváními orgánů příslušných k řešení krize zajistit, aby byly příslušné smlouvy týkající se poskytování služeb v oblasti IKT odolné vůči takovým krizím. Dokud jsou zásadní a důležité funkce v oblasti IKT nadále prováděny, měly by tyto finanční subjekty zajistit, aby smlouvy vedle jiných požadavků obsahovaly doložku o zákazu vypovězení, pozastavení jejich platnosti a zákazu změny z důvodu restrukturalizace nebo řešení krize.

(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.

(55a) Evropské orgány dohledu by měly být pověřeny vypracováním prováděcích technických a regulačních norem upřesňujících očekávání politik týkajících se řízení rizik v oblasti IKT spojených s třetími stranami a smluvních požadavků. Do vstupu těchto norem v platnost by se finanční subjekty měly řídit příslušnými pokyny a dalšími opatřeními vydanými evropskými orgány dohledu a příslušnými orgány.

(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 ***rámec*** dohledu. 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 podporu plnění úkolů*** na úrovni Eurosystému***, jak je uvedeno*** v čl. 127 odst. 2 Smlouvy o fungování Evropské unie, by měli být následně vyňati. ***Stejně tak by se neměl mechanismus pro určování kritických subjektů vztahovat ani na podniky, které jsou součástí finanční skupiny a které poskytují služby v oblasti IKT výlučně finančním subjektům v rámci stejné finanční skupiny.***

(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. ***Požadovaný podnik, jako je dceřiná společnost založená v Unii podle práva členského státu, má sloužit jako kontaktní místo mezi poskytovatelem služeb IKT z řad třetích***

stran na jedné straně a hlavním orgánem dohledu a společným orgánem dohledu na straně druhé a zajistit, aby hlavní orgán dohledu a společný orgán dohledu byly schopny plnit své povinnosti a vykonávat své pravomoci v oblasti dohledu a prosazování pravidel stanovené v tomto nařízení. Smluvní služby poskytovatele služeb IKT z řad třetích stran nemusí být poskytovány jeho subjektem v Unii.

(58a) Vzhledem k možnému závažnému dopadu určení poskytovatelů služeb IKT z řad třetích stran jakožto kritických je nutné stanovit předchozí právo na vyslechnutí coby povinnost evropských orgánů dohledu a společného orgánu dohledu řádně přihlédnout k veškerým dodatečným informacím, jež poskytovatelé služeb IKT z řad třetích stran předají v rámci procesu určování.

(59) ***Rámec dohledu*** 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***, prostřednictvím nově zřízeného společného orgánu dohledu vydávajícího*** jak individuální rozhodnutí určená kritickým poskytovatelům služeb IKT z řad třetích stran, tak 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 zřízen společný orgán dohledu za účelem provádění přímého dohledu poskytovatelů služeb IKT z řad třetích stran***. ***Kromě toho*** by měl být pro každého poskytovatele služeb IKT z řad třetích stran určen jeden evropský orgán dohledu jako hlavní orgán dohledu***, který by prováděl a koordinoval každodenní dohled a vyšetřování, působil jako jednotné kontaktní místo a zajišťoval kontinuitu***. ***Společný orgán dohledu a hlavní orgán dohledu by měly efektivně spolupracovat na zajištění účinného každodenního dohledu, jakož i uceleného přístupu k rozhodování a doporučením.***

(62) Hlavním orgánům by měly být přiznány nezbytné pravomoci k provádění šetření, kontrol u kritických poskytovatelů služeb IKT z řad třetích stran na místě, 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.

(62a) Pověření ***společného orgánu dohledu přímým*** 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) ***Společný orgán dohledu*** by měl mít možnost ***vydávat*** 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 ***společným orgánem dohledu***. ***Před finalizací těchto doporučení by měli mít kritičtí poskytovatelé služeb IKT z řad třetích stran možnost poskytnout informace, o nichž mají důvod se domnívat, že by měly být před finalizací a vydáním doporučení vzaty v úvahu.***

(63a) Aby se hlavní orgány dohledu a společný orgán dohledu vyvarovaly zdvojování technických a organizačních opatření, která se vztahují na kritické poskytovatelé služeb IKT z řad třetích stran, a rozporů mezi nimi, měly by při výkonu svých pravomocí v souladu s rámcem dohledu uvedeného v tomto nařízení řádně přihlížet k rámci stanovenému ve směrnici (EU) 2016/1148. Před výkonem těchto pravomocí by měl společný orgán dohledu a hlavní orgán dohledu konzultovat s relevantními příslušnými orgány, které jsou příslušné podle směrnice (EU) 2016/1148.

(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 ***při obecných šetřeních nebo kontrolách na místě*** 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[16], a konzultace s evropskými orgány dohledu prostřednictvím vzájemné výměny informací a poskytování pomoci v souvislosti s činnostmi dohledu. ***Jednotný výbor pro řešení krizí, ačkoli pro účely tohoto nařízení není příslušným orgánem, by měl být přesto zapojen do mechanismů vzájemné výměny informací pro subjekty, které spadají do oblasti působnosti nařízení Evropského parlamentu a Rady (EU) č. 806/2014[17]***.

(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 vedla v rámci přípravné činnosti 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[18]. 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 setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(69) Protože toto nařízení, společně se směrnicí Evropského parlamentu a Rady (EU) 20xx/xx[19], 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.

V rámci konsolidace je nutné přezkoumat a přepracovat příslušné pokyny, které vydaly nebo v současnosti připravují evropské orgány dohledu ohledně příslušných nařízení a směrnic, tak aby právní základ vztahující se na požadavky uvedené v právních předpisech Unie vyplýval výlučně z tohoto nařízení, jeho prováděcích aktů a rozhodnutí a doporučení přijatých v souladu s ním, pokud jde o subjekty spadající do jeho působnosti.

(69a) Konzistentní harmonizaci požadavků stanovených tímto nařízením by měly zajišťovat

---

[16] 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).

[17] ***Nařízení Evropského parlamentu a Rady (EU) č. 806/2014 ze dne 15. července 2014, kterým se stanoví jednotná pravidla a jednotný postup pro řešení krize úvěrových institucí a některých investičních podniků v rámci jednotného mechanismu pro řešení krizí a Jednotného fondu pro řešení krizí a mění nařízení (EU) č. 1093/2010 (Úř. věst. L 225, 30.7.2014, s. 1).***

[18] Úř. věst. L 123, 12.5.2016, s. 1.

[19] *[vložte úplný odkaz]*.

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. ***Při vypracovávání návrhů regulačních technických norem by měly evropské orgány dohledu řádně přihlížet ke svému mandátu, pokud jde o otázku proporcionality, a žádat o radu svůj poradní výbor pro otázky proporcionality, zejména pokud jde o uplatňování tohoto nařízení na malé a střední podniky a podniky se střední kapitalizací.***

(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 ***povahu,*** velikost, složitost ***a podnikatelský profil*** finančních subjektů, jakož i povahu a úroveň rizika jejich činnosti. 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, 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,

– ***hlášení závažných provozních nebo bezpečnostních incidentů souvisejících s platbami příslušným orgánům ze strany finančních subjektů uvedených v čl. 2 odst. 1 písm. a) až c);***

– 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 ***zajišťované*** 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.

2a. Tímto nařízením není dotčena příslušnost členských států, pokud jde o udržování veřejné bezpečnosti, obranu a národní bezpečnost.

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 a ***subjekty, které je nabízejí,*** vydavatele tokenů vázaných na aktiva ***a subjekty, které je nabízejí,*** a vydavatele významných tokenů vázaných na aktiva,

f) centrální depozitáře cenných papírů ***a provozovatele systémů vypořádání 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***, kteří nejsou mikropodniky, malými nebo středními podniky, s výjimkou případů, kdy tyto mikropodniky, malé nebo střední podniky spoléhají výlučně na systémy organizovaného automatického prodeje,***

o) instituce zaměstnaneckého penzijního pojištění, ***které neprovozují penzijní systémy, jež mají dohromady méně než 15 členů,***

p) ratingové agentury;

g) statutární auditory a auditorské společnosti, ***které nejsou mikropodniky, malými nebo středními podniky, s výjimkou případů, kdy tyto mikropodniky, malé nebo střední podniky poskytují auditorské služby subjektům uvedeným v tomto článku, s výjimkou mikropodniků, malých nebo středních podniků, které jsou neziskovými auditními subjekty podle čl. 2 odst. 3 nařízení (EU) č. 537/2014, pokud příslušný orgán nerozhodne, že výjimka není platná,***

r) správce kritických referenčních hodnot;

s) poskytovatele služeb skupinového financování;

t) registry sekuritizací;

u) poskytovatele služeb IKT z řad třetích stran.

1a. Toto nařízení se s výjimkou kapitoly V oddílu II rovněž vztahuje na poskytovatele služeb IKT v rámci skupiny.

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

2a. Pro účely tohoto nařízení, s výjimkou kapitoly V oddílu II, se poskytovatelé služeb IKT z řad třetích stran a poskytovatelé služeb IKT v rámci skupiny souhrnně označují jako „poskytovatelé služeb IKT z řad třetích stran“.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

(1) „digitální provozní odolností“ schopnost finančního subjektu budovat, zajišťovat a revidovat svoji provozní integritu ▌prostřednictvím zajištění, ať již přímo, či nepřímo s využitím služeb IKT poskytovaných třetími stranami, ▌nepřetržitého poskytování finančních služeb a jejich kvality, ***v případě narušení provozu, které má dopad na schopnosti finančního subjektu v oblasti IKT***;

(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 vyplývající z používání sítě a informačních systémů ▌, které mohou narušit bezpečnost sítí a informačních systémů, jakýchkoli na ***IKT*** závislých nástrojů nebo procesů, provozu a fungování procesů nebo poskytování služeb▌ ;

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

(6) „incidentem souvisejícím s IKT“ nepředvídaný zjištěný ***incident nebo řada souvisejících incidentů***, která ohrožuje bezpečnost sítí a informačních systémů ▌nebo která nepříznivě dopadá na dostupnost, důvěrnost, kontinuitu***, integritu*** či autenticitu finančních služeb poskytovaných finančním subjektem;

(6a) „provozním nebo bezpečnostním incidentem souvisejícím s platbami“ událost nebo řada souvisejících událostí, které finanční instituce uvedené v čl. 2 odst. 1 písm. a) až c) nepředvídaly a které mají nebo mohou mít nepříznivý dopad na integritu, dostupnost, důvěrnost, autenticitu nebo kontinuitu služeb souvisejících s platbami;

(7) „závažným incidentem souvisejícím s IKT“ incident související s IKT, ***který má nebo může mít*** rozsáhlý nepříznivý dopad na síť a informační systémy využívané k zajištění zásadních funkcí finančního subjektu;

(7a) „závažným provozním nebo bezpečnostním incidentem souvisejícím s platbami“ závažný provozní nebo bezpečnostní incident související s platbami, který splňuje kritéria uvedená v článku 16;

(8) „kybernetickou hrozbou“ kybernetická hrozba dle vymezení v čl. 2 bodě 8 nařízení Evropského parlamentu a Rady (EU) 2019/881[20];

(8a) „závažnou kybernetickou hrozbou“ kybernetická hrozba, jejíž charakteristika jasně ukazuje, že může vést k závažnému incidentu souvisejícímu s IKT;

(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

[20] 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).

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 ***kybernetická*** 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;

(15) „poskytovatelem služeb IKT z řad třetích stran“ ▌ podnik poskytující ▌ služby ***IKT, včetně finančního subjektu poskytujícího služby IKT, který je součástí podniku, jenž poskytuje širší rozsah produktů nebo služeb***, 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[21];

(15a) „poskytovatelem služeb IKT v rámci skupiny“ podnik, který je součástí finanční skupiny a poskytuje služby v oblasti IKT výlučně finančním subjektům v rámci téže skupiny nebo finančním subjektům v rámci téhož institucionálního systému ochrany, včetně jejich mateřských podniků, dceřiných podniků nebo poboček či dalších subjektů, které jsou ve společném vlastnictví nebo pod společnou kontrolou;

(16) „službami IKT“ digitální a datové služby ***průběžně*** poskytované prostřednictvím systémů IKT jednomu či více interním nebo externím uživatelům***, s výjimkou telekomunikačních smluv***;

(17) „zásadní nebo důležitou funkcí“ ***činnost nebo služba, jež má zásadní význam z hlediska provozu finančního subjektu a jejíž narušení by významně narušilo spolehlivost nebo kontinuitu služeb a činností finančního subjektu, nebo*** 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***, včetně jeho „zásadních funkcí“ ve smyslu čl. 2 odst. 1 bodu 35 směrnice 2014/59/EU;***

(18) „kritickým poskytovatelem služeb IKT z řad třetích stran“ poskytovatel služeb IKT z řad třetích stran určený v souladu s článkem ***28*** a podléhající rámci dohledu uvedenému v článcích ***29*** 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 ▌a

[21] 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).

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 ▌ 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 ***finanční stabilitu Unie jako celku nebo*** schopnost finančního subjektu ▌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[22], čl. 3 odst. 1 ***bod 18***) nařízení Evropského parlamentu a Rady (EU) 20xx/xx[23] [MICA] nebo 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[24];

(23a) „úvěrovou institucí vyňatou z působnosti směrnice 2013/36/EU“ instituce, na níž se podle čl. 2 odst. 5 bodů 4) až 23) směrnice 2013/36/EU vztahuje výjimka;

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

(24a) „malým a nepropojeným investičním podnikem“ investiční podnik, který splňuje podmínky stanovené v čl. 12 odst. 1 nařízení (EU) 2019/2033;

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

(25a) „platební institucí vyňatou z působnosti směrnice (EU) 2015/2366“ platební instituce, na níž se podle čl. 32 odst. 1 směrnice 2015/2366 vztahuje výjimka;

(26) „institucí elektronických peněz“ instituce elektronických peněz dle vymezení v čl. 2 bodě 1 směrnice Evropského parlamentu a Rady 2009/110/ES[25];

(26a) „institucí elektronických peněz vyňatou z působnosti směrnice 2009/110/ES“ instituce elektronických peněz, na níž se podle článku 9 směrnice 2009/110/ES vztahuje

---

22 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).

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

24 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).

25 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).

výjimka;

(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 ***odst. 1*** bodě 3 směrnice (EU) 2016/97;

(37) „zprostředkovatelem doplňkového pojištění“ zprostředkovatel pojištění dle vymezení v čl. 2 ***odst. 1*** bodě 4 směrnice (EU) 2016/97;

(38) „zprostředkovatelem zajištění“ zprostředkovatel zajištění dle vymezení ***v čl. 2 odst. 1*** 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;

(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 ***bodě 8*** nařízení (EU) 202x/xx [OP: vložte odkaz na nařízení MICA];

(44) „vydavatelem kryptoaktiv“ vydavatel kryptoaktiv dle vymezení v čl. 3 odst. 1 ***bodě 6*** [Úř. věst: vložte odkaz na nařízení MICA];

(44a) „nabízejícím subjektem“ nabízející subjekt dle vymezení v čl. 3 odst. 1 bodě [XX] [Úř. věst.: vložte odkaz na nařízení MICA];

(44b) „subjektem nabízejícím kryptoaktiva“ subjekt nabízející kryptoaktiva dle vymezení v čl. 3 odst. 1 bodě [XX] [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];

(45a) „subjektem nabízejícím tokeny vázané na aktiva“ subjekt nabízející tokeny vázané na aktiva dle vymezení v čl. 3 odst. 1 bodě [XX] [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 ***bodě XX***) [Úř. věst: vložte odkaz na nařízení MICA];

(47) „správcem kritických referenčních hodnot“ správce kritických referenčních hodnot dle vymezení v čl. ***3*** bodě ***25*** nařízení ***2016/1011*** [Úř. věst: vložte odkaz na nařízení o referenčních hodnotách];

(48) „poskytovatelem služeb skupinového financování“ poskytovatel služeb skupinového financování dle vymezení v ***čl. 2 odst. 1 písm. e)*** nařízení (EU) ***2020/1503*** [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***, malým a středním podnikem***“ finanční subjekt dle vymezení v článku 2 přílohy doporučení 2003/361/ES.

(50a) „orgánem příslušným k řešení krize“ orgán určený členským státem v souladu s článkem 3 směrnice 2014/59/EU nebo Jednotný výbor pro řešení krizí zřízený v souladu s článkem 42 nařízení (EU) č. 806/2014.

Článek 3a

Zásada proporcionality

1. Finanční subjekty uplatňují pravidla zavedená kapitolami II, III a IV v souladu se zásadou proporcionality a s přihlédnutím ke své velikosti, povaze, rozsahu a složitosti svých služeb, činností a operací i ke svému celkovému rizikovému profilu.

2. Podle zásady proporcionality se články 4 až 14 tohoto nařízení nevztahují na:

a) malé a nepropojené investiční podniky nebo platební instituce vyňaté z působnosti směrnice (EU) 2015/2366;

b) úvěrové instituce vyňaté z působnosti směrnice 2013/36/EU;

c) instituce elektronických peněz vyňaté z působnosti směrnice 2009/110/ES; nebo

d) malé instituce zaměstnaneckého penzijního pojištění;

3. Na základě výroční zprávy o přezkumu rámce pro řízení rizik v oblasti IKT podle čl. 5 odst. 6 a čl. 14a odst. 2 dotčené příslušné orgány přezkoumají a vyhodnotí uplatňování proporcionality finančním subjektem a určí, zda rámec finančního subjektu pro řízení rizik v oblasti IKT zajišťuje řádné řízení a digitální provozní odolnost a pokrytí rizik v oblasti IKT. Příslušné orgány přitom zohlední velikost finančního subjektu, povahu, rozsah a složitost jeho služeb, činností a operací a jeho celkový rizikový profil.

4. V případě, že relevantní příslušný orgán považuje rámec finančního subjektu pro řízení rizik v oblasti IKT za nedostatečný a nepřiměřený, zahájí s finančním subjektem dialog s cílem napravit nedostatky a zajistit plný soulad s kapitolou II.

5. Evropské orgány dohledu vypracují návrhy regulačních technických norem, pokud jde o:

a) určení rozsahu, v jakém se povinnosti řízení rizik v oblasti IKT vztahují na každý z finančních subjektů uvedených v odstavci 1;

b) další upřesnění obsahu a formátu výroční zprávy o přezkumu rámce pro řízení rizik v oblasti IKT podle odstavce 3;

c) další upřesnění pravidel a postupů, které mají příslušné orgány a finanční subjekty dodržovat při dialogu podle odstavce 4.

6. Evropské orgány dohledu předloží návrhy regulačních technických norem podle odstavce 5 Komisi do [Úř. věst.: vložte 1 rok po datu vstupu tohoto nařízení v platnost].

Na Komisi je přenesena pravomoc přijímat regulační technické normy uvedené v odstavci 5 tohoto článku v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, nařízení (EU) č. 1094/2010 a nařízení (EU) č. 1095/2010.

KAPITOLA II

ŘÍZENÍ RIZIK V OBLASTI IKT

ODDÍL I

Článek 4

Řízení a organizace

1. Finanční subjekty disponují ***interním řídicím a kontrolním rámcem***, který zajistí účinné a obezřetné řízení všech rizik v oblasti IKT ***s cílem dosáhnout vysoké míry digitální provozní odolnosti***.

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;

   aa) zavádí postupy a strategie, jejichž cílem je zajistit zachování přísných norem v oblasti bezpečnosti, důvěrnosti a integrity dat;

   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, kontroluje a pravidelně přezkoumává strategii finančního subjektu pro zachování provozu a jeho plán obnovy provozu po havárii IKT***, který může být přijat jako zvláštní politika a jako nedílná součást širší podnikové strategie zachování provozu a plánu obnovy provozu po havárii*** podle čl. 10 odst.1 a 3;

   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 ***příslušných*** školení o rizicích v oblasti IKT a zajištění odpovídajících dovedností všech ▌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 ***pravidelně*** informován ***alespoň o závažných*** incidentech souvisejících s IKT a jejich dopadech a opatřeních v rámci reakce, obnovy provozu a nápravy.

3. Finanční subjekty jiné než mikropodniky vytvoří ***v rámci finančního subjektu*** funkci sledování ujednání o využívání služeb IKT***, zejména ujednání uzavřených s poskytovateli služeb IKT 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 ***finančního subjektu aktivně usilují o*** dostatečné a aktuální znalosti a dovednosti k pochopení a hodnocení rizik v oblasti IKT a jejich dopadů na fungování finančního subjektu***, mimo jiné pravidelným absolvováním specifického školení úměrného rizikům v oblasti IKT***.

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 ▌.

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 ***a o svém rámci pro řízení rizik v oblasti IKT*** podle požadavků příslušných orgánů.

4. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v odstavci 1 zavedou finanční subjekty jiné než mikropodniky systém řízení bezpečnosti informací vycházející z uznávaných mezinárodních norem a odpovídající pokynům dohledu***, pokud jsou již k dispozici a jsou vhodné, včetně pokynů stanovených v příslušných dokumentech evropských orgánů dohledu***, a pravidelně jej revidují.

5. Finanční subjekty jiné než mikropodniky ***pověří odpovědností za řízení a kontrolu rizik v oblasti IKT kontrolní funkci a zajistí nezávislost této kontrolní funkce, aby nedocházelo ke střetům zájmů.*** Finanční subjekty ▌ zajistí náležitou ***nezávislost*** 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.

Příslušnému orgánu se každoročně předkládá zpráva o přezkumu rámce pro řízení rizik v oblasti IKT.

7. ***Pokud jde o finanční subjekty jiné než mikropodniky,*** podléhá rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 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. ▌

9. Rámec pro řízení rizik v oblasti IKT uvedený v odstavci 1 zahrnuje strategii digitální ***provozní*** 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 ▌ struktury 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) ***určení*** klíčových závislostí na poskytovatelích služeb IKT z řad třetích stran ***a podrobné vymezení výstupních strategií ve vztahu k těmto klíčovým závislostem***;

   h) zavedení testování digitální provozní odolnosti ***v souladu s kapitolou IV tohoto nařízení***;

   i) popisu komunikační strategie v případě incidentů souvisejících s IKT***, které je třeba zveřejnit v souladu s článkem 13***.

10. Finanční subjekty mohou po schválení příslušnými orgány ***externalizovat*** úkoly ověřování shody s požadavky řízení rizik v oblasti IKT na ▌externí podniky.

Finanční subjekty mohou po informování příslušných orgánů delegovat úkol spojený s ověřováním souladu s požadavky na řízení rizik v oblasti IKT na podniky v rámci skupiny.

Pokud dojde k delegování podle druhého pododstavce, nese finanční subjekt za ověřování souladu s požadavky na řízení rizik v oblasti IKT i nadále plnou odpovědnost.

Článek 6

Systémy, protokoly a nástroje IKT

1. ***Za účelem řešení a řízení rizik v oblasti IKT*** finanční subjekty využívají a udržují aktualizované systémy, protokoly a nástroje IKT, které splňují následující podmínky:

   a) systémy a nástroje jsou přiměřené ▌ 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 ***zásadní nebo důležité*** 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 ***zásadnost nebo důležitost funkcí souvisejících s IKT v rámci činnosti organizace a*** 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 ***zásadní nebo důležité*** 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***, pokud je to vhodné,*** 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 ***zásadních nebo důležitých*** aktiv IKT, ***a to s ohledem na jejich účel*** a propojení a vzájemné závislosti těchto různých prostředků IKT.

5. Finanční subjekty identifikují a dokumentují veškeré ***zásadní nebo důležité*** procesy závislé na poskytovatelích služeb IKT z řad třetích stran a identifikují vzájemná propojení s poskytovateli služeb IKT z řad třetích stran***, kteří zásadní nebo důležité funkce podporují***.

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, ***a to včetně systémů, které se stále používají a plní svou funkci, ale:***

   a) jsou staré nebo na konci své životnosti v případě hardwaru;

   b) již nemohou dostávat podporu nebo údržbu od svého dodavatele nebo

   c) jejich aktualizace je nemožná nebo nehospodárná. Roční posouzení rizik v oblasti IKT se provádí u stávajících systémů IKT, zejména před propojením a po propojení ▌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 ***podporujících zásadní nebo důležité funkce*** 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 ▌technologie a procesy IKT, které:

   a) ***maximalizují*** 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 ***interními*** riziky ***v oblasti IKT včetně*** špatné správy, rizik souvisejících se zpracováním ***a chyb způsobených lidským faktorem***.

4. Jako součást rámce pro řízení rizik v oblasti IKT uvedeného v čl. 5 odst. 1 finanční subjekty ***v souladu se svým rizikovým profilem***:

a) vypracují a zdokumentují politiku zabezpečení informací s vymezením pravidel ochrany důvěrnosti, integrity a dostupnosti svých ***prostředků IKT, dat a informačních aktiv a zároveň zajistí plnou ochranu*** prostředků IKT, dat a informačních aktiv svých klientů, ***pokud jsou součástí systémů IKT finančních subjektů***;

b) zavedou vhodné řízení sítí a infrastruktury na základě rizik využívající odpovídajících technik, metod a protokolů, ***které mohou zahrnovat*** zavedení ▌ mechanismů pro izolaci dotčených informačních aktiv v případě kybernetických útoků;

c) uplatňují politiky***, postupy a kontroly*** omezující fyzický a virtuální přístup k prostředkům systémů IKT a k datům na minimum nezbytné pro výkon oprávněných a schválených funkcí a činností ▌;

d) zavedou postupy a protokoly pro silné ověřovací mechanismy ***a ochranu kryptografických klíčů*** založené na příslušných normách a systémech speciálních kontrol ▌;

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 co nejrychlejší*** 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***, pokud je to technologicky možné,*** mechanismy identifikace ***a sledování*** všech 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 ▌ spustí detekci incidentů souvisejících s IKT a procesů reakce na ně, ***včetně*** automatických výstražných mechanismů pro příslušné pracovníky odpovědné za reakce na incidenty související s IKT.

3. Finanční subjekty věnují ▌ dostatečné zdroje a prostředky na sledování aktivity uživatelů a výskytu anomálií IKT a incidentů souvisejících s IKT, zejména kybernetických útoků.

3a Finanční subjekty zaznamenávají všechny incidenty související s IKT, které mají dopad na stabilitu, kontinuitu nebo kvalitu finančních služeb, včetně případů, kdy incident má nebo může mít dopad na tyto služby.

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 ▌ucelenou strategii zachování provozu IKT***, která může být přijata jako zvláštní politika a*** jakožto nedílná součást ***širší podnikové*** operační strategie zachování provozu finančního subjektu.

   Cílem strategie zachování provozu IKT je řídit a zmírňovat rizika, která by mohla mít škodlivý dopad na systémy IKT a služby IKT finančních subjektů , a v případě potřeby usnadnit jejich rychlou obnovu. Při přípravě strategie zachování provozu IKT se finanční subjekty zabývají konkrétně riziky, která by mohla mít nepříznivý dopad na služby a systémy v oblasti IKT.

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

   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 ***zásadních nebo důležitých*** systémů 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***, buď jako zvláštní funkci, nebo jako součást funkcí s odpovědností za reakci na incidenty a jejich řízení. Funkce řízení krizí*** 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 ***relevantní*** 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 ***odhadované finanční*** náklady a ztráty způsobené ***významnými*** výpadky IKT a ***závažnými*** incidenty souvisejícími s IKT.

9a. Evropské orgány dohledu vypracují prostřednictvím společného výboru společné pokyny týkající se metodiky pro výpočet nákladů a vyčíslování ztrát ve smyslu odstavce 9.

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. ***V souladu se zásadou zálohování uvedenou v odst. 1 písm. a)*** se záložní systémy 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***, které jsou fyzicky nebo logicky odděleny*** od hlavního ***systému IKT*** a jsou zabezpečeny 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 ***posoudí potřebu*** udržovat rezervní kapacity IKT vybavené zdroji, prostředky a funkcemi, jež jsou dostatečné a vhodné pro zajištění potřeb jejich činnosti ***a splňují požadavky v oblasti digitální provozní odolnosti stanovené v tomto nařízení***.

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 ▌přístupné pro personál finančního subjektu zajišťující kontinuitu zásadních ***nebo důležitých funkcí*** v případě, že primární místo zpracování přestane být dostupné.

6. Při stanovení cílové doby a okamžiku obnovy provozu jednotlivých funkcí finanční subjekty zohlední***, zda se jedná o zásadní nebo důležitou funkci,*** a 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 ***zajistí, aby byla zajištěna nejvyšší možná úroveň integrity dat, například*** provedením různých kontrol, včetně porovnání dat. ***Takové*** 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, 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 ***souvisejících s řešením***

rizik v oblasti IKT zjištěných na základě přezkumu po závažných výpadcích IKT nahlásí ***všechny významné*** změny příslušným orgánům, ***přičemž specifikují požadovaná zlepšení a způsob, jakým mají tato opatření budoucím výpadkům předcházet nebo je zmírňovat***. ***Změny mohou být příslušným orgánům oznámeny před provedením změn nebo po něm.***

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***, včetně blízkosti těchto rizik k zásadním a důležitým funkcím,*** 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. ***Programy zvyšování povědomí o bezpečnosti v oblasti IKT jsou povinné pro všechny zaměstnance.*** Školení ***v oblasti digitální provozní odolnosti jsou povinné alespoň*** pro všechny zaměstnance***, kteří mají práva přímého přístupu do systémů IKT,*** a vyšší vedoucí pracovníky. ***Složitost vzdělávacích modulů je úměrná úrovni přímého přístupu zaměstnance do systémů IKT, a zejména zohledňuje jeho přístup k zásadním nebo důležitým funkcím.***

Finanční subjekty ***jiné než mikropodniky*** 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 ***alespoň*** o ***závažných*** incidentech souvisejících s IKT nebo hlavních slabých místech.

   Komunikační plány uvedené v prvním pododstavci rovněž zajistí, aby byli klienti a protistrany prostřednictvím stručného shrnutí každoročně informováni o všech incidentech souvisejících s IKT. Toto informování musí plně respektovat obchodní tajemství finančního subjektu a jeho klientů a protistran a nesmí ohrozit rámec pro řízení rizik v oblasti IKT uvedený v čl. 5 odst. 1.

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 ***alespoň na závažné*** 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 ***a zbytečných odkladů***;

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.

Článek 14a

Rámec pro řízení rizik v oblasti IKT pro malé, nepropojené a vyňaté subjekty

1. V souladu s článkem 3a malé a nepropojené investiční společnosti, platební instituce vyňaté z působnosti směrnice (EU) 2015/2366, úvěrové instituce vyňaté z působnosti směrnice 2013/36/EU, instituce elektronických peněz vyňaté z působnosti směrnice 2009/110/ES a malé instituce zaměstnaneckého penzijního pojištění zavedou a udržují solidní a zdokumentovaný rámec pro řízení rizik v oblasti IKT, který

a) podrobně popisuje mechanismy a opatření zaměřené na rychlé, účinné a komplexní řízení všech rizik v oblasti IKT, mj. pokud jde o ochranu příslušných fyzických komponentů a infrastruktur;

b) průběžně sleduje bezpečnost a fungování všech systémů IKT;

c) minimalizuje dopad rizik v oblasti IKT používáním solidních, odolných a aktualizovaných systémů, protokolů a nástrojů v oblasti IKT, které jsou vhodné k podpoře provádění jejich činnosti a poskytování služeb;

d) přiměřeným způsobem chrání důvěrnost, integritu a dostupnost datových sítí a informačních systémů,

e) umožňuje rychlé vyhledávání a zjišťování zdrojů rizik a anomálií v síti a informačních systémech a urychlené řešení incidentů v oblasti IKT.

2. 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 orgánů dohledu nebo závěrů vyvozených z příslušných testů či auditů digitální provozní odolnosti. Je průběžně zdokonalován na základě zkušeností, které vyplynuly z jeho provádění a monitorování.

Zpráva o přezkumu rámce pro řízení rizik v oblasti IKT se každoročně předkládá příslušnému orgánu.

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 ***postupy a*** procesy zajišťující konzistentní a integrované sledování, řešení a následná opatření pro incidenty související s IKT, aby byla zajištěna identifikace a ***řešení*** 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 ***alespoň*** 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 ***závažných*** 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 ▌;

   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 ***v koordinaci*** 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 ***závažných*** incidentů souvisejících s IKT, které budou sdíleny s dalšími příslušnými orgány podle čl. 17 odst. 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 dále přihlédnou k tomu, že včasné a účinné zvládnutí incidentu ze strany malých podniků a mikropodniků není omezeno nutností dodržovat klasifikační požadavky stanovené v tomto článku. Evropské orgány dohledu rovněž přihlédnou k velikosti finančních subjektů, povaze, rozsahu a složitosti jejich služeb, činností a operací a k jejich celkovému rizikovému profilu.***

Evropské orgány dohledu předloží tento společný návrh regulačních technických norem Komisi do [Úř. věst. [vložte datum ***2 roky*** 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.

1a. Finanční subjekty mohou dobrovolně hlásit vážné kybernetické hrozby příslušnému orgánu, pokud se domnívají, že hrozba je relevantní pro finanční systém, uživatele služeb nebo klienty. Příslušný orgán může tyto informace poskytnout jiným příslušným orgánům v souladu s odstavcem 5.

2. ***Dojde-li k závažnému incidentu souvisejícímu*** s IKT ***nebo má-li takový incident***

podstatný dopad na finanční zájmy uživatelů služeb a klientů, finanční subjekty bez zbytečného prodlení ***poté, co se o něm dozvědí, informují*** uživatele svých služeb a klienty o tomto závažném incidentu souvisejícím s IKT a ▌informují ***je*** o veškerých ***relevantních*** opatřeních přijatých ke zmírnění nepříznivých dopadů tohoto incidentu. ***Pokud v důsledku protiopatření přijatých finančním subjektem nedojde k újmě uživatelů služeb a klientů, požadavek na informování uživatelů a klientů neplatí.***

3. Finanční subjekty předloží příslušnému orgánu podle článku 41:

a) prvotní oznámení ▌závažného incidentu souvisejícího s IKT, ***které obsahuje informace, jež má oznamující subjekt k dispozici s vynaložením nejvyššího úsilí:***

i) v případě incidentů, které významně narušují dostupnost služeb poskytovaných finančním subjektem, je nutné bez prodlení, nejpozději však do 24 hodin od zjištění incidentu, informovat příslušný orgán;

ii) v případě incidentů, které mají významný dopad na finanční subjekt s výjimkou dostupnosti služeb poskytovaných tímto finančním subjektem, je nutné bez prodlení, nejpozději však do 72 hodin od zjištění incidentu, informovat příslušný orgán;

iii) v případě incidentů, které mají dopad na integritu, důvěrnost nebo bezpečnost osobních údajů uchovávaných tímto finančním subjektem, je nutné bez prodlení, nejpozději však do 24 hodin od zjištění incidentu, informovat příslušný orgán;

b) průběžnou zprávu***, ihned po výrazné změně stavu původního incidentu nebo po zjištění nových informací, které by mohly mít zásadní vliv na to, jak příslušný orgán řeší incident související s IKT,*** 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 ***data*** odeslání prvotní zprávy;

ca) v případě, že v době předložení závěrečné zprávy podle písmene c) incident stále probíhá, předloží se závěrečná zpráva jeden měsíc po vyřešení incidentu.

Příslušný orgán uvedený v článku 41 stanoví, že v řádně odůvodněných případech se finanční subjekt může odchýlit od lhůt stanovených v písmenech a), b) a c) tohoto odstavce, s náležitým zohledněním schopnosti finančních subjektů poskytovat přesné a smysluplné informace o závažných incidentech souvisejících s IKT.

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. ***V případě delegování těchto povinností nese za plnění povinnosti spojené s nahlašováním incidentů i nadále plnou odpovědnost finanční subjekt.***

5. Po obdržení hlášení podle odstavce 1 poskytne příslušný orgán bez zbytečného prodlení podrobné informace o ***závažném*** incidentu ***souvisejícím s IKT***:

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 ***nebo týmům CSIRT zřízeným podle článku 9 směrnice (EU) 2016/1148***;

ca) orgánu příslušnému k řešení krize odpovědnému za příslušný finanční subjekt; Jednotnému výboru pro řešení krizí (SRB) v případě subjektů uvedených v čl. 7 odst. 2 nařízení (EU) č. 806/2014 a v případě subjektů a skupin uvedených v čl. 7 odst. 4 písm. b) a odst. 5 nařízení (EU) č. 806/2014, jsou-li splněny podmínky pro použití uvedených odstavců;

cb) vnitrostátnímu orgánu příslušnému k řešení krize v případě subjektů a skupin uvedených v čl. 7 odst. 3 nařízení (EU) č. 806/2014; vnitrostátní orgány příslušné k řešení krize poskytnou SRB čtvrtletně souhrn zpráv, které obdržely podle tohoto písmene v souvislosti se subjekty a skupinami uvedenými v čl. 7 odst. 3 nařízení (EU) č. 806/2014;

cc) jiným příslušným veřejným orgánům, včetně orgánů v jiných členských státech.

6. EBA, ESMA nebo EIOPA a ECB posoudí ***ve spolupráci s ENISA*** 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;

(3) specifikaci kritérií pro určení dopadu závažného incidentu souvisejícího s IKT na finanční subjekt pro účely čl. 17 odst. 3

písm. a);

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 písm. a) ***prvního pododstavce*** a společný návrh prováděcích technických norem podle písm. b) ***prvního pododstavce*** Komisi do xx 202x [Úř. věst.: [vložte datum ***2 roky*** od data vstupu v platnost].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím společných regulačních technických norem uvedených v písm. a) ***prvním pododstavci*** 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 písm. b) ***prvním pododstavci*** postupem podle článku 15 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010, respektive (EU) č. 1094/2010.

2. Dokud nebude znám výsledek zprávy uvedené v článku 19 hodnotící proveditelnost další centralizace hlášení incidentů, vypracují evropské orgány dohledu prostřednictvím společného výboru a ve spolupráci s příslušnými orgány, ECB, SRB a ENISA pokyny pro výměnu informací o hlášení závažných incidentů souvisejících s IKT v souladu s čl. 17 odst. 5.

Pokyny uvedené v prvním pododstavci zahrnují alespoň následující:

a) nejúčinnější komunikační spojení;

b) zachování bezpečnosti, důvěrnosti a integrity vyměňovaných údajů;

c) případné zapojení finančních subjektů do doplnění výměny informací podle článku 40.

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 ***jednotného*** centra EU;

b) přínosy, omezení a případná rizika;

ba) schopnost zajistit interoperabilitu a posoudit její přínos s ohledem na jiné příslušné systémy nahlašování, včetně směrnice (EU) 2016/1148.

c) prvky provozního řízení;

d) podmínky členství;

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

f) předběžné posouzení finančních nákladů vytvoření provozní platformy podporující ***jednotné*** 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 od data 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***, a rovněž poskytne všem příslušným finančním subjektům, pro které by to mohlo být užitečné, náležitě anonymizovanou zpětnou vazbu, náhled a analýzy na základě jakýchkoli obdržených hlášení o závažných incidentech souvisejících s IKT***.

2. Evropské orgány dohledu každoročně anonymizovaně a souhrnně informují prostřednictvím společného výboru o hlášeních ***závažných*** 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, ***odhadované*** náklady a přijatá nápravná opatření.

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

Článek 20a

Provozní nebo bezpečnostní incidenty související s platbami, které se týkají určitých finančních subjektů

Požadavky stanovené v této kapitole se v případech, kdy se týkající finančních subjektů uvedených v čl. 2 odst. 1 písm. a), b) a c), vztahují rovněž na provozní nebo bezpečností incidenty související s platbami a na závažné provozní a bezpečností incidenty související s platbami.

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 ***jiné než mikropodniky*** ▌ 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. ***Pokud testy provádí interní subjekt, vyčlení finanční subjekty dostatečné zdroje a zajistí, aby během fáze návrhu a provádění testu nedocházelo ke střetům zájmů.***

5. Finanční subjekty vytvoří postupy a strategie pro stanovení priorit, klasifikaci a ***řešení*** 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 zajistí***, aby byly*** alespoň jednou ročně ***provedeny náležité testy všech kritických systémů a aplikací*** IKT.

Článek 22

Testování nástrojů a systémů IKT

1. Program testování digitální provozní odolnosti uvedený v článku 21 stanoví provedení úplné škály vhodných testů***.***

Tyto testy mohou zahrnovat hodnocení a zkoumání zranitelnosti, ***analýzy*** otevřených zdrojů, posouzení zabezpečení sítě, ***analýzy*** nedostatků, ***přezkumy*** fyzického zabezpečení, ***dotazníky*** a ***antivirová softwarová*** řešení, v proveditelných případech ***přezkumy*** zdrojových kódů, ***testy*** na základě scénářů, testování kompatibility, testování výkonnosti***,*** testování mezi koncovými body nebo ***penetrační*** 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 ***odst. 3 druhého pododstavce*** provádějí alespoň jednou za tři roky pokročilé testování s využitím penetračního testování na základě hrozeb.

2. Penetrační testování na základě hrozeb pokrývá alespoň zásadní ***nebo důležité*** funkce a služby finančního subjektu a provádí se ***pokud možno*** za provozu na systémech skutečně využívaných ***nebo na předprodukčních systémech se stejnou konfigurací zabezpečení***. Přesný rozsah penetračního testování na základě hrozeb vycházející z posouzení zásadních ***nebo důležitých*** funkcí a služeb stanoví finanční subjekty a potvrdí příslušné orgány. ***Nevyžaduje se, aby jedno penetrační testování na základě hrozeb pokrývalo všechny zásadní nebo důležité funkce.***

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

   Jsou-li ***kritičtí*** poskytovatelé služeb IKT z řad třetích stran ***nebo případně nekritičtí poskytovatelé služeb IKT z řad třetích stran*** zařazeni do penetračního testování na základě hrozeb, přijme finanční subjekt nezbytná opatření pro zajištění účasti těchto poskytovatelů. ***Tito poskytovatelé služeb IKT z řad třetích stran nejsou povinni sdělovat informace či poskytovat podrobnosti ohledně položek, které nejsou relevantní pro kontroly příslušných kritických nebo důležitých služeb příslušných finančních subjektů prováděné v rámci řízení rizik. Toto testování nesmí mít nepříznivý dopad na jiné zákazníky poskytovatelů služeb IKT z řad třetích stran.***

   V případech, kdy by zapojení poskytovatele služeb IKT z řad třetích stran do provádění penetračního testování na základě hrozeb mohlo potenciálně mít dopad na kvalitu, důvěrnost nebo bezpečnost služeb IKT tohoto poskytovatele z řad třetích stran jiným zákazníkům, kteří nespadají do působnosti tohoto nařízení, nebo na celkovou integritu operací poskytovatele služeb IKT z řad třetích stran, mohou se finanční subjekt a poskytovatel služeb IKT z řad třetích stran smluvně dohodnout, že tento poskytovatel smí uzavřít smluvní ujednání přímo s externím testerem. Poskytovatelé služeb IKT z řad třetích stran mohou uzavřít taková ujednání jménem všech svých uživatelů služeb finančních subjektů s cílem provést společné testování.

   Finanční subjekty použijí účinné kontroly v rámci řízení rizik, aby ***zmírnily*** rizika jakéhokoliv případného dopadu na data, poškození aktiv a narušení zásadních ***nebo důležitých funkcí*** 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***jedinému veřejnému*** orgánu ***určenému v souladu s odstavcem 3a, nebo v případě, že poskytovatelé služeb IKT z řad třetích stran uzavřou smluvní ujednání přímo s externími subjekty provádějícími testování, agentuře ENISA, důvěrný souhrn výsledků testu a*** dokumentaci potvrzující, že bylo penetrační testování na základě hrozeb provedeno v souladu s požadavky. ***Jediný veřejný orgán nebo případně ENISA*** vydají osvědčení***, kterým potvrdí, že test byl proveden v souladu s požadavky stanovenými v dokumentaci, aby mohly příslušné orgány tyto penetrační testy na základě hrozeb vzájemně uznávat***. ***Osvědčení je sdíleno***

s příslušným orgánem finančního subjektu a případně s hlavním orgánem dohledu kritického poskytovatele služeb IKT z řad třetích stran.

3. Finanční subjekty ***nebo poskytovatelé služeb IKT z řad třetích stran, kterým je povoleno přímo uzavírat smluvní ujednání s externím subjektem provádějícím testování v souladu s odstavcem 2 tohoto článku,*** uzavřou ***za účelem provedení penetračních testů na základě hrozeb*** smlouvy s testery v souladu s článkem 24.

Aniž je dotčena jejich schopnost delegovat úkoly a pravomoci podle tohoto článku na jiné příslušné orgány odpovědné za penetrační testování na základě hrozeb, určí příslušné orgány 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.

3a. Členské státy určí jediný veřejný orgán, který bude na vnitrostátní úrovni odpovědný za penetrační testování na základě hrozeb ve finančním sektoru, s výjimkou určení finančních subjektů v souladu s odstavcem 3, včetně penetračního testování na základě hrozeb, které provádějí finanční subjekty a poskytovatelé služeb IKT z řad třetích stran, kteří přímo uzavírají smluvní ujednání s externími testery. Určenému jedinému veřejnému orgánu se za tímto účelem svěřují veškeré pravomoci a úkoly.

4. Evropské orgány dohledu***v koordinaci s ENISA,*** po konzultaci s ECB a s přihlédnutím k příslušným rámcům Unie platným pro penetrační testy na základě ***hrozeb a*** operativních informací***, včetně rámce TIBER-EU***, vypracují návrh ***souboru*** regulačních technických norem, který bude specifikovat:

a) kritéria použitá pro účely uplatňování ***odst. 3 druhého pododstavce*** tohoto článku;

b) požadavky týkající se:

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

ii) metodiky a postupů testování pro jednotlivé fáze procesu testování;

iii) výsledků a fáze ukončení testování a nápravy;

c) druh spolupráce v oblasti dohledu potřebný k provádění ***a usnadnění neomezeného vzájemného uznávání*** penetračního testování na základě hrozeb, pokud jde o finanční subjekty působící ve více než jednom členském státě ***a testování prováděného externími testery, kteří uzavřeli smluvní ujednání přímo s poskytovateli služeb IKT z řad třetích stran v souladu s odstavcem 2 tohoto článku***, 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 ***6 měsíců*** před datem 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 ***a poskytovatelé služeb IKT z řad třetích stran, kterým je povoleno přímo uzavřít smluvní ujednání s externím testerem v souladu s čl. 23 odst. 2,*** 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***, ať už jsou testery z Unie nebo ze třetí země***;

   d) ▌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) ▌jsou řádně a plně kryti příslušným pojištěním odpovědnosti za škody při výkonu povolání, včetně rizik pochybení a nedbalosti***;***

   ea) v případě interních testerů bylo jejich použití schváleno příslušným orgánem a jediným veřejným orgánem určeným v souladu s čl. 23 odst. 3a a tyto orgány ověřily, že finanční subjekt vyčlenil dostatečné zdroje a zajistil, že během fáze návrhu a provádění testu nedojde ke střetu zájmů.

2. Finanční subjekty ***a poskytovatelé služeb IKT z řad třetích stran, kterým je povoleno uzavírat přímo smluvní ujednání s externím testerem v souladu s čl. 23 odst. 2,*** 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) ***povahu,*** 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***;***

   ba) skutečnost, zda se v případě poskytovatele služeb IKT jedná o vnitroskupinového poskytovatele služeb IKT.

3. Finanční subjekty ***jiné než mikropodniky*** jako součást svého rámce pro řízení rizik v oblasti IKT přijmou a pravidelně revidují strategii pro rizika v oblasti IKT spojená s třetími stranami ▌. 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 ***podporujících zásadní nebo důležité funkce*** poskytovaných třetími stranami.

   Smluvní ujednání uvedená v prvním pododstavci se řádně zdokumentují ▌.

   Než vstoupí v platnost prováděcí technické normy uvedené v odstavci 10, řídí se finanční subjekty pokyny a dalšími opatřeními vydanými evropskými orgány dohledu a příslušnými orgány, jsou-li takové pokyny a opatření k dispozici.

   Finanční subjekty alespoň jednou ročně nahlásí příslušným orgánům informace o počtu nových ujednání o využívání služeb IKT ***podporujících zásadní nebo důležité funkce***,

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 ***aktuální*** normy v oblasti bezpečnosti informací. ***K nejnovějším normám se rovněž přihlíží při určování, zda jsou zavedené bezpečnostní normy vhodné.***

7. Finanční subjekty při výkonu práv na přístup, kontrolu a audit u poskytovatele služeb IKT z řad třetích stran***, pokud jde o zásadní nebo důležité funkce,*** 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 ***podrobných a*** 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, aby smluvní ujednání o využívání služeb IKT ***umožňovala finančním subjektům přijmout vhodná opravná nebo nápravná opatření, která by mohla zahrnovat úplné ukončení ujednání, není-li oprava možná, nebo částečné ukončení ujednání, je-li oprava možná, podle platného práva*** alespoň za těchto podmínek:

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

   aa) společný orgán dohledu vydal doporučení podle článku 37 kritickému poskytovateli služeb IKT z řad třetích stran;

   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 ***v rámci smlouvy s finančním subjektem*** 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 ***prokazatelně*** nedokáže dále efektivně dohlížet na finanční subjekt, které vzniknou v důsledku příslušného smluvního ujednání.

8a. S cílem omezit riziko narušení na úrovni finančního subjektu se za řádně odůvodněných podmínek a po dohodě s příslušnými orgány může finanční subjekt rozhodnout, že neukončí smluvní ujednání s poskytovatelem služeb IKT z řad třetích stran do doby, než je schopen v souladu se strategií ukončení smluvního vztahu uvedenou v odstavci 9 přejít k jinému poskytovateli služeb IKT z řad třetích stran nebo na vlastní řešení odpovídající složitostí poskytované služby.

8b. V případech, kdy jsou smluvní ujednání s poskytovateli služeb IKT z řad třetích stran ukončena za některé z podmínek uvedených v odst. 8 písm. a) až d), nenesou finanční subjekty náklady na přenos dat od třetí strany poskytující služby IKT, pokud tento přenos převyšuje náklady na přenos dat stanovené v původní smlouvě.

9. ***Pro služby IKT související se zásadními nebo důležitými funkcemi zavedou*** finanční subjekty strategie ukončení smluvního vztahu***, které budou pravidelně přezkoumávány. Strategie ukončení smluvního vztahu zohlední*** 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***, nebo v případě ukončení smluvních ujednání s poskytovateli služeb IKT z řad třetích stran za kterékoli z podmínek uvedených v odst. 8 písm. a) až d)***.

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 regulačních 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 [Úř. věst.: vložte datum ***18 měsíců*** 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 ***podporujícími zásadní nebo důležité funkce*** 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 ***podporujících zásadní nebo důležité funkce*** 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 ***podporujících zásad***ní ***nebo důležité funkce*** 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 ▌.

Jsou-li smluvní ujednání o využívání služeb IKT ***podporujících zásadní nebo důležité funkce*** uzavřena se třetí stranou poskytující služby IKT ▌, finanční subjekty považují za relevantní alespoň následující faktory:

a) ▌

b) ▌

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

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

Jsou-li smluvní ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce uzavřena se třetí stranou poskytující služby IKT usazenou ve třetí zemi, finanční subjekty kromě faktorů uvedených v prvním a druhém pododstavci rovněž zváží:

i) dodržování pravidel Unie o ochraně údajů; a

ii) účinné prosazování pravidel stanovených v tomto nařízení.

Pokud taková smluvní ujednání zahrnují subdodávky zásadních nebo důležitých funkcí, finanční subjekty posoudí, zda a jak mohou potenciální dlouhé nebo složité subdodavatelské řetězce ovlivnit jejich schopnost plně ***posoudit faktory uvedené ve druhém a třetím pododstavci za účelem sledování nasmlouvaných funkcí*** a ***schopnosti*** 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 ***písemně a je dostupná*** stranám ve fyzické formě, nebo ve formátu, který lze stáhnout a je přístupný.

2. ***Finanční subjekty a poskytovatele služeb IKT z řad třetích stran zajistí, aby*** smluvní ujednání o využívání služeb IKT ***obsahovaly*** minimálně:

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, ***konkrétně regiony nebo země,*** kde budou nasmlouvané nebo subdodavatelem zajišťované funkce a služby v oblasti IKT poskytovány a kde budou zpracovávána data, včetně místa jejich uchovávání, a povinnost třetí strany poskytující služby IKT oznámit ***předem*** finančnímu subjektu, plánuje-li změnu těchto míst;

c) ustanovení o přístupnosti, dostupnosti, integritě, bezpečnosti***, důvěrnosti*** a ochraně ***dat, včetně*** osobních údajů;

ca) ustanovení 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 ***nebo v případě ukončení smluvních ujednání***;

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) ▌

f) povinnost třetí strany poskytující služby IKT poskytnout v případě incidentu souvisejícího s IKT ***týkajícího se poskytované služby*** 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 zajistí ***odpovídající úroveň bezpečného*** poskytování služeb finančním subjektem v souladu s jeho regulačním rámcem;

h) ▌

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 dobu pro ukončení smlouvy v souladu s očekáváními příslušných orgánů ***a orgánů příslušných k řešení krize, a pokud má toto smluvní ujednání dopad na vnitroskupinového poskytovatele služeb IKT v rámci téže skupiny, analýzu založenou na posouzení rizik***;

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

i) během kterého bude třetí strana poskytující služby IKT s ohledem na snížení rizika výpadků u finančního subjektu ***nebo na zajištění účinného řešení a restrukturalizace*** nadále poskytovat příslušné funkce nebo služby;

ii) které umožní finančnímu subjektu podle složitosti poskytované služby změnit třetí stranu poskytující služby IKT, nebo přejít na vlastní řešení***;***

iia) pokud má smluvní ujednání dopad na vnitroskupinového poskytovatele služeb IKT v rámci téže skupiny, analyzuje se na základě posouzení rizik;

ka) ustanovení o zpracování osobních údajů poskytovatelem služeb IKT z řad třetích stran, které má být v souladu s nařízením (EU) 2016/679.

2a. Smluvní ujednání o poskytování zásadních nebo důležitých funkcí musí kromě odstavce 2 minimálně obsahovat:

a) 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;

b) 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 kontrolovat kopie příslušné dokumentace na místě, pokud jsou zásadní z hlediska provozu poskytovatele služeb IKT z řad třetích stran, přičemž výkon těchto práv

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 poskytovatele služeb IKT z řad třetích stran plně spolupracovat při kontrolách a auditech na místě a auditech prováděných příslušnými orgány, hlavním orgánem dohledu, finančním subjektem nebo určenou třetí stranou a podrobnosti o rozsahu, způsobech a četnosti těchto kontrol a auditů;

Odchylně od písmene b) se poskytovatel služeb IKT z řad třetích stran a finanční subjekt mohou dohodnout, že práva na přístup, kontrolu a audit mohou být přenesena na nezávislou třetí stranu jmenovanou poskytovatelem služeb IKT z řad třetích stran a že finanční subjekt může od této třetí strany kdykoli požadovat informace a ujištění o výkonnosti poskytovatele služeb IKT z řad třetích stran.

2b. Smluvní ujednání o poskytování služeb IKT poskytovatelem služeb IKT z řad třetích stran usazeným ve třetí zemi a označeným podle čl. 28 odst. 9 za kritického musí kromě odstavců 2 a 2a tohoto článku:

a) stanovit, že se smlouva řídí právem členského státu; a

b) zaručovat, že společný orgán dohledu a hlavní orgán dohledu mohou plnit úkoly uvedené v článku 30 na základě jejich pravomocí stanovených v článku 31.

Služby, pro něž jsou uzavřena smluvní ujednání, nemusí poskytovat podnik registrovaný v Unii podle práva členského státu.

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

3a. Příslušné orgány mají zajištěn přístup ke smluvním ujednáním uvedeným v tomto článku. Strany těchto smluvních ujednání se mohou dohodnout, že před poskytnutím přístupu příslušným orgánům utají obchodně citlivé nebo důvěrné informace, pokud jsou tyto orgány plně informovány o rozsahu a povaze utajení.

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). ***Při vypracovávání tohoto návrhu regulačních technických norem evropské orgány dohledu přihlédnou k velikosti finančních subjektů, povaze, rozsahu a složitosti jejich služeb, činností a operací a k jejich celkovému rizikovému profilu.***

Evropské orgány dohledu předloží tento návrh regulačních technických norem Komisi do [Úř. věst.: vložte datum ***18 měsíců*** 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 ***po konzultaci s ENISA*** prostřednictvím společného výboru a na základě doporučení ***orgánu*** 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.

   Hlavní orgán dohledu jmenovaný v souladu s písm. b) prvním pododstavcem odpovídá za každodenní dohled nad kritickou třetí stranou poskytující služby IKT.

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***;***

fa) závažnost a význam služeb poskytovaných příslušnou třetí stranu poskytující služby IKT.

2a. Společný orgán dohledu před zahájením svého posuzování pro účely určení uvedeného v odst. 1 písm. a) o tom třetí stranu poskytující služby IKT informuje.

Společný orgán dohledu informuje třetí stranu poskytující služby IKT o výsledku posouzení uvedeného v prvním pododstavci tím, že jí poskytne návrh doporučení ohledně jejího zařazení mezi kritické poskytovatele. Do šesti týdnů od data obdržení tohoto návrhu doporučení může třetí strana poskytující služby IKT předložit společnému orgánu dohledu odůvodněné prohlášení o posouzení. Toto odůvodněné prohlášení obsahuje veškeré důležité další informace, které třetí strana poskytující služby IKT považuje za vhodné s cílem podpořit úplnost a přesnost postupu určení nebo zpochybnit návrh doporučení ohledně jejího zařazení mezi kritické poskytovatele. Společný výbor evropských orgánů dohledu před přijetím rozhodnutí o určení toto odůvodněné prohlášení náležitě uváží a může si od třetí strany poskytující služby IKT vyžádat další informace nebo podklady.

Společný výbor evropských orgánů dohledu informuje třetí stranu poskytující služby IKT o tom, že ji určil jako kritickou. Třetí strana poskytující služby IKT má nejméně tři měsíce od data obdržení oznámení na provedení nezbytných úprav, aby mohl společný orgán dohledu plnit své úkoly podle článku 30, a na informování finančních subjektů, kterým tato třetí strana poskytující služby IKT poskytuje služby. Společný orgán dohledu může v případě, že jej o to třetí strana poskytující služby IKT požádá a řádně odůvodní, povolit prodloužení této lhůty o maximálně tři měsíce.

3. Komisi je svěřena pravomoc přijmout akt v přenesené pravomoci v souladu s článkem 50 k ***další specifikaci*** 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. ***Společný orgán dohledu po konzultaci s ENISA vypracuje***, zveřejní a ***pravidelně aktualizuje*** 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 ***společnému orgánu*** dohledu vytvořenému v souladu s článkem 29. ***Společný orgán*** dohledu posoudí na základě informací obdržených od příslušných orgánů závislost finančních subjektů na třetích stranách v oblasti 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.

8a. Společný výbor evropských orgánů dohledu na doporučení společného orgánu dohledu určí třetí strany poskytující služby IKT usazené ve třetí zemi, které jsou kritické pro finanční subjekty v souladu s odst. 1 písm. a).

Při určování podle prvního pododstavce tohoto odstavce se evropské orgány dohledu a společný orgán dohledu řídí procedurálními kroky stanovenými v odstavci 2a.

9. Finanční subjekty nesmí využívat ***kritickou*** třetí stranu poskytující služby IKT usazenou ve třetí zemi***, pokud tato třetí strana poskytující služby IKT nemá podnik registrovaný v Unii podle práva členského státu a neuzavřela smluvní ujednání v souladu s čl. 27 odst. 2b***.

Článek 29

Struktura rámce dohledu

1. ***Společný orgán dohledu je vytvořen*** pro účely podpory ***dohledu***, co se týče rizik v oblasti IKT spojených s třetími stranami ve všech finančních odvětvích a ***provádění přímého dohledu nad třetími stranami poskytujícími služby IKT určenými podle článku 28 za kritické***.

   Úloha společného orgánu dohledu je omezena na pravomoci dohledu týkající se rizik spojených s IKT při poskytování služeb v oblasti IKT ze strany kritických třetích stran poskytujících služby IKT finančním subjektům.

   Společný orgán 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. ***Společný orgán*** 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.

   Společný orgán 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.

3. ***Společný orgán*** dohledu se skládá z ***výkonných ředitelů*** evropských orgánů dohledu***,*** jednoho zástupce na vysoké úrovni z řad stávajících zaměstnanců ***evropských orgánů dohledu a jednoho zástupce na vysoké úrovni z nejméně osmi příslušných vnitrostátních orgánů***. ▌Jako pozorovatelé se účastní rovněž po jednom zástupci z Evropské komise, ESRB, ECB a ENISA ***a nejméně jeden nezávislý odborník jmenovaný v souladu s odstavcem 3a tohoto článku***.

Po každoročním určení kritických poskytovatelů služeb IKT z řad třetích stran podle čl. 28 odst. 1 písm. a) rozhodne společný výbor evropských orgánů dohledu o tom, které příslušné vnitrostátní orgány budou členy společného orgánu dohledu, a to s přihlédnutím k těmto faktorům:

a) počet kritických poskytovatelů služeb IKT z řad třetích stran, kteří jsou usazeni nebo poskytují služby v daném členském státě,

b) do jaké míry využívají finanční subjekty v členském státě kritické poskytovatele služeb IKT z řad třetích stran,

c) odborné znalosti příslušného vnitrostátního orgánu,

d) dostupné zdroje a kapacita příslušného vnitrostátního orgánu,

e) nutnost, aby bylo fungování a rozhodování společného orgánu dohledu efektivní, jednoduché a účelné.

Společný orgán dohledu sdílí svou dokumentaci a rozhodnutí se všemi příslušnými vnitrostátními orgány, které nejsou členy společného orgánu dohledu.

Společnému orgánu dohledu jsou při jeho činnosti nápomocni vyhrazení pracovníci evropských orgánů dohledu.

3a. Nezávislého odborníka uvedeného v odstavci 3 tohoto článku jmenuje společný orgán dohledu pozorovatelem po provedení veřejného a transparentního výběrového procesu.

Tento nezávislý odborník je jmenován na období dvou let na základě svých odborných znalostí v oblasti finanční stability, digitální provozní odolnosti a otázek bezpečnosti IKT.

Jmenovaný nezávislý odborník nezastává žádnou funkci na vnitrostátní, unijní či mezinárodní úrovni. Jedná nezávisle a objektivně ve výlučném zájmu Unie jako celku a nevyžaduje ani nepřijímá pokyny od orgánů či subjektů Unie, od vlád členských států ani od jiných veřejných či soukromých subjektů.

Společný orgán dohledu se může rozhodnout jmenovat více než jednoho nezávislého odborného pozorovatele.

4. 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 ***do [Úř. věst.: vložte datum 18 měsíců po vstupu tohoto nařízení v platnost]*** pokyny pro spolupráci mezi ***společným orgánem dohledu, hlavním orgánem dohledu*** a příslušnými orgány

týkající se podrobných postupů a podmínek souvisejících s výkonem úkolů příslušných orgánů a ***společného orgánu dohledu*** a podrobností o výměně informací, jež příslušné orgány potřebují k zajištění dodržování doporučení vydaných ***společným orgánem dohledu*** podle čl. 31 odst. 1 písm. d) kritickým poskytovatelům služeb IKT z řad třetích stran.

5. 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.

6. ***Společný orgán dohledu*** ▌ každý rok předloží Evropskému parlamentu, Radě a Komisi zprávu o uplatňování tohoto oddílu.

Článek 30

Úkoly hlavního orgánu dohledu

1. Hlavní orgán dohledu***, jmenovaný podle čl. 28 odst. 1 písm. b), vede a koordinuje každodenní dohled nad kritickými poskytovateli služeb IKT z řad třetích stran a je pro tyto poskytovatele hlavním kontaktním místem.***

1a. ***Hlavní orgán dohledu*** posoudí, zda jednotliví kritičtí poskytovatelé služeb IKT z řad třetích stran disponují komplexními, jasnými a účinnými pravidly, postupy, mechanismy a ujednáními pro řízení rizik v oblasti IKT, jež mohou představovat pro finanční subjekty. ***Toto posouzení se zaměří především na služby IKT podporující kritické nebo důležité funkce, které kritický poskytovatel služeb IKT z řad třetích stran poskytuje finančním subjektům, avšak může být i širší, pokud je to pro posouzení rizik pro tyto funkce relevantní.***

2. Posouzení uvedené v odstavci 1***a*** zahrnuje:

   a) požadavky v oblasti IKT k zajištění zejména bezpečnosti, dostupnosti, kontinuity, škálovatelnosti a kvality služeb, které kritický poskytovatel služeb IKT z řad třetích stran 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 ***závažných*** 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. Na základě hodnocení uvedeného v odstavci 1***a provedeného hlavním orgánem dohledu společný orgán dohledu v koordinaci a pod vedením hlavního orgánu dohledu vypracuje a navrhne*** jasné, podrobné a odůvodněné individuální plány dohledu pro jednotlivé kritické poskytovatele služeb IKT z řad třetích stran.

Společný orgán dohledu konzultuje při vypracovávání návrhu plánu dohledu se všemi relevantními příslušnými orgány a jednotnými kontaktními místy uvedenými v článku 8 směrnice (EU) 2016/1148, aby bylo zajištěno, že nedochází k nesouladu s povinnostmi kritických poskytovatelů služeb IKT z řad třetích stran stanovenými v této směrnici ani k jejich zdvojování.

Plán dohledu přijímá každoročně správní rada hlavního orgánu dohledu.

Před přijetím je návrh plánu dohledu sdělen kritickému poskytovateli služeb IKT z řad třetích stran.

Po obdržení návrhu plánu dohledu má kritický poskytovatel služeb IKT z řad třetích stran lhůtu šesti týdnů, během které návrh plánu dohledu posoudí a předloží k němu odůvodněné vyjádření. Toto odůvodněné vyjádření může předložit pouze, pokud je kritický poskytovatel služeb IKT z řad třetích stran schopen předložit důkazy o tom, že provádění plánu dohledu by mělo nepřiměřený dopad nebo představovalo nepřiměřené narušení ve vztahu k zákazníkům, na něž se toto nařízení nevztahuje, nebo že existuje účinnější nebo účelnější řešení pro řízení zjištěných rizik IKT. Pokud je takové vyjádření předloženo, navrhne kritický poskytovatel služeb IKT z řad třetích stran společnému orgánu dohledu účinnější či účelnější řešení, jak dosáhnout cílů uvedených v návrhu plánu dohledu.

Před přijetím plánu dohledu správní rada hlavního orgánu dohledu toto odůvodněné vyjádření řádně posoudí a může si od poskytovatele služeb IKT z řad třetích stran vyžádat další informace nebo doklady.

4. Po ***přijetí*** a oznámení plánů dohledu uvedených v odstavci 3 kritickým poskytovatelům služeb IKT z řad třetích stran mohou příslušné orgány přijímat opatření týkající se kritických poskytovatelů služeb IKT z řad třetích stran pouze po dohodě se ***společným orgánem dohledu***.

Článek 31

Pravomoci dohledu

1. Pro účely provádění povinností stanovených v tomto oddíle disponuje hlavní orgán dohledu těmito pravomocemi***, pokud jde o služby poskytované kritickými poskytovateli služeb IKT z řad třetích stran finančním subjektům***:

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

b) provádět obecná šetření a kontroly ***na místě*** podle článků 33 a 34;

c) požadovat zprávy po dokončení činností dohledu, kde jsou uvedena provedená opatření nebo nápravné prostředky uplatněné kritickými poskytovateli služeb IKT z řad třetích stran v souvislosti s doporučeními uvedenými v ***odstavci 1a***;

1a. Pro účely provádění povinností stanovených v tomto oddíle a na základě informací získaných hlavním orgánem dohledu a výsledků vyšetřování prováděného hlavním

orgánem dohledu disponuje společný orgán dohledu pravomocí 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 ***společný 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 kritičtí poskytovatelé služeb IKT z řad třetích stran poskytují své služby finančním subjektům a které ***společný 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 kritičtí poskytovatelé služeb IKT z řad třetích stran plánují uzavřít s dalšími poskytovateli služeb IKT z řad třetích stran nebo subdodavateli IKT usazenými ve třetí zemi, všechna plánovaná externí zajišťování služeb, včetně subdodávek, u nichž se ***společný 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 poskytovatelem služeb IKT z řad třetích stran nebo subdodavatelem IKT usazeným ve třetí zemi ***a nemá podnik založený v Unii podle práva některého členského státu***;

– subdodávky se týkají zásadní nebo důležité funkce finančního subjektu;

– ***subdodávky představují vážná a jasná rizika pro finanční subjekt nebo finanční stabilitu finančního systému Unie.***

1b. Pravomoci uvedené v odstavcích 1 a 1a se s ohledem na služby IKT podporující jiné než kritické nebo důležité funkce, které poskytuje kritický poskytovatel služeb IKT z řad třetích stran, uplatňují v případě potřeby.

1c. Aby nedocházelo ke zbytečnému zdvojování technických a organizačních opatření, která se mohou vztahovat na kritické poskytovatele služeb IKT z řad třetích stran podle směrnice (EU) 2016/1148, přihlíží hlavní orgán dohledu a společný orgán dohledu při uplatňování pravomocí uvedených v odstavcích 1 a 1a tohoto článku řádně k rámci stanovenému v uvedené směrnici a v případě nutnosti konzultují relevantní příslušné orgány zřízené touto směrnicí.

2. ***Společný orgán dohledu před finalizací a vydáním doporučení v souladu s odstavcem 1a informuje o svých záměrech kritického poskytovatele služeb IKT z řad třetích stran a umožní kritickému poskytovateli služeb IKT z řad třetích stran předložit informace, o nichž se důvodně domnívá, že by měly být zohledněny před finalizací doporučení,***

nebo za účelem vyslovení připomínek k zamýšleným doporučením. Mezi důvody pro vyslovení připomínek k doporučení může patřit skutečnost, že by mělo nepřiměřený dopad nebo představovalo nepřiměřené narušení ve vztahu k zákazníkům, na něž se toto nařízení nevztahuje, nebo že existuje účinnější nebo účelnější řešení pro řízení zjištěných rizik.

3. Kritičtí poskytovatelé služeb IKT z řad třetích stran v dobré víře spolupracují s hlavním orgánem dohledu ***a se společným orgánem dohledu*** a pomáhají ***jim*** při plnění ***jejich*** úkolů.

4. Hlavní orgán dohledu může ***v případě úplného nebo částečného nedodržování opatření, která mají být přijata v souladu s odst. 1 písm. a), b) nebo c), a po vypršení lhůty nejméně 60 kalendářních dnů od data, kdy kritický poskytovatel služeb IKT z řad třetích stran obdržel oznámení o tomto opatření,*** ukládat opakované pokuty, aby přiměl kritického poskytovatele služeb IKT z řad třetích stran dodržovat ***daná*** ustanovení.

4a. ***Opakované pokuty uvedené v odstavci 4 ukládá hlavní orgán dohledu pouze v krajním případě a tehdy, když kritický poskytovatel služeb IKT z řad třetích stran nedodržel opatření požadovaná v souladu s odst. 1 písm. a), b) nebo 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 kritického poskytovatele služeb IKT z řad třetích stran.

6. Výše opakovaných pokut vypočítaná od data uvedeného v rozhodnutí o uložení opakovaných pokut činí ***až*** 1 % průměrného denního celosvětového obratu daného kritického poskytovatele služeb IKT z řad třetích stran v předcházejícím obchodním roce ***v oblasti služeb poskytovaných finančním subjektům, na něž se vztahuje toto nařízení***.

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 kritického poskytovatele služeb IKT z řad třetích stran, jíž se řízení týká, slyšení ohledně zjištění a svá rozhodnutí založí pouze na zjištěních, k nimž měl kritický poskytovatel služeb IKT z řad třetích stran, kterého 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

poskytovatele služeb IKT z řad třetích stran, 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 kritický poskytovatel služeb IKT z řad třetích stran externě zadal zajišťování provozních funkcí nebo činnosti.

Kritičtí poskytovatelé služeb IKT z řad třetích stran mají povinnost poskytnout informace uvedené v prvním pododstavci pouze s ohledem na služby poskytované finančním subjektům, na které se vztahuje toto nařízení a které využívají služby kritických poskytovatelů služeb IKT z řad třetích stran pro kritické nebo důležité funkce. Kritičtí poskytovatelé služeb IKT z řad třetích stran informují příslušný finanční subjekt o žádostech, které se jej týkají.

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 kritického poskytovatele služeb IKT z řad třetích stran, od něhož 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 ***přiměřenou*** lhůtu, v níž mají být informace poskytnuty;

   e) upozorní na pokuty stanovené v čl. 31 odst. 4, pokud budou poskytnuté informace neúplné ***nebo pokud nebudou tyto informace poskytnuty ve lhůtě stanovené v písm. d)***;

   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 poskytovatelů služeb IKT z řad třetích stran jsou povinni požadované informace dodat. Informace za své klienty mohou sdělit řádně zmocnění právní zástupci. Kritický poskytovatel služeb IKT z řad třetích stran 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 poskytovatelů služeb IKT z řad třetích stran.

Článek 33

Obecná šetření

1. Aby mohl provádět své povinnosti podle tohoto nařízení, může hlavní orgán dohledu s pomocí vyšetřovacího týmu podle čl. ***35*** odst. 1 provádět nezbytná šetření kritických poskytovatelů služeb IKT z řad třetích stran ***v souladu se zásadou proporcionality. Při provádění šetření postupuje hlavní orgán dohledu obezřetně a zajistí ochranu práv zákazníků kritických poskytovatelů služeb IKT z řad třetích stran, na něž se toto nařízení nevztahuje, a to i v souvislosti s dopadem na úroveň služeb, dostupnost údajů a důvěrnost informací***:

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) ***provádět zabezpečený přezkum*** ověřených kopií takových záznamů, údajů, postupů a jiných materiálů nebo výpisů z nich;

   c) předvolat zástupce poskytovatele služeb IKT z řad třetích stran 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 poskytovatele služeb IKT z řad třetích stran, nebo nebudou-li úplné.

4. Zástupci poskytovatelů služeb IKT z řad třetích stran 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 tohoto poskytovatele služeb IKT z řad třetích stran 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 poskytovatelů služeb IKT z řad třetích stran, jako jsou jejich sídla, provozní střediska, druhotná pracoviště, a rovněž může provádět kontroly na

dálku.

Pravomoc provádět kontroly na místě uvedená v prvním pododstavci se neomezuje na místa v Unii za předpokladu, že kontrola místa ve třetí zemi splňuje všechny tyto požadavky:

- ***je nezbytná proto, aby hlavní orgán dohledu splnil své povinnosti podle tohoto nařízení;***
- ***má přímou souvislost s poskytováním služeb IKT finančním subjektům Unie;***
- ***je relevantní pro některé probíhající šetření.***

1a. Při provádění kontrol na místě hlavní orgán dohledu a vyšetřovací tým postupují obezřetně a zajistí ochranu práv zákazníků kritických poskytovatelů služeb IKT z řad třetích stran, na něž se toto nařízení nevztahuje, a to i pokud jde o dopad na úroveň služeb, dostupnost údajů a důvěrnost informací.

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 poskytovatelů služeb IKT z řad třetích stran kontrole nepodrobí.

3. Hlavní orgán dohledu informuje s dostatečným předstihem před kontrolou příslušné orgány finančních subjektů využívajících tohoto poskytovatele služeb IKT z řad třetích stran.

4. Kontroly se týkají všech relevantních systémů IKT, sítí, zařízení, informací a dat***, která hlavní orgán dohledu považuje za vhodná a technologicky relevantní,*** ať už jsou používána nebo přispívají k poskytování služeb finančním subjektům.

5. Hlavní orgán dohledu před jakoukoliv plánovanou ***kontrolou*** na místě zašle kritickým poskytovatelům služeb IKT z řad třetích stran 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. Kritický poskytovatel služeb IKT z řad třetích stran 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 kritický poskytovatel služeb IKT z řad třetích stran odmítá podrobit se kontrole nařízené podle tohoto článku, hlavní orgán dohledu informuje ***kritického poskytovatele služeb IKT z řad třetích stran*** o důsledcích tohoto odporu, včetně možnosti, že příslušné orgány dotčených finančních subjektů ukončí smluvní ujednání uzavřená s tímto kritickým poskytovatelem služeb IKT z řad třetích stran.

Článek 35

Průběžný dohled

1. Hlavnímu orgánu dohledu je při provádění obecných šetření nebo kontrol na místě nápomocen vyšetřovací tým vytvořený pro každého kritického poskytovatele služeb IKT z řad třetích stran.

2. Společný vyšetřovací tým uvedený v odstavci 1 bude tvořit maximálně 10 členů z řad pracovníků hlavního orgánu dohledu***, ostatních evropských orgánů dohledu*** a příslušných orgánů dohledu nad finančními subjekty, jimž daný kritický poskytovatel služeb IKT z řad třetích stran 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 tyto návrhy 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. ***Společný orgán dohledu*** do 3 měsíců po dokončení šetření nebo kontroly na místě přijme doporučení, která budou adresována kritickému poskytovateli služeb IKT z řad třetích stran podle pravomocí uvedených v článku 31.

5. Doporučení uvedená v odstavci 4 budou neprodleně sdělena kritickému poskytovateli služeb IKT z řad třetích stran a příslušným orgánům finančních subjektů, jimž dodává služby.

   Pro účely plnění činností dohledu může ***společný orgán dohledu*** přihlédnout ke všem relevantním osvědčením třetích stran a interním nebo externím auditním zprávám třetích stran v oblasti IKT předloženým kritickým poskytovatelem služeb IKT z řad třetích stran.

Článek 36

Harmonizace podmínek umožňujících provádění dohledu

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

   a) informace, jež mají být předloženy kritickým poskytovatelem služeb IKT z řad třetích stran 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 kritický poskytovatel služeb IKT z řad třetích stran předložit, zveřejnit nebo nahlásit podle čl. 31 odst. 1;

d) podrobnosti o vyhodnocení opatření přijatých kritickými poskytovateli služeb IKT z řad třetích stran na základě doporučení ***společného orgánu dohledu*** podle čl. 37 odst. 2 příslušnými orgány.

2. Evropské orgány dohledu předloží tyto návrhy 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. Kritičtí poskytovatelé služeb IKT z řad třetích stran do 30 kalendářních dnů od přijetí doporučení vydaných ***společným orgánem dohledu*** podle čl. 31 odst. ***1a*** oznámí ***společnému orgánu dohledu***, zda mají v úmyslu se těmito doporučeními řídit. ***Společný orgán dohledu*** tuto informaci neprodleně předá příslušným orgánům ***daných finančních subjektů***.

2. Příslušné orgány ***informují finanční subjekty, které uzavřely smluvní ujednání s kritickými poskytovateli služeb IKT z řad třetích stran, o rizicích zjištěných v doporučeních vydaných těmto kritickým poskytovatelům služeb IKT z řad třetích stran společným orgánem dohledu v souladu s čl. 31 odst. 1a a*** sledují, zda finanční subjekty tato rizika zohledňují. ***Společný orgán dohledu sleduje, zda se kritičtí poskytovatelé služeb IKT z řad třetích stran zabývají riziky zjištěnými v těchto doporučeních.***

3. ***Pokud nelze regulační cíle zajistit jinými opatřeními a příslušné vnitrostátní orgány vydaly dotčeným finančním subjektům varování na základě informací sdělených společným orgánem dohledu, může správní rada hlavního orgánu dohledu rozhodnout na základě doporučení společného orgánu dohledu a po konzultaci s*** příslušnými orgány ***dotčených*** finančních subjektů, že částečně či úplně přestanou využívat služby dodávané ***finančním subjektům vystaveným rizikům uvedeným v doporučeních adresovaných kritickým poskytovatelům služeb IKT z řad třetích stran,*** a to do doby, ***než tato*** rizika odstraní. Bude-li to nutné, mohou ***v krajním případě kritické poskytovatele služeb IKT z řad třetích stran*** požádat, aby zcela či zčásti ukončily příslušná smluvní ujednání uzavřená s ***finančními subjekty vystavenými zjištěným rizikům***.

4. ***Správní rada hlavního orgánu dohledu*** při přijímání rozhodnutí podle odstavce 3 zohlední druh a rozsah rizik, která kritický poskytovatel služeb IKT z řad třetích stran neodstranil, a rovněž závažnost porušení předpisů, přičemž přihlédne 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 kritického poskytovatele služeb IKT z řad třetích stran;

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.

da) zda přerušení nebo ukončení poskytování služeb představuje riziko pro zajištění kontinuity činnosti pro uživatele služeb kritického poskytovatele služeb IKT z řad třetích stran.

4a. Rozhodnutí podle odstavce 3 je vykonatelné až poté, co o něm byly řádně informovány všechny dotčené finanční subjekty. Dotčeným finančním subjektům je poskytnuta lhůta, která nepřekročí rámec toho, co je nezbytně nutné, aby mohly upravit svá dodavatelská a smluvní ujednání s kritickými poskytovateli služeb IKT z řad třetích stran tak, aby neohrožovaly digitální provozní odolnost a uskutečňovaly strategie ukončení smluvního vztahu a plány přechodu uvedené v článku 25.

Kritičtí poskytovatelé služeb IKT z řad třetích stran, na něž se vztahují rozhodnutí podle odstavce 3, s dotčenými finančními subjekty plně spolupracují.

5. Příslušné orgány pravidelně informují ***společný orgán dohledu*** o přístupech a opatřeních přijatých v rámci jejich pracovních úkolů týkajících se finančních subjektů.

Článek 38

Poplatky za dohled

1. Evropské orgány dohledu naúčtují kritickým poskytovatelům služeb IKT z řad třetích stran 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 kritickému poskytovateli služeb IKT z řad třetích stran bude zahrnovat všechny výdaje ***spojené s výkonem povinností stanovených v tomto oddíle*** a bude poměrná k obratu poskytovatele služeb IKT.

1a. Pokud je uzavřeno správní ujednání s regulačním a dohledovým orgánem třetí země v souladu s odstavcem 1 tohoto článku, může být tento orgán součástí vyšetřovacího týmu uvedeného v čl. 35 odst. 1.

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 ***se snaží*** si mezi sebou ***a s poskytovateli služeb IKT z řad třetích stran*** 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 ***a poskytovatelů služeb IKT z řad třetích stran***, 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 ***a poskytovatelů služeb IKT z řad třetích stran***;

   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[26] a dodržování pokynů týkajících se hospodářské soutěže[27].

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.

[26] 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).

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

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 ***a osob nabízejících kryptoaktiva***, vydavatelů tokenů vázaných k vlastnictví aktiv ***a osob nabízejících tyto tokeny*** 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 ***a provozovatelů systémů vypořádání 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;

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;

g) v případě správců kritických referenčních hodnot příslušný orgán určený v souladu s články 40 a 41 nařízení ***(EU) 2016/1011***;

r) v případě poskytovatelů služeb skupinového financování příslušný orgán určený v souladu s článkem ***29*** nařízení ***(EU) 2020/1503***;

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, ***jsou*** evropské orgány dohledu a příslušné orgány ***přizvány k účasti na činnosti skupiny pro spolupráci, pokud se tato činnost týká dozoru, resp. dohledu nad subjekty uvedenými v bodě 7 přílohy II směrnice (EU) 2016/1148, které byly podle článku 28 tohoto nařízení označeny také za kritické poskytovatele služeb IKT z řad třetích stran***.

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.

2a. Hlavní orgán dohledu informuje příslušné orgány stanovené směrnicí (EU) 2016/1148 před prováděním obecných šetření a kontrol na místě podle článku 33 a 34 tohoto nařízení a spolupracuje se nimi.

Článek 43

Cvičení, komunikace a spolupráce ve finančním sektoru

1. Evropské orgány dohledu mohou prostřednictvím společného výboru a ve spolupráci s příslušnými orgány, ECB***, Jednotným výborem pro řešení krizí, pokud jde o informace týkající se subjektů spadajících do působnosti nařízení (EU) č. 806/2014,*** 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 ***významné kybernetické*** 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, ECB***, orgány členských států příslušné k řešení krizí a Jednotný výbor pro řešení krizí, pokud jde o informace týkající se subjektů spadajících do působnosti nařízení (EU) č. 806/2014,*** 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 ***považovaných*** 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 ***12 měsíců*** 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, ***uložených sankcích a výjimečně i*** totožnosti odpovědných osob.

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]. ***Komise vypracuje nejpozději devět měsíců před koncem tohoto pětiletého období zprávu o výkonu přenesení pravomoci. Přenesení pravomoci se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament ani Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.***

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 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 ***tří*** 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 ***tři*** 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. ***Tato zpráva přezkoumá alespoň následující body:***

a) ***možnost rozšíření rozsahu působnosti tohoto nařízení na provozovatele platebních systémů;***

b) ***dobrovolnou povahu hlášení závažných kybernetických hrozeb;***

c) kritéria určování kritických poskytovatelů služeb IKT z řad třetích stran v čl. 28 odst. 2; ***a***

d) ***efektivitu rozhodování společného orgánu dohledu a výměny informací mezi společným orgánem dohledu a nečlenskými příslušnými vnitrostátními orgány.***

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 (EU) 2021/xx Evropského parlamentu a Rady […] (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].“;

▌

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 – ***24*** 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.

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*

POSTUP V PŘÍSLUŠNÉM VÝBORU

Název	Digitální provozní odolnost ve finančním sektoru a změna nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014
Referenční údaje	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Datum předložení Parlamentu	24.9.2020
Příslušný výbor Datum oznámení na zasedání	ECON 17.12.2020
Výbory požádané o stanovisko Datum oznámení na zasedání	ITRE IMCO 17.12.2020 17.12.2020
Nezaujetí stanoviska Datum rozhodnutí	ITRE IMCO 15.10.2020 27.10.2020
Zpravodajové Datum jmenování	Billy Kelleher 15.10.2020
Projednání ve výboru	14.4.2021 14.6.2021
Datum přijetí	1.12.2021
Výsledek konečného hlasování	+: 44 –: 5 0: 5
Členové přítomní při konečném hlasování	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Náhradníci přítomní při konečném hlasování	Lefteris Christoforou
Datum předložení	7.12.2021

JMENOVITÉ KONEČNÉ HLASOVÁNÍ V PŘÍSLUŠNÉM VÝBORU

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Lefteris Nikolaou-Alavanos

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se