**EVROPSKÁ UNIE**

**EVROPSKÝ PARLAMENT** **RADA**

**Brusel 17. listopadu 2022**
**(OR. en)**

**2020/0266 (COD)** **PE-CONS 41/22**

**EF 197**
**ECOFIN 699**
**TELECOM 308**
**CYBER 249**
**CODEC 1071**

**PRÁVNÍ PŘEDPISY A JINÉ AKTY**

| | |
|---|---|
| Předmět: | 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, (EU) č. 909/2014 a (EU) 2016/1011 |

**NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY**

**(EU) 2022/…**

**ze dne ...**

**o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011**

**(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[1],

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[2],

v souladu s řádným legislativním postupem[3],

---

1 Úř. věst. C 343, 26.8.2021, s. 1.
2 Úř. věst. C 155, 30.4.2021, s. 38.
3 Postoj Evropského parlamentu ze dne 10. listopadu 2022. (dosud nezveřejněný v Úředním věstníku) a rozhodnutí Rady ze dne ...

vzhledem k těmto důvodům:

(1) V digitálním věku podporují informační a komunikační technologie (IKT) složité systémy používané pro každodenní činnosti. Udržují v chodu klíčová odvětví našich ekonomik, včetně finančního sektoru, a zlepšují fungování vnitřního trhu. Vyšší míra digitalizace a vzájemné propojenosti rovněž násobí riziko v oblasti IKT, kvůli němuž se celá společnost, a zejména finanční systém, stávají zranitelnějšími vůči kybernetickým hrozbám nebo narušením v oblasti IKT. I když všudypřítomné používání systémů IKT a vysoká míra digitalizace a propojení dnes tvoří základní charakteristiku činnosti finančních subjektů Unie, jejich digitální odolnost je nutné ještě lépe řešit a začlenit do jejich širších provozních rámců.

(2) Používání IKT získalo v posledních desetiletích při poskytování finančních služeb klíčovou úlohu, a to do té míry, že dnes má zásadní význam při provádění obvyklých běžných funkcí všech finančních subjektů. Digitalizace se nyní týká například 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. Vzhledem k používání IKT se proměnilo rovněž pojišťovnictví, od vzniku zprostředkovatelů pojištění nabízejících své služby online s využitím technologií v pojišťovnictví až po digitální uzavírání pojištění. Finanční sektor nejenže se digitalizoval jako celek, ale v důsledku digitalizace se rovněž prohloubila jeho vzájemná 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 potvrdila, jak stávající vysoká míra vzájemného propojení finančních subjektů, finančních trhů a infrastruktur finančních trhů, a zejména vzájemná závislost jejich systémů IKT, by mohla potenciálně představovat systémovou zranitelnost, protože se kybernetické incidenty vzniklé v jednom místě mohou bez omezení geografickými hranicemi rychle rozšířit z kteréhokoliv z přibližně 22 000 finančních subjektů Unie na celý finanční systém. Závažná narušení IKT, k nimž dochází ve finančním sektoru, nedopadají pouze na izolované finanční subjekty. Rovněž usnadňují šíření lokalizovaných zranitelností napříč finančními přenosovými kanály a potenciálně vytvářejí negativní důsledky pro stabilitu finančního systému Unie, neboť vedou například k hromadným výběrům hotovosti a celkové ztrátě jistoty a důvěry na finančních trzích.

(4) Riziko v oblasti IKT v poslední době přitahuje pozornost mezinárodních, unijních a vnitrostátních tvůrců politik, regulátorů a standardizačních orgánů, které se snaží o zlepšení digitální odolnosti, stanovení norem a koordinaci regulatorních a dohledových činností. Na mezinárodní úrovni se Basilejský výbor pro bankovní dohled, Výbor pro platební styk a tržní infrastrukturu, Rada pro finanční stabilitu, Institut pro finanční stabilitu a rovněž skupiny G7 a G20 zaměřují na to, aby příslušným orgánům a účastníkům trhu v různých jurisdikcích poskytly nástroje pro posílení odolnosti jejich finančních systémů. Tato práce je rovněž motivována potřebou řádně zohlednit riziko v oblasti IKT v kontextu vysoce propojeného globálního finančního systému a usilovat o větší konzistentnost příslušných osvědčených postupů.

(5) Přes cílené politické a legislativní iniciativy na unijní i vnitrostátní úrovni představuje riziko v oblasti IKT problém pro provozní odolnost, výkonnost a stabilitu finančního systému Unie. Reformy, které následovaly po finanční krizi z roku 2008, primárně posílily finanční odolnost finančního sektoru Unie a zaměřovaly se na zajištění konkurenceschopnosti a stability Unie z hlediska ekonomiky, obezřetnosti a chování trhu. Přestože jsou bezpečnost IKT a digitální odolnost součástí operačního rizika, regulatorní agenda se jim po finanční krizi věnovala méně, přičemž byly rozvíjeny pouze v některých oblastech strategického a regulatorního rámce finančních služeb Unie nebo jen v několika málo členských státech.

(6) Ve svém sdělení ze dne 8. března 2018 nazvaném „Akční plán pro finanční technologie: Za konkurenceschopnější a inovativnější evropský finanční sektor“ Komise zdůraznila, že je nanejvýš důležité zlepšit odolnost finančního sektoru Unie, mimo jiné z provozního hlediska, aby byla zajištěna jeho technologická bezpečnost a správné fungování, jeho rychlé zotavení z narušení a incidentů souvisejících s IKT a aby v konečném důsledku mohly být finanční služby efektivně a bezproblémově poskytovány v celé Unii, a to i v krizových situacích, a aby byla současně zachována důvěra spotřebitelů a trhu.

(7) V dubnu 2019 Evropský orgán dohledu (Evropský orgán pro bankovnictví) (EBA) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1093/2010[1], Evropský orgán dohledu (Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění) (EIOPA) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1094/2010[2] a Evropský orgán dohledu (Evropský orgán pro cenné papíry a trhy) (ESMA) zřízený nařízením Evropského parlamentu a Rady (EU) č. 1095/2010[3] (společně označovány jako „evropské orgány dohledu“) společně vydaly technické doporučení, ve kterém vyzvaly k jednotnému přístupu k riziku v oblasti IKT ve finančním sektoru a doporučily odpovídajícím způsobem posílit digitální provozní odolnost odvětví finančních služeb prostřednictvím iniciativy Unie zaměřené na toto odvětví.

---

1 Nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovnictví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

2 Nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro pojišťovnictví a zaměstnanecké penzijní pojištění), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/79/ES (Úř. věst. L 331, 15.12.2010, s. 48).

3 Nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro cenné papíry a trhy), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/77/ES (Úř. věst. L 331, 15.12.2010, s. 84).

(8) Finanční sektor Unie je upraven jednotným souborem pravidel a řídí jej Evropský systém dohledu nad finančním trhem. Nicméně ustanovení zabývající se digitální provozní odolností a bezpečností IKT nejsou dosud plně nebo konzistentně harmonizována, 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 digitální provozní odolnost, a to posílením mandátů příslušných orgánů s cílem umožnit jim vykonávat dohled nad řízením rizika v oblasti IKT ve finančním sektoru, aby byla chráněna integrita a efektivnost vnitřního trhu a bylo usnadněno jeho řádné fungování.

(9) Legislativní nesrovnalosti a nevyrovnané vnitrostátní regulatorní nebo dohledové přístupy, pokud jde o riziko v oblasti IKT, jsou příčinou překážek fungování vnitřního trhu s finančními službami a brání bezproblémovému výkonu svobody usazování a poskytování služeb finančním subjektům s přeshraniční působností. Rovněž by mohlo docházet k narušení hospodářské soutěže mezi finančními subjekty stejného typu působícími v různých členských státech. Je tomu tak zejména v oblastech, kde byla harmonizace Unie velmi omezená, jako u testování digitální provozní odolnosti, nebo v oblastech, kde chybí, například při sledování rizika v oblasti IKT spojeného s třetími stranami. Rozdíly vyplývající z předpokládaného vývoje na vnitrostátní úrovni by mohly vytvářet další překážky fungování vnitřního trhu na úkor účastníků trhu a finanční stability.

(10) V důsledku toho, že ustanovení týkající se rizika v oblasti IKT byla na unijní úrovni řešena pouze částečně, v současnosti existují mezery či přesahy ve významných oblastech, jako jsou hlášení incidentů souvisejících s IKT a testování digitální provozní odolnosti, a nesrovnalosti vyplývající z nových rozdílných vnitrostátních pravidel nebo nákladově neefektivního používání překrývajících se pravidel. Poškozuje to zejména intenzivního uživatele IKT, jakým je finanční sektor, protože technologická rizika neznají hranice a finanční sektor poskytuje své služby ve velké míře přeshraničně jak v rámci Unie, tak mimo ni. Jednotlivé finanční subjekty fungující na přeshraničním základě nebo vlastnící několik oprávnění (například jeden finanční subjekt může mít bankovní licenci a oprávnění pro investiční podnik a platební instituci, přičemž je mohly vydat různé příslušné orgány v jednom či několika členských státech) čelí provozním problémům při řešení rizika v oblasti IKT a zmírňování negativních dopadů incidentů souvisejících s IKT vlastními silami a jednotným nákladově efektivním způsobem.

(11) Protože jednotný soubor pravidel není doprovázen uceleným rámcem pro riziko v oblasti IKT nebo operační riziko, je nutná harmonizace klíčových požadavků na provozní digitální odolnost pro všechny finanční subjekty. Rozvoj schopností v oblasti IKT a celková odolnost finančních subjektů založená na těchto klíčových požadavcích by pomohly zachovat stabilitu a integritu finančních trhů Unie a tím přispět k zajištění vysoké úrovně ochrany investorů a spotřebitelů v Unii. Jelikož cílem tohoto nařízení je přispět k bezproblémovému fungování vnitřního trhu, mělo by vycházet z ustanovení článku 114 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“), jak je vykládáno v souladu s konzistentní judikaturou Soudního dvora Evropské unie (dále jen „Soudní dvůr“).

(12) Cílem tohoto nařízení je konsolidovat a aktualizovat požadavky na riziko v oblasti IKT jako součást požadavků na operační riziko, které byly až dosud řešeny v různých právních aktech Unie samostatně. Tyto akty se sice zabývají hlavními kategoriemi finančního rizika (například úvěrovým rizikem, tržním rizikem, úvěrovým rizikem protistrany a rizikem likvidity, rizikem chování trhu), ale v době svého přijetí komplexně nepostihly všechny složky provozní odolnosti. Pravidla týkající se operačního rizika, jsou-li dále rozpracována prostřednictvím těchto právních aktů Unie, často upřednostňují při řešení tohoto rizika tradiční kvantitativní přístup (konkrétně stanovení kapitálových požadavků na krytí rizika v oblasti IKT) namísto kvalitativních pravidel zaměřených na schopnosti ochrany, detekce, omezení šíření, obnovy a nápravy v souvislosti s incidenty souvisejícími s IKT nebo na schopnosti hlášení a digitálního testování. Tyto akty byly primárně určeny k pokrytí a aktualizaci základních pravidel obezřetnostního dohledu, integrity trhu nebo chování na něm.

Vzhledem ke konsolidaci a aktualizaci různých pravidel týkajících se rizika v oblasti IKT by všechna ustanovení zabývající se digitálním rizikem ve finančním sektoru měla být poprvé a konzistentně shrnuta v jediném legislativním aktu. Toto nařízení tudíž zaplňuje mezery či napravuje nesrovnalosti v některých z těchto předchozích právních aktů, včetně v nich použité terminologie, a výslovně odkazuje na riziko v oblasti IKT prostřednictvím pravidel zaměřených na schopnosti řízení rizika v oblasti IKT, hlášení incidentů, testování provozní odolnosti a sledování rizika v oblasti IKT spojeného s třetími stranami. Tímto nařízením by se tudíž rovněž mělo zvýšit povědomí o riziku v oblasti IKT a mělo by se v něm uznat, že incidenty související s IKT a nedostatečná provozní odolnost mohou ohrozit finanční stabilitu finančních subjektů.

(13) Finanční subjekty by měly při řešení rizika v oblasti IKT uplatňovat stejný přístup a stejná pravidla založená na zásadách s přihlédnutím ke své velikosti a celkovému rizikovému profilu a k povaze, rozsahu a složitosti svých služeb, činností a operací. Konzistentnost přispívá ke zvýšení důvěry ve finanční systém a zachování jeho stability, zejména v době velké závislosti na systémech, platformách a infrastrukturách IKT, které jsou spojeny se zvýšenými digitálními riziky. Dodržování základní kybernetické hygieny by rovněž mělo zabránit vysokým nákladům v ekonomice, protože minimalizuje dopad a náklady způsobené narušením v oblasti IKT.

(14) Nařízení pomáhá snižovat složitost právních předpisů, posiluje konvergenci dohledu a zvyšuje právní jistotu, přičemž 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 je proto nejvhodnější způsob, jak zaručit homogenní a jednotné využívání všech složek řízení rizika v oblasti IKT ve finančním sektoru Unie.

(15) Směrnice Evropského parlamentu a Rady (EU) 2016/1148[1] byla prvním horizontálním rámcem pro kybernetickou bezpečnost přijatým na unijní úrovni, přičemž se vztahuje rovněž na tři druhy finančních subjektů, konkrétně na úvěrové instituce, obchodní systémy a ústřední protistrany. Protože však směrnice (EU) 2016/1148 stanovila na vnitrostátní úrovni mechanismus identifikace provozovatelů základních služeb, v praxi byly do oblasti její působnosti zahrnuty pouze některé úvěrové instituce, obchodní systémy a ústřední protistrany identifikované členskými státy, které tudíž musí splňovat požadavky na bezpečnost IKT a hlášení incidentů stanovené v uvedené směrnici. Směrnice Evropského parlamentu a Rady (EU).../...[2+] stanoví jednotné kritérium pro určení subjektů, které spadají do oblasti její působnosti (pravidlo velikosti), přičemž do její oblasti působnosti patří rovněž tři druhy finančních subjektů.

---

[1] 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).

[2] Směrnice Evropského parlamentu a Rady (EU).../... ze dne... o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice o bezpečnosti sítí a informací 2) (Úř. věst. L ..., ..., s. ...).

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)) a v příslušné poznámce pod čarou číslo, datum přijetí a odkaz na zveřejnění této směrnice.

(16) Protože však toto nařízení zvyšuje zavedením požadavků na řízení rizika v oblasti IKT a hlášení incidentů souvisejících s IKT, které jsou přísnější než požadavky stanovené v současném právu Unie v oblasti finančních služeb, úroveň harmonizace různých složek digitální odolnosti, tato vyšší úroveň představuje lepší harmonizaci i ve srovnání s požadavky uvedenými ve směrnici (EU) .../...[+]. Proto toto nařízení představuje *lex specialis*, pokud jde o směrnici (EU) ../...[+]. Současně je zásadní zachovat pevný vztah mezi finančním sektorem a horizontálním rámcem Unie pro kybernetickou bezpečnost, jak je v současnosti stanoven ve směrnici (EU) .../...[+], aby byla zajištěna konzistentnost se strategiemi kybernetické bezpečnosti přijatými členskými státy a byla umožněna informovanost orgánů finančního dohledu o kybernetických incidentech dopadajících na jiná odvětví, na něž se uvedená směrnice vztahuje.

[+] Úř. věst.: vložte prosím v textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(17) V souladu s čl. 4 odst. 2 Smlouvy o Evropské unii, a aniž je dotčen soudní přezkum Soudním dvorem, by tímto nařízením neměla být dotčena odpovědnost členských států ve vztahu k základním funkcím státu, které se týkají veřejné bezpečnosti, obrany a ochrany národní bezpečnosti, například pokud jde o poskytování informací, které by byly v rozporu s ochranou národní bezpečnosti.

(18) S cílem umožnit meziodvětvové učení a účinně čerpat ze zkušeností jiných odvětví při řešení kybernetických hrozeb by finanční subjekty uvedené ve směrnici (EU).../...[+] měly zůstat součástí „ekosystému“ uvedené směrnice (například skupina pro spolupráci a týmy pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“). Evropské orgány dohledu a vnitrostátní příslušné orgány by rovněž měly být schopny účastnit se politických diskusí o strategii a technických činností skupiny pro spolupráci v rámci uvedené směrnice a vyměňovat si informace a dále spolupracovat s jednotnými kontaktními místy určenými nebo zřízenými v souladu s uvedenou směrnicí. Příslušné orgány podle tohoto nařízení by měly rovněž konzultovat týmy CSIRT a spolupracovat s nimi. Příslušné orgány by rovněž měly mít možnost požádat o technické poradenství příslušné orgány určené nebo zřízené v souladu se směrnicí (EU) .../...[+] a uzavírat ujednání o spolupráci, jejichž cílem je zabezpečit účinné a rychle reagující koordinační mechanismy.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(19) Vzhledem k silným vzájemným vazbám mezi digitální odolností a fyzickou odolností finančních subjektů je v tomto nařízení a směrnici Evropského parlamentu a Rady (EU).../...[1+] nezbytný soudržný přístup, pokud jde o odolnost kritických subjektů. Vzhledem k tomu, že fyzická odolnost finančních subjektů je uceleným způsobem řešena v rámci povinností týkajících se řízení rizika v oblasti IKT a hlášení, na něž se vztahuje toto nařízení, neměly by se povinnosti stanovené v kapitolách III a IV směrnice (EU).../...[++] vztahovat na finanční subjekty spadající do oblasti působnosti uvedené směrnice.

---

1 Směrnice Evropského parlamentu a Rady (EU) .../... ze dne ... o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (Úř. věst. L ..., ..., s. ...).

\+ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)) a v příslušné poznámce pod čarou číslo, datum přijetí a odkaz na zveřejnění uvedené směrnice.

\++ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 51/22 (2020/0365(COD)).

(20) Poskytovatelé cloudových služeb jsou jednou z kategorií digitálních infrastruktur upravených směrnicí (EU) …/…[+]. Unijní rámec dohledu vytvořený tímto nařízením (dále jen „rámec dohledu“) se vztahuje na všechny kritické poskytovatele služeb IKT z řad třetích stran, včetně poskytovatelů cloudových služeb, pokud poskytují služby IKT finančním subjektům, a měl by být považován za doplnění dohledu podle směrnice (EU) …/…[+]. Kromě toho by se měl rámec dohledu vytvořený tímto nařízením vztahovat i na poskytovatele cloudových služeb, neboť v Unii neexistuje horizontální rámec, kterým se zřizuje orgán pro digitální dohled.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(21) Aby zůstala zajištěna úplná kontrola nad rizikem v oblasti IKT, musí mít finanční subjekty k dispozici komplexní schopnosti umožňující silné a účinné řízení rizika v oblasti IKT a specifické mechanismy a politiky pro zvládnutí všech incidentů souvisejících s IKT a pro hlášení závažných incidentů souvisejících s IKT. Podobně by finanční subjekty měly mít zavedeny politiky pro testování systémů, kontrol a procesů v oblasti IKT, jakož i pro řízení rizika v oblasti IKT spojeného s třetími stranami. Je třeba zvýšit základní úroveň digitální provozní odolnosti finančních subjektů a současně umožnit proporcionální uplatňování požadavků na určité finanční subjekty, zejména mikropodniky, jakož i finanční subjekty, na něž se vztahuje zjednodušený rámec pro řízení rizika v oblasti IKT. Aby se usnadnil účinný dohled nad institucemi zaměstnaneckého penzijního pojištění, který je přiměřený a řeší potřebu snížit administrativní zátěž příslušných orgánů, měly by příslušné vnitrostátní předpisy o dohledu nad těmito finančními subjekty zohledňovat jejich velikost a celkový rizikový profil, jakož i povahu, rozsah a složitost jejich služeb, činností a operací, a to i v případě překročení příslušných prahových hodnot stanovených v článku 5 směrnice Evropského parlamentu a Rady (EU) 2016/2341[1]. Činnosti v oblasti dohledu by se měly zaměřit především na potřebu řešit vážná rizika spojená s řízením rizika v oblasti IKT konkrétního subjektu.

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/2341 ze dne 14. prosince 2016 o činnostech institucí zaměstnaneckého penzijního pojištění (IZPP) a dohledu nad nimi (Úř. věst. L 354, 23.12.2016, s. 37).

Příslušné orgány by rovněž měly zachovávat obezřetný, ale přiměřený přístup, pokud jde o dohled nad institucemi zaměstnaneckého penzijního pojištění, které v souladu s článkem 31 směrnice (EU) 2016/2341 zadávají významnou část své hlavní činnosti, jako je správa aktiv, pojistně-matematické výpočty, účetnictví a správa údajů, poskytovatelům služeb.

(22) Prahové hodnoty a taxonomie pro hlášení incidentů souvisejících s IKT se na vnitrostátní úrovni významně liší. Zatímco je možné společné pozice dosáhnout příslušnou prací Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) zřízené nařízením Evropského parlamentu a Rady (EU) 2019/881[1] a skupiny pro spolupráci podle směrnice (EU) .../...[+], mohou u ostatních finančních subjektů stále existovat či vznikat různé přístupy ke stanovení prahových hodnot a použití taxonomií. Kvůli těmto rozdílům existuje množství požadavků, které musí finanční subjekty dodržovat, zejména při fungování v několika členských státech a v rámci finanční skupiny. Takové rozdíly mohou navíc omezovat vytváření dalších jednotných nebo centralizovaných unijních mechanismů urychlujících proces hlášení a podporujících rychlou a bezproblémovou výměnu informací mezi příslušnými orgány, která je zásadní pro řešení rizika v oblasti IKT v případě rozsáhlých útoků s potenciálně systémovými dopady.

---

1 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, 15).

+ Úř. věst.: vložte prosím v textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(23) Aby se snížila administrativní zátěž a potenciálně zdvojené povinnosti hlášení pro některé finanční subjekty, měly by se požadavky na hlášení incidentů podle směrnice Evropského parlamentu a Rady (EU) 2015/2366[1] přestat vztahovat na poskytovatele platebních služeb, kteří spadají do oblasti působnosti tohoto nařízení. V důsledku toho by úvěrové instituce, instituce elektronických peněz, platební instituce a poskytovatelé služeb informování o účtu uvedení v čl. 33 odst. 1 uvedené směrnice měli ode dne použitelnosti tohoto nařízení hlásit podle tohoto nařízení všechny provozní nebo bezpečnostní incidenty související s platbami, které byly dříve oznamovány podle uvedené směrnice, bez ohledu na to, zda se tyto incidenty týkají IKT.

[1] Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35).

(24) Aby mohly příslušné orgány plnit úkoly v oblasti dohledu požadováním 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, mělo by toto nařízení stanovit spolehlivý režim hlášení incidentů souvisejících s IKT, v jehož rámci by se relevantní požadavky zaměřily na stávající mezery v právu v oblasti finančních služeb, a odstranit stávající překrytí a zdvojení s cílem snížit náklady. Je nutné harmonizovat režim hlášení incidentů souvisejících s IKT tím, že všechny finanční subjekty budou muset podávat hlášení svým příslušným orgánům na základě jednotného zjednodušeného rámce stanoveného v tomto nařízení. Kromě toho by měly evropské orgány dohledu mít pravomoc dále upřesnit relevantní prvky rámce pro hlášení incidentů souvisejících s IKT, jako jsou taxonomie, časové rámce, soubory údajů, vzory a platné prahové hodnoty. Aby byl zajištěn plný soulad se směrnicí (EU) .../...[+], mělo by být finančním subjektům umožněno dobrovolně oznamovat vážné kybernetické hrozby relevantnímu příslušnému orgánu, pokud se domnívají, že kybernetická hrozba je relevantní pro finanční systém, uživatele služeb nebo klienty.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(25) Některá finanční pododvětví vypracovala požadavky na testování digitální provozní odolnosti, jež stanoví rámce, které nejsou vždy plně sladěny. To vede k potenciálnímu zdvojení nákladů pro finanční subjekty s přeshraniční působností a činí vzájemné uznávání výsledků testování digitální provozní odolnosti složitým, což následně může vést k fragmentaci vnitřního trhu.

(26) Dále, nebude-li požadováno testování IKT, zůstanou nezjištěny zranitelnosti, jež povedou k vystavení finančního subjektu riziku v oblasti IKT, a v konečném důsledku vznikne vyšší riziko pro stabilitu a integritu finančního sektoru. Bez zásahu Unie by bylo testování digitální provozní odolnosti nadále nekonzistentní a neexistoval by systém vzájemného uznávání výsledků testování IKT v různých jurisdikcích. Protože je rovněž nepravděpodobné, že by další finanční pododvětví přijala schémata testování ve smysluplném rozsahu, promarnily by potenciální výhody rámce testování, pokud jde o odhalení zranitelností a rizik v oblasti IKT a schopnosti testování bezpečnosti a zachování provozu, které přispívají k rostoucí důvěře klientů, dodavatelů a obchodních partnerů. K odstranění uvedených přesahů, rozdílů a mezer je nutné stanovit pravidla pro režim koordinovaného testování, což usnadní vzájemné uznávání pokročilého testování u finančních subjektů splňujících kritéria stanovená tímto nařízením.

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

(28) Toto rozsáhlé využívání služeb 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 vymáhání konkrétních práv, jako jsou práva na přístup nebo práva týkající se auditů, a to i tehdy, když jsou tato práva začleněna do jejich smluvních ujednání. Kromě toho mnoho těchto smluvních ujednání 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 taková smluvní ujednání vždy přiměřeně ošetřovat individuální nebo konkrétní požadavky aktérů finančního sektoru.

(29) Přestože právo Unie v oblasti finančních služeb obsahují určitá obecná pravidla o externím zajištění služeb, není sledování smluvního rozměru v právu 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 rizika v oblasti IKT vyřešen komplexně. Je proto nezbytné stanovit určité klíčové zásady, jimiž se budou řídit finanční subjekty v případě řízení rizika v oblasti IKT spojeného s třetími stranami a které jsou obzvláště důležité, pokud finanční subjekty využívají poskytovatele služeb IKT z řad třetích stran na podporu svých zásadních nebo důležitých funkcí. Tyto zásady by měly být doplněny souborem základních smluvních práv ve vztahu k několika prvkům plnění a ukončení smluvních ujednání s cílem poskytnout určité minimální záruky na podporu schopnosti finančních subjektů účinně sledovat veškeré riziko v oblasti IKT vznikající na úrovni poskytovatelů služeb z řad třetích stran. Tyto zásady doplňují odvětvové právní předpisy použitelné na externí zajištění služeb.

(30) V současné době je patrné, že pokud jde o sledování rizika v oblasti IKT spojeného s třetími stranami a závislosti na poskytovatelích služeb IKT z řad třetích stran, chybí určitá jednotnost a sbližování. Přes úsilí o vyřešení externího zajištění služeb, jako jsou pokyny EBA pro externí služby z roku 2019 a pokyny ESMA pro spolupráci s externími poskytovateli cloudových služeb, neřeší právo Unie dostatečně širší problém potírání systémového rizika, které může vzniknout při vystavení finančního sektoru omezenému počtu kritických poskytovatelů služeb IKT z řad třetích stran. Skutečnost, že chybí pravidla na úrovni Unie, ještě zhoršuje absence vnitrostátních pravidel týkajících se oprávnění a nástrojů, které umožňují orgánům finančního dohledu správně pochopit závislosti na třetích stranách v oblasti IKT a adekvátně sledovat rizika vyplývající z koncentrace závislostí na třetích stranách v oblasti IKT.

(31) S přihlédnutím k potenciálnímu systémovému riziku souvisejícímu s rostoucí praxí externího poskytování služeb a koncentrací závislosti na třetích stranách v oblasti IKT a s ohledem na nedostatečné vnitrostátní mechanismy, pokud jde o poskytování přiměřených nástrojů orgánům finančního dohledu za účelem kvantifikace, kvalifikace a nápravy důsledků rizika v oblasti IKT, které se objevuje u kritických poskytovatelů služeb IKT z řad třetích stran, je nezbytné vytvořit vhodný rámec dohledu, který umožní nepřetržité sledování činností poskytovatelů služeb IKT z řad třetích stran, jež jsou pro finanční subjekty kritickými poskytovateli služeb IKT z řad třetích stran, a současně zabezpečí, že bude zachována důvěryhodnost a bezpečnost jiných zákazníků, než jsou finanční subjekty. Ačkoli poskytování služeb IKT v rámci skupiny s sebou nese specifická rizika a přínosy, nemělo by být automaticky považováno za méně rizikové než poskytování služeb IKT poskytovateli mimo finanční skupinu, a proto by mělo podléhat stejnému regulačnímu rámci. Pokud jsou však služby IKT poskytovány v rámci téže finanční skupiny, finanční subjekty by mohly mít vyšší úroveň kontroly nad poskytovateli v rámci skupiny, což by mělo být zohledněno v celkovém posouzení rizik.

(32) Jak se rizika v oblasti IKT stávají stále složitějšími a sofistikovanějšími, závisí správná opatření pro detekci a prevenci rizika v oblasti IKT ve značné míře na pravidelném sdílení operativních informací o hrozbách a zranitelnosti mezi finančními subjekty. Sdílení informací přispívá k vytváření zvýšeného povědomí o kybernetických hrozbách. To zase zlepšuje kapacitu finančních subjektů zabránit tomu, aby se z hrozeb staly skutečné incidenty související s IKT, a umožňuje těmto subjektům účinněji omezit dopad incidentů souvisejících s IKT a rychleji se z nich zotavit. Vzhledem k absenci pokynů na úrovni Unie se zdá, že tomuto sdílení operativních informací brání několik faktorů, zejména nejistota ohledně jejich kompatibility s předpisy pro ochranu osobních údajů, antimonopolními předpisy a předpisy upravujícími odpovědnost.

(33) 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 vymáhání práva), navíc vedou k neposkytování užitečných informací. Rozsah a kvalita sdílení informací zůstávají tudíž v současné době omezené a roztříštěné a příslušné výměny informací probíhají většinou na místní úrovni (prostřednictvím vnitrostátních iniciativ) a bez konzistentních celounijních dohod o sdílení informací přizpůsobených požadavkům integrovaného finančního systému. Je proto důležité tyto komunikační kanály posílit.

(34) Finanční subjekty by měly být vybízeny, aby si vzájemně vyměňovaly operativní informace o kybernetických hrozbách a 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, a to zapojením do ujednání o sdílení informací. Je proto nezbytné umožnit, aby na úrovni Unie vznikly mechanismy ujednání o dobrovolném sdílení informací, které při zavedení v důvěryhodných prostředích pomohou komunitě finančního sektoru bránit se a společně reagovat na kybernetické hrozby rychlým omezením šíření rizika v oblasti IKT a zabráněním potenciálnímu šíření nákazy finančními kanály. Tyto mechanismy by měly být v souladu s platnými pravidly práva Unie v oblasti hospodářské soutěže, jak jsou vymezena ve sdělení Komise ze dne 14. ledna 2011 nazvaném „Pokyny k použitelnosti článku 101 Smlouvy o fungování Evropské unie na dohody o horizontální spolupráci“, jakož i s pravidly Unie pro ochranu údajů, zejména s nařízením Evropského parlamentu a Rady (EU) 2016/679[1]. Měly by fungovat na základě použití jednoho nebo více právních základů stanovených v článku 6 uvedeného nařízení, například v souvislosti se zpracováním osobních údajů, které je nezbytné pro účely oprávněného zájmu správce nebo třetí strany, jak je uvedeno v čl. 6 odst. 1 písm. f) uvedeného nařízení, jakož i v souvislosti se zpracováním osobních údajů nezbytných pro splnění právní povinnosti správce, které je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, jak je uvedeno v čl. 6 odst. 1 písm. c) a e) uvedeného nařízení.

[1] 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).

(35) Aby se zachovala vysoká úroveň digitální provozní odolnosti celého finančního sektoru a zároveň držel krok s technologickým vývojem, mělo by se toto nařízení zabývat rizikem vyplývajícím ze všech druhů služeb IKT. Za tímto účelem by definice služeb IKT v kontextu tohoto nařízení měla být chápána široce a měla by zahrnovat digitální a datové služby průběžně poskytované prostřednictvím systémů IKT jednomu nebo více interním nebo externím uživatelům. Tato definice by měla například zahrnovat tzv. služby „over the top“, které spadají do kategorie služeb elektronických komunikací. Měla by vyloučit pouze omezenou kategorii tradičních analogových telefonních služeb, které jsou kvalifikovány jako služby veřejné komutované telefonní sítě (PSTN), služby pevné sítě, služby tradičního analogového telefonního systému (POTS) nebo telefonní služby pevné linky.

(36) Bez ohledu na širokou platnost uvedenou v tomto nařízení by mělo používání pravidel pro digitální provozní odolnost zohledňovat výrazné rozdíly ve velikosti a celkovém rizikovém profilu jednotlivých finančních subjektů. Obecným principem při rozdělování zdrojů a schopností na realizaci rámce pro řízení rizika v oblasti IKT by mělo být, že finanční subjekty správně vyváží své požadavky na IKT podle své velikosti a celkového rizikového profilu a povahy, rozsahu a složitosti svých služeb, činnosti a provozu, zatímco příslušné orgány budou nadále hodnotit a revidovat způsob tohoto rozdělení.

(37) Poskytovatelé služeb informování o účtu uvedení v čl. 33 odst. 1 směrnice (EU) 2015/2366 jsou výslovně zahrnuti do oblasti působnosti tohoto nařízení s přihlédnutím ke zvláštní povaze jejich činností a rizikům, která z nich vyplývají. Kromě toho do oblasti působnosti tohoto nařízení spadají instituce elektronických peněz a platební instituce vyňaté podle čl. 9 odst. 1 směrnice Evropského parlamentu a Rady 2009/110/ES[1] a čl. 32 odst. 1 směrnice (EU) 2015/2366, i v případě, že jim nebylo v souladu se směrnicí 2009/110/ES uděleno povolení k vydávání elektronických peněz nebo pokud jim nebylo v souladu se směrnicí (EU) 2015/2366 uděleno povolení k poskytování a provádění platebních služeb. Z oblasti působnosti tohoto nařízení jsou však vyňaty poštovní žirové instituce uvedené v čl. 2 odst. 5 bodu 3 směrnice Evropského parlamentu a Rady 2013/36/EU[2]. Příslušným orgánem v případě platebních institucí vyňatých podle směrnice (EU) 2015/2366, institucí elektronických peněz vyňatých podle směrnice 2009/110/ES a poskytovatelů služeb informování o účtu uvedených v čl. 33 odst. 1 směrnice (EU) 2015/2366 by měl být příslušný orgán určený v souladu s článkem 22 směrnice (EU) 2015/2366.

---

[1] 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).

[2] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

(38) Protože větší finanční subjekty by mohly využívat více prostředků a mohou 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 ujednáními s poskytovateli služeb IKT z řad třetích stran nebo pro zvládání krizového řízení, k organizaci svého řízení rizika souvisejícího s IKT podle tří linií modelu obrany nebo k zavedení modelu interního řízení rizika a kontroly a předložení svých rámců pro řízení rizika v oblasti IKT vnitřnímu auditu.

(39) Některé finanční subjekty využívají výjimky nebo se na ně podle příslušných odvětvových právních předpisů Unie vztahuje velmi zjednodušený regulační rámec. Tyto finanční subjekty zahrnují správce alternativních investičních fondů uvedené v čl. 3 odst. 2 směrnice Evropského parlamentu a Rady 2011/61/EU[1], pojišťovny a zajišťovny uvedené v článku 4 směrnice Evropského parlamentu a Rady 2009/138/ES[2] a instituce zaměstnaneckého penzijního pojištění, které provozují penzijní plány, které dohromady nemají více než 15 účastníků. S ohledem na tyto výjimky by nebylo přiměřené zahrnout tyto finanční subjekty do oblasti působnosti tohoto nařízení. Kromě toho toto nařízení uznává specifika struktury trhu zprostředkování pojištění, v důsledku čehož by se toto nařízení nemělo vztahovat na zprostředkovatele pojištění, zprostředkovatele zajištění a zprostředkovatele doplňkového pojištění kvalifikované jako mikropodniky nebo malé nebo střední podniky.

(40) Vzhledem k tomu, že subjekty uvedené v čl. 2 odst. 5 bodech 4 až 23 směrnice 2013/36/EU jsou vyňaty z oblasti působnosti uvedené směrnice, měly by mít členské státy možnost vyloučit z oblasti působnosti tohoto nařízení subjekty usazené na jejich území.

---

1 Směrnice Evropského parlamentu a Rady 2011/61/EU ze dne 8. června 2011 o správcích alternativních investičních fondů a o změně směrnic 2003/41/ES a 2009/65/ES a nařízení (ES) č. 1060/2009 a (EU) č. 1095/2010 (Úř. věst. L 174, 1.7.2011, s. 1).

2 Směrnice Evropského parlamentu a Rady 2009/138/ES ze dne 25. listopadu 2009 o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II) (Úř. věst. L 335, 17.12.2009, s. 1).

(41) Obdobně v zájmu sladění tohoto nařízení s oblastí působnosti směrnice Evropského parlamentu a Rady 2014/65/EU[1] je rovněž vhodné vyloučit z oblasti působnosti tohoto nařízení fyzické a právnické osoby uvedené v článcích 2 a 3 uvedené směrnice, které mohou poskytovat investiční služby, aniž by musely získat povolení podle směrnice 2014/65/EU. Článek 2 směrnice 2014/65/EU však z oblasti působnosti uvedené směrnice rovněž vylučuje subjekty, které jsou pro účely tohoto nařízení považovány za finanční subjekty, jako jsou centrální depozitáře cenných papírů, subjekty kolektivního investování nebo pojišťovny a zajišťovny. Vyloučení osob a subjektů podle článků 2 a 3 uvedené směrnice z oblasti působnosti tohoto nařízení by nemělo tyto centrální depozitáře cenných papírů, subjekty kolektivního investování nebo pojišťovny a zajišťovny zahrnovat.

[1] Směrnice Evropského parlamentu a Rady 2014/65/EU ze dne 15. května 2014 o trzích finančních nástrojů a o změně směrnic 2002/92/ES a 2011/61/EU (Úř. věst. L 173, 12.6.2014, s. 349).

(42) Některé finanční subjekty podléhají podle odvětvových právních předpisů Unie mírnějším požadavkům nebo výjimkám z důvodů spojených s jejich velikostí nebo službami, které poskytují. Tato kategorie finančních subjektů zahrnuje malé a nepropojené investiční podniky, malé instituce zaměstnaneckého penzijního pojištění, které mohou být dotčeným členským státem vyloučeny z oblasti působnosti směrnice (EU) 2016/2341 za podmínek stanovených v článku 5 uvedené směrnice a provozují penzijní plány, které dohromady nemají více než 100 účastníků, jakož i instituce vyňaté podle směrnice 2013/36/EU. Proto je v souladu se zásadou proporcionality a v zájmu zachování smyslu odvětvových právních předpisů Unie rovněž vhodné podrobit tyto finanční subjekty zjednodušenému rámci pro řízení rizika v oblasti IKT podle tohoto nařízení. Přiměřenost rámce pro řízení rizika v oblasti IKT, který se vztahuje na tyto finanční subjekty, by neměla být měněna regulačními technickými normami, které mají být vypracovány evropskými orgány dohledu. Kromě toho je v souladu se zásadou proporcionality vhodné, aby se na platební instituce uvedené v čl. 32 odst. 1 směrnice (EU) 2015/2366 a na instituce elektronických peněz uvedené v článku 9 směrnice 2009/110/ES vyňaté v souladu s vnitrostátním právem provádějícím tyto právní akty Unie vztahoval zjednodušený rámec pro řízení rizika v oblasti IKT podle tohoto nařízení, zatímco platební instituce a instituce elektronických peněz, které nebyly vyňaty v souladu s vnitrostátním právem provádějícím odvětvové právní předpisy Unie, by měly dodržovat obecný rámec stanovený tímto nařízením.

(43) Obdobně by se po finančních subjektech, které jsou považovány za mikropodniky nebo se na ně vztahuje zjednodušený rámec pro řízení rizika v oblasti IKT podle tohoto nařízení, nemělo požadovat, aby vytvořily funkci sledování ujednání o využívání služeb IKT uzavřených s poskytovateli z řad třetích stran nebo pověřily jednoho vedoucího pracovníka jako osobu odpovědnou za dohled nad expozicí souvisejícím rizikům a příslušnou dokumentací; pověřily odpovědností za řízení a kontrolu rizika v oblasti IKT kontrolní funkci a zajistily odpovídající nezávislost této kontrolní funkce, aby nedocházelo ke střetům zájmů; zdokumentovaly a přezkoumaly rámec pro řízení rizika v oblasti IKT alespoň jednou ročně; pravidelně prováděly interní audit rámce pro řízení rizika v oblasti IKT; prováděly hloubková posouzení po velkých změnách svých infrastruktur sítí a informačních systémů a procesů, pravidelně analyzovaly rizika původních systémů IKT; prováděly nezávislý interní audit provádění plánů reakce a obnovy v oblasti IKT; zavedly funkci řízení krizí, rozšířily testování zachování provozu a plány reakce a obnovy tak, aby zahrnovaly i scénáře přepnutí mezi primární infrastrukturou IKT a redundantními zařízeními; na žádost oznamovaly příslušným orgánům odhad souhrnných ročních nákladů a ztrát způsobených závažnými incidenty souvisejícími s IKT, udržovaly rezervní kapacity IKT; informovaly příslušné vnitrostátní orgány o změnách v návaznosti na přezkumy realizované po incidentech souvisejících s IKT; nepřetržitě sledovaly relevantní technologický vývoj, zavedly ucelený program testování digitální provozní odolnosti jako nedílnou součást rámce pro řízení rizika v oblasti IKT stanoveného v tomto nařízení nebo přijaly a pravidelně revidovaly strategii týkající se rizika v oblasti IKT spojeného s třetími stranami.

Kromě toho by se od mikropodniků mělo pouze vyžadovat, aby posoudily potřebu zachovat tyto nadbytečné kapacity IKT na základě svého rizikového profilu. Mikropodniky by měly mít prospěch z flexibilnějšího režimu, pokud jde o programy testování digitální provozní odolnosti. Při zvažování druhu a četnosti testů, které mají být prováděny, by měly náležitě vyvážit cíl zachování vysoké digitální provozní odolnosti, dostupné zdroje a svůj celkový rizikový profil. Mikropodniky a finanční subjekty, na něž se vztahuje zjednodušený rámec pro řízení rizika v oblasti IKT podle tohoto nařízení, by měly být osvobozeny od požadavku provádět pokročilé testování nástrojů, systémů a procesů IKT na základě penetračního testování na základě hrozeb, neboť by se mělo požadovat, aby takové testování prováděly pouze finanční subjekty splňující kritéria stanovená tímto nařízením. Vzhledem ke svým omezeným možnostem by měly mít mikropodniky možnost dohodnout se s poskytovatelem služeb IKT z řad třetích stran na přenesení práv finančního subjektu na přístup, kontrolu a audit na nezávislou třetí stranu, kterou určí poskytovatel služeb IKT z řad třetích stran, za předpokladu, že finanční subjekt může kdykoli požádat příslušnou nezávislou třetí stranu o veškeré relevantní informace a ujištění o výkonnosti poskytovatele služeb IKT z řad třetích stran.

(44) Protože provádění penetračních testů na základě hrozeb bude požadováno pouze u finančních subjektů označených pro účely pokročilého testování digitální odolnosti, měly by se administrativní postupy a finanční náklady související s těmito testy týkat malého procenta finančních subjektů.

(45) Aby byla zajištěna úplná harmonizace a celková konzistentnost obchodních strategií finančních subjektů na jedné straně a provádění řízení rizika v oblasti IKT na straně druhé, je třeba po vedoucích orgánech finančních subjektů požadovat, aby si zachovávaly klíčovou a aktivní úlohu při řízení a přizpůsobování rámce pro řízení rizika v oblasti IKT a celkové strategie digitální provozní odolnosti. Přístup vedoucích orgánů by se neměl zaměřovat pouze na prostředky k zajištění odolnosti systémů IKT, ale měl by prostřednictvím souboru politik zahrnovat rovněž osoby a procesy, které na každé úrovni podniku a pro všechny zaměstnance utvářejí silné povědomí o kybernetických rizicích a závazek k dodržování striktní kybernetické hygieny na všech úrovních. Nejvýznamnějším úkolem vedoucího orgánu při řízení rizika finančního subjektu v oblasti IKT by měl být zastřešující princip tohoto uceleného přístupu dále vyjádřeného prostřednictvím nepřetržitého angažování vedoucího orgánu při kontrole sledování řízení rizika v oblasti IKT.

(46) Kromě toho zásada plné a konečné odpovědnosti vedoucího orgánu za řízení rizika finančního subjektu v oblasti IKT jde ruku v ruce s potřebou zabezpečit míru investic souvisejících s IKT a celkový rozpočet finančního subjektu, který by mu umožnil dosáhnout vysoké úrovně digitální provozní odolnosti.

(47) Toto nařízení, které je inspirováno příslušnými mezinárodními, vnitrostátními a odvětvovými osvědčenými postupy, pokyny, doporučeními a přístupy k řízení kybernetického rizika, podporuje soubor zásad usnadňujících celkovou strukturalizaci řízení rizika v oblasti IKT. V důsledku toho, pokud existují hlavní schopnosti, které finanční subjekty zavedly s cílem řešit různé funkce řízení rizika v oblasti IKT (identifikace, ochrana a prevence, detekce, reakce a obnova, poučení a vývoj a komunikace), uvedené v tomto nařízení, měly by finanční subjekty nadále volně používat modely řízení rizika v oblasti IKT s různými rámci nebo kategoriemi.

(48) Aby finanční subjekty udržely krok s vývojem v oblasti kybernetických hrozeb, měly by udržovat aktualizované systémy IKT, které budou spolehlivé a schopné zaručit nejen zpracování údajů požadovaných k realizaci jejich služeb, ale které budou mít rovněž dostatečnou technologickou odolnost umožňující finančním subjektům adekvátně se vypořádat s dalšími požadavky na zpracování, které se mohou objevit v důsledku napjatých podmínek na trhu nebo jiných nepříznivých situací.

(49) 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 opatření k obnově činností, a to v souladu se svými záložními postupy. Toto obnovení by však v žádném případě nemělo ohrozit integritu a bezpečnost sítí a informačních systémů ani dostupnost, hodnověrnost, integritu nebo důvěrnost údajů.

(50) I když toto nařízení umožňuje, aby finanční subjekty flexibilně stanovily své cíle, pokud jde o dobu obnovy a bod dosažení obnovy, tedy aby stanovily tyto cíle s úplným zohledněním povahy a významu relevantních funkcí a všech konkrétních provozních potřeb, mělo by po nich nicméně vyžadovat, aby při stanovování těchto cílů provedly posouzení potenciálního celkového dopadu na tržní efektivitu.

(51) Šiřitelé kybernetických útoků mají tendenci usilovat o finanční zisky přímo u zdroje, čímž vystavují finanční subjekty závažným důsledkům. Aby se předešlo ztrátě integrity systémů IKT či jejich nedostupnosti, a tudíž se zabránilo prolomení důvěrných údajů nebo poškození fyzické infrastruktury IKT, je třeba výrazně zlepšit a zjednodušit hlášení závažných incidentů souvisejících s IKT finančními subjekty. Hlášení incidentů souvisejících s IKT by mělo být pro všechny finanční subjekty harmonizováno prostřednictvím zavedení požadavku, aby podávaly hlášení přímo svým relevantním příslušným orgánům. Pokud finanční subjekt podléhá dohledu více než jednoho příslušného vnitrostátního orgánu, měly by členské státy určit jediný příslušný orgán, jemuž bude takové hlášení určeno. Úvěrové instituce klasifikované jako významné v souladu s čl. 6 odst. 4 nařízení Rady (EU) č. 1024/2013[1] by měly tato hlášení předkládat vnitrostátním příslušným orgánům, které by měly zprávu následně předat Evropské centrální bance (ECB).

[1] 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).

(52) Přímé hlášení by mělo orgánům finančního dohledu umožnit získat okamžitý přístup k informacím o závažných incidentech souvisejících s IKT. Orgány finančního dohledu by však na oplátku měly podrobné informace o závažných incidentech souvisejících s IKT poskytnout veřejným nefinančním orgánům (jako jsou příslušné orgány a jednotná kontaktní místa podle směrnice (EU) .../...[+], vnitrostátní úřady pro ochranu osobních údajů a v případě závažných incidentů souvisejících s IKT trestní povahy donucovací orgány), aby se posílilo povědomí těchto orgánů o takových incidentech a aby se v případě týmů CSIRT usnadnila rychlá pomoc, kterou je možné finančním subjektům případně poskytnout. Členské státy by navíc měly mít možnost stanovit, že finanční subjekty by měly tyto informace poskytovat veřejným orgánům mimo oblast finančních služeb samy. Tyto informační toky by měly finančním subjektům umožnit rychle využít veškerých relevantních technických vstupů, poradenství ohledně nápravy a následných opatření ze strany těchto orgánů. Informace o závažných incidentech souvisejících s IKT by měly být poskytovány vzájemně: orgány finančního dohledu by měly finančnímu subjektu poskytovat veškerou nezbytnou zpětnou vazbu nebo pokyny a evropské orgány dohledu by měly sdílet anonymizované údaje o kybernetických hrozbách a zranitelnostech týkající se daného incidentu, aby pomohly širší společné obraně.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(53) Přestože by se hlášení incidentů mělo vyžadovat po všech finančních subjektech, neočekává se, že tento požadavek ovlivní všechny subjekty stejným způsobem. Příslušné prahové hodnoty významnosti, jakož i lhůty pro hlášení by měly být řádně upraveny v kontextu aktů v přenesené pravomoci založených na regulačních technických normách, které vypracují evropské orgány dohledu, a to tak, aby se vztahovaly pouze na závažné incidenty související s IKT. Při stanovování lhůt pro povinnost hlášení by navíc měla být zohledněna specifika finančních subjektů.

(54) Toto nařízení by mělo vyžadovat, aby úvěrové instituce, platební instituce, poskytovatelé služeb informování o účtu a instituce elektronických peněz hlásili všechny provozní nebo bezpečnostní incidenty související s platbami – dříve hlášené podle směrnice (EU) 2015/2366 – bez ohledu na povahu incidentu z hlediska IKT.

(55) Evropské orgány dohledu by měly být pověřeny posouzením proveditelnosti a podmínek možné centralizace hlášení incidentů souvisejících s IKT na úrovni Unie. Tato centralizace by mohla sestávat z jednotného centra EU pro hlášení závažných incidentů souvisejících s IKT, které bude buď přímo přijímat příslušná hlášení a automaticky informovat příslušné vnitrostátní orgány, nebo bude soustřeďovat příslušná hlášení zasílaná příslušnými vnitrostátními orgány, a plnit tak úlohu koordinátora. Evropské orgány dohledu by měly být pověřeny, aby společně s ECB a ENISA vypracovaly společnou zprávu zabývající se proveditelností vytvoření jednotného centra EU.

(56) Aby finanční subjekty dosáhly vysoké úrovně digitální provozní odolnosti a fungovaly v souladu s příslušnými mezinárodními normami (například základními prvky skupiny G7 pro penetrační testování na základě hrozeb) i s rámci uplatňovanými v Unii, jako je například TIBER–EU, měly by pravidelně testovat své systémy IKT a personál zodpovědný za IKT na efektivitu jejich prostředků prevence, detekce, reakce a obnovy, aby byly zjištěny a odstraněny potenciální zranitelnosti IKT. Aby se zohlednily rozdíly vyskytující se napříč různými finančními pododvětvími a v jejich rámci, pokud jde o úroveň připravenosti finančních subjektů v oblasti kybernetické bezpečnosti, mělo by testování zahrnovat širokou škálu nástrojů a opatření od posouzení základních požadavků (například posouzení a zjišťování zranitelnosti, analýzy otevřených zdrojů, posouzení bezpečnosti sítí, analýzy nedostatků, přezkumy fyzické bezpečnosti, dotazníky a antivirová softwarová řešení, přezkumy zdrojových kódů, pokud jsou proveditelné, testy založené na scénářích, testování kompatibility, testování výkonu nebo testování mezi koncovými body) až po pokročilejší testování prostřednictvím penetračního testování na základě hrozeb. Taková pokročilá testování by měla být vyžadována pouze u finančních subjektů dostatečně vyspělých z hlediska IKT, aby je mohly přiměřeně provést. Testování digitální provozní odolnosti vyžadované tímto nařízením by tedy mělo být pro některé finanční subjekty splňující kritéria stanovená v tomto nařízení (například pro systémové a v oblasti IKT vyspělé úvěrové instituce, burzy, centrální depozitáře cenných papírů a ústřední protistrany) náročnější než pro jiné finanční subjekty. Současně by testování digitální provozní odolnosti prostřednictvím penetračního testování na základě hrozeb mělo být vhodnější pro finanční subjekty, které vykonávají činnost v pododvětvích hlavních finančních služeb a hrají systémovou roli (například platby, bankovnictví a clearing a vypořádání), a méně vhodné pro jiná pododvětví (například správci aktiv a ratingové agentury).

(57) Finanční subjekty, které působí přeshraničně a vykonávají své právo usadit se nebo právo poskytovat služby v rámci Unie, by měly ve svém domovském členském státě splňovat jednotný soubor požadavků na pokročilé testování (například penetrační testování na základě hrozeb), které by mělo zahrnovat infrastruktury IKT ve všech jurisdikcích, kde přeshraniční finanční skupina v rámci Unie působí, což takovým přeshraničním finančním skupinám umožní mít náklady na testování související s IKT pouze v jedné jurisdikci.

(58) S cílem využít odborných znalostí, které již některé příslušné orgány získaly, zejména pokud jde o provádění rámce TIBER–EU, by toto nařízení mělo členským státům umožnit, aby na vnitrostátní úrovni určily jediný veřejný orgán jako odpovědný za všechny záležitosti penetračního testování na základě hrozeb ve finančním sektoru nebo aby v případě, že k takovému určení nedojde, pověřily prováděním úkolů souvisejících s penetračním testováním na základě hrozeb jiný vnitrostátní příslušný finanční orgán.

(59) Vzhledem k tomu, že toto nařízení nevyžaduje, aby finanční subjekty pokrývaly všechny zásadní nebo důležité funkce v rámci jediného penetračního testu na základě hrozeb, měly by mít finanční subjekty možnost určit, které zásadní nebo důležité funkce by do rozsahu tohoto testování měly být zahrnuty a kolik by jich mělo být.

(60) Společné testování ve smyslu tohoto nařízení – zahrnující zapojení několika finančních subjektů do penetračního testování na základě hrozeb, kdy poskytovatel služeb IKT z řad třetích stran může přímo uzavřít smluvní ujednání s externím subjektem provádějícím testování – by se mělo umožnit pouze tehdy, pokud se odůvodněně předpokládá, že by to nemělo nepříznivý dopad na kvalitu nebo bezpečnost služeb IKT poskytovaných poskytovatelem z řad třetích stran zákazníkům, kteří nejsou subjekty spadajícími do oblasti působnosti tohoto nařízení, nebo na důvěrnost údajů souvisejících s těmito službami. Společné testování by mělo podléhat zárukám (řízení jedním určeným finančním subjektem, kalibrace zapojených finančních subjektů) s cílem zajistit důkladné testování zapojených finančních subjektů, které splňuje cíle penetračního testování na základě hrozeb podle tohoto nařízení.

(61) Aby bylo možné využít interních zdrojů dostupných na úrovni podniku, mělo by toto nařízení pro účely provádění penetračního testování na základě hrozeb umožnit používání interních subjektů za předpokladu, že orgán dohledu souhlasí, že nedochází ke střetům zájmů a že se pravidelně mění používání interních a externích subjektů provádějících testování (jeden ze tří testů), a zároveň by se mělo vyžadovat, aby poskytovatel operativních informací o hrozbách byl v rámci penetračního testování vždy externí subjekt, který není součástí daného finančního subjektu. Odpovědnost za provádění penetračního testování na základě hrozeb by měl plně nést finanční subjekt. Osvědčení vydávaná orgány by měla být výhradně pro účely vzájemného uznávání a neměla by vylučovat jakákoli následná opatření potřebná k řešení rizika v oblasti IKT, jemuž je finanční subjekt vystaven, ani by neměla být chápána jako potvrzení ze strany orgánů dohledu o schopnostech finančního subjektu řídit a snižovat rizika v oblasti IKT.

(62) Za účelem zajištění řádného sledování rizika v oblasti IKT spojeného s třetími stranami ve finančním sektoru je nutné stanovit soubor pravidel založených na zásadách jako vodítko pro finanční subjekty, pokud sledují riziko, které vzniká v souvislosti s funkcemi externě zajišťovanými poskytovateli služeb IKT z řad třetích stran, a to zejména v případě služeb IKT podporujících zásadní nebo důležité funkce, jakož i obecněji v kontextu závislostí na všech třetích stranách v oblasti IKT.

(63) Aby bylo možné řešit složitost různých zdrojů rizika v oblasti IKT a zároveň zohlednit množství a rozmanitost poskytovatelů technologických řešení, která umožňují bezproblémové poskytování finančních služeb, mělo by se toto nařízení vztahovat na širokou škálu poskytovatelů služeb IKT z řad třetích stran, včetně poskytovatelů cloudových služeb, softwaru, služeb analýzy dat a poskytovatelů služeb datových center. Podobně vzhledem k tomu, že by finanční subjekty měly účinně a jednotně identifikovat a řídit všechny druhy rizika, a to i v souvislosti se službami IKT pořízenými v rámci finanční skupiny, mělo by být vyjasněno, že podniky, které jsou součástí finanční skupiny a poskytují služby IKT převážně svému mateřskému podniku nebo dceřiným podnikům či pobočkám svého mateřského podniku, jakož i finanční subjekty poskytující služby IKT jiným finančním subjektům, by měly být rovněž považovány za poskytovatele služeb IKT z řad třetích stran podle tohoto nařízení. A konečně s ohledem na vyvíjející se trh platebních služeb, který je stále závislejší na složitých technických řešeních, a s ohledem na nově se objevující druhy platebních služeb a řešení související s platbami by účastníci ekosystému platebních služeb, kteří poskytují činnosti zpracování plateb nebo provozují platební infrastruktury, měli být rovněž považováni za poskytovatele služeb IKT z řad třetích stran podle tohoto nařízení, s výjimkou centrálních bank při provozování platebních systémů nebo systémů vypořádání obchodů s cennými papíry a veřejných orgánů při poskytování služeb souvisejících s IKT v kontextu státní správy.

(64) Za dodržování svých povinností podle tohoto nařízení by měl vždy zůstat plně odpovědný finanční subjekt. Finanční subjekty by měly uplatňovat proporcionální přístup ke sledování rizik vznikajících na úrovni poskytovatelů služeb IKT z řad třetích stran, a to řádným přihlédnutím k povaze, rozsahu, složitosti a významu své 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.

(65) Toto sledování by se mělo řídit strategickým přístupem k riziku v oblasti IKT spojeným s třetími stranami formalizovaným prostřednictvím specializované strategie pro riziko v oblasti IKT spojené s třetími stranami přijaté vedoucím orgánem finančního subjektu, která bude založena na nepřetržité kontrole všech takových závislostí na třetích stranách v oblasti IKT. V zájmu zvýšení povědomí orgánů dohledu o závislosti na třetích stranách v oblasti IKT a s cílem dále podpořit práci v souvislosti s rámcem dohledu zřízeným tímto nařízením by všechny finanční subjekty měly mít povinnost vést registr informací se všemi smluvními ujednáními o využívání služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran. Orgány finančního dohledu by měly mít možnost požádat o registr v plném rozsahu nebo požádat o jeho konkrétní části, a získat tak nezbytné informace pro širší pochopení závislostí finančních subjektů na IKT.

(66) Základem formálního uzavření smluvních ujednání by měla být důkladná analýza před uzavřením smlouvy, přičemž by se měla zaměřit zejména na prvky, jak jsou služby podporované zamýšlenou smlouvou o IKT zásadní nebo důležité, nezbytná schválení orgánů dohledu nebo jiné podmínky, možné riziko koncentrace, které s sebou nese, jakož i uplatňování náležité péče v procesu výběru a posuzování poskytovatelů služeb IKT z řad třetích stran a posuzování potenciálních střetů zájmů. U smluvních ujednání týkajících se zásadních nebo důležitých funkcí by finanční subjekty měly zvážit, zda poskytovatelé služeb IKT z řad třetích stran uplatňují aktuální a nejvyšší normy bezpečnosti informací. K ukončení smluvních ujednání by mohlo docházet na základě alespoň série okolností ukazujících na nedostatky vzniklé na úrovni poskytovatele služeb IKT z řad třetích stran, zejména na významné porušení právních předpisů nebo smluvních podmínek, okolnosti odhalující potenciální změnu v plnění funkcí poskytovaných na základě smluvních ujednání, důkazy o slabých stránkách poskytovatele služeb IKT z řad třetích stran v jeho celkovém řízení rizika v oblasti IKT nebo okolnosti naznačující, že relevantní příslušný orgán není schopen vykonávat účinný dohled nad finančním subjektem.

(67) Za účelem řešení systémového dopadu rizika koncentrace třetích stran v oblasti IKT podporuje toto nařízení vyvážené řešení prostřednictvím flexibilního a postupného přístupu k tomuto riziku koncentrace, neboť stanovení jakýchkoli pevných mezních hodnot nebo přísných omezení by mohlo bránit podnikání a omezovat smluvní svobodu. Finanční subjekty by měly důkladně vyhodnocovat svá plánovaná smluvní ujednání, aby identifikovaly pravděpodobnost vzniku takového rizika, včetně využití hloubkových analýz subdodavatelských ujednání, zejména budou-li uzavírány s poskytovateli služeb IKT z řad třetích stran usazenými ve třetí zemi. V této fázi a s ohledem na dosažení spravedlivé rovnováhy mezi nutným zachováním smluvní svobody a nutným zajištěním finanční stability není považováno za vhodné stanovit pro expozici třetím stranám v oblasti IKT pravidla v podobě striktních mezních hodnot a omezení. V kontextu rámce dohledu by hlavní orgán dohledu jmenovaný podle tohoto nařízení měl s ohledem na kritické poskytovatele služeb IKT z řad třetích stran věnovat zvláštní pozornost úplnému pochopení rozsahu vzájemných závislostí, 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 udržovat dialog s kritickými poskytovateli služeb IKT z řad třetích stran, u nichž je toto konkrétní riziko identifikováno.

(68) Za účelem pravidelného hodnocení a sledování schopnosti poskytovatele služeb IKT z řad třetích stran bezpečně poskytovat služby finančnímu subjektu bez nepříznivých dopadů na digitální provozní odolnost finančního subjektu by mělo být několik klíčových smluvních prvků s poskytovateli služeb IKT z řad třetích stran harmonizováno. Taková harmonizace by se měla týkat alespoň oblastí, které jsou klíčové pro to, aby finanční subjekt mohl plně sledovat rizika, která by mohl způsobit poskytovatel služeb IKT z řad třetích stran, a to z hlediska potřeby finančního subjektu zabezpečit svoji digitální odolnost, protože ta velmi závisí na stabilitě, funkčnosti, dostupnosti a bezpečnosti služeb IKT, které mu jsou poskytovány.

(69) V rámci nového sjednávání smluvních ujednání s cílem dosáhnout souladu s požadavky tohoto nařízení by finanční subjekty a poskytovatelé služeb IKT z řad třetích stran měli zajistit pokrytí klíčových smluvních ustanovení, jak je stanoveno v tomto nařízení.

(70) Definice „zásadní nebo důležitá funkce“ stanovená v tomto nařízení by měla zahrnovat „zásadní funkce“ uvedené v čl. 2 odst. 1 bodě 35 směrnice Evropského parlamentu a Rady 2014/59/EU[1]. Obdobně jsou funkce považované za zásadní podle směrnice 2014/59/EU zahrnuty do definice zásadních funkcí ve smyslu tohoto nařízení.

---

[1] 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).

(71) Bez ohledu na to, jak jsou funkce podporované službami IKT zásadní nebo důležité, měla by smluvní ujednání zejména obsahovat specifikace úplných popisů funkcí a služeb, míst, kde jsou dotčené funkce poskytovány a kde budou zpracovávána data, a rovněž popisy úrovní služeb. Mezi další zásadní prvky umožňující finančnímu subjektu sledovat riziko v oblasti IKT spojené s třetími stranami patří: smluvní ustanovení, která upřesňují, jak poskytovatel služeb IKT z řad třetích stran zajišťuje přístupnost, dostupnost, integritu, bezpečnost a ochranu osobních údajů, ustanovení obsahující relevantní záruky umožňující přístup k údajům, obnovu a navrácení údajů v případě platební neschopnosti, řešení krize nebo ukončení obchodní činnosti poskytovatele služeb IKT z řad třetích stran, jakož i ustanovení požadující, aby poskytovatel služeb IKT z řad třetích stran poskytl pomoc v případě incidentů v oblasti IKT v souvislosti s poskytovanými službami, a to bez dodatečných nákladů nebo za cenu určenou následně; ustanovení o povinnosti poskytovatele služeb IKT z řad třetích stran plně spolupracovat s příslušnými orgány a orgány příslušnými k řešení krize finančního subjektu; a ustanovení o právech na ukončení smlouvy a související minimální výpovědní lhůtě pro ukončení smluvních ujednání v souladu s očekáváními příslušných orgánů a orgánů příslušných k řešení krize.

(72) Kromě těchto smluvních ustanovení a s cílem zajistit, aby finanční subjekty měly i nadále plnou kontrolu nad veškerým vývojem na úrovni třetích stran, který by mohl ohrozit jejich bezpečnost IKT, by smlouvy o poskytování služeb IKT podporujících zásadní nebo důležité funkce měly rovněž obsahovat: upřesnění popisů úrovní úplné služby doplněné o přesné kvantitativní i kvalitativní výkonnostní cíle, aby bylo možné neprodleně přijmout vhodné kroky k nápravě, nejsou-li sjednané úrovně služeb splněny; příslušné 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 příslušné služby IKT; požadavek, aby poskytovatel služeb IKT z řad třetích stran zavedl a otestoval plány zachování provozu a měl bezpečnostní opatření, nástroje a politiky v oblasti IKT umožňující bezpečné poskytování služeb a aby se podílel na penetračním testu na základě hrozeb prováděném finančním subjektem a plně na něm spolupracoval.

(73) Smlouvy o poskytování služeb IKT podporujících zásadní nebo důležité funkce by měly rovněž obsahovat ustanovení poskytující finančnímu subjektu nebo určené třetí straně práva na přístup, kontrolu a audit a právo pořizovat si kopie, což jsou společně s úplnou spoluprací poskytovatele služeb IKT z řad třetích stran klíčové nástroje průběžného sledování plnění těchto poskytovatelů služeb. Podobně by měl příslušný orgán finančního subjektu mít právo provést po předchozím oznámení kontrolu a audit poskytovatele služeb IKT z řad třetích stran, s výhradou ochrany důvěrných informací.

(74) Taková smluvní ujednání by měla rovněž stanovit specializované strategie ukončení smluvního vztahu umožňující zejména povinná přechodná období, během nichž by měli poskytovatelé služeb IKT z řad třetích stran nadále poskytovat příslušné služby s cílem snížit riziko narušení na úrovni finančního subjektu nebo mu podle složitosti poskytované služby IKT umožnit začít účinně využívat jiného poskytovatele služeb IKT z řad třetích stran, případně změnit interní řešení. Finanční subjekty spadající do oblasti působnosti směrnice 2014/59/EU by navíc měly zajistit, aby příslušné smlouvy týkající se služeb IKT byly v případě řešení krize těchto finančních subjektů spolehlivé a plně vymahatelné. Tyto finanční subjekty by měly v souladu s předpoklady orgánů příslušných k řešení krize zajistit, aby byly příslušné smlouvy týkající se služeb IKT odolné vůči takovým krizím. Pokud tyto finanční subjekty nadále plní své platební povinnosti, měly by mimo jiné zajistit, aby příslušné smlouvy týkající se služeb IKT obsahovaly doložky o neukončení, nepozastavení a nezměněném stavu z důvodu restrukturalizace nebo řešení krize.

(75) Kromě toho by dobrovolné použití standardních smluvních doložek vypracovaných veřejnými orgány nebo orgány Unie, zejména použití standardních smluvních doložek vypracovaných Komisí pro cloudové služby, mohlo dále zjednodušit situaci finančních subjektů a poskytovatelů služeb IKT z řad třetích stran, protože se zvýší jejich úroveň právní jistoty ohledně využívání cloudových služeb ve finančním sektoru v úplném souladu s požadavky a předpoklady stanovenými v právu Unie v oblasti finančních služeb. Vypracování standardních smluvních doložek 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.

(76) S cílem podpořit konvergenci a účinnost v souvislosti s přístupy k dohledu při řešení rizika v oblasti IKT spojeného s třetími stranami ve finančním sektoru, jakož i posílit digitální provozní odolnost finančních subjektů, které se při poskytování služeb IKT podporujících poskytování finančních služeb spoléhají na kritické poskytovatele služeb IKT z řad třetích stran, a pomoci tak zachovat stabilitu finančního systému Unie a integritu vnitřního trhu s finančními službami, by měli kritičtí poskytovatelé služeb IKT z řad třetích stran podléhat unijnímu rámci dohledu. I když je zřízení rámce dohledu odůvodněno přidanou hodnotou přijetí opatření na úrovni Unie a inherentní úlohou a zvláštnostmi využívání služeb IKT při poskytování finančních služeb, mělo by být zároveň připomenuto, že toto řešení se jeví jako vhodné pouze v kontextu tohoto nařízení, které se konkrétně zabývá digitální provozní odolností ve finančním sektoru. Tento rámec dohledu by však neměl být považován za nový model dohledu Unie v oblasti finančních služeb a činností.

(77) Rámec dohledu by se měl vztahovat pouze na kritické poskytovatele služeb IKT z řad třetích stran. Proto by měl existovat mechanismus určování, který by zohlednil rozměr a povahu závislosti finančního sektoru na těchto poskytovatelích služeb IKT z řad třetích stran. Tento mechanismus by měl zahrnovat soubor kvantitativních a kvalitativních kritérií pro stanovení parametrů kritičnosti jako základu pro začlenění do rámce dohledu. Aby byla zajištěna přesnost tohoto posouzení a bez ohledu na organizační strukturu poskytovatele služeb IKT z řad třetích stran, měla by tato kritéria v případě poskytovatele služeb IKT z řad třetích stran, který je součástí širší skupiny, zohlednit celou strukturu skupiny poskytovatele služeb IKT z řad třetích stran. Na jedné straně by kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří nebudou automaticky určeni na základě použití výše uvedených kritérií, měli mít možnost zapojit se do rámce dohledu dobrovolně, na straně druhé by poskytovatelé služeb IKT z řad třetích stran, na něž se již vztahují rámce mechanismů dohledu podporující plnění úkolů na úrovni Evropského systému centrálních bank podle čl. 127 odst. 2 Smlouvy o fungování EU, by z něj měli být následně vyňati.

(78) Podobně by finanční subjekty poskytující služby IKT jiným finančním subjektům, ačkoli patří do kategorie poskytovatelů služeb IKT z řad třetích stran podle tohoto nařízení, měly být rovněž vyňaty z rámce dohledu, neboť již podléhají mechanismům dohledu stanoveným příslušným právem Unie v oblasti finančních služeb. Příslušné orgány by případně měly v rámci svých dohledových činností zohlednit riziko v oblasti IKT, které pro finanční subjekty představují finanční subjekty poskytující služby IKT. Stejně tak by vzhledem ke stávajícím mechanismům sledování rizika na úrovni skupiny měla být stejná výjimka zavedena pro poskytovatele služeb IKT z řad třetích stran, kteří poskytují služby převážně subjektům své vlastní skupiny. Poskytovatelé služeb IKT z řad třetích stran, kteří poskytují služby IKT pouze v jednom členském státě finančním subjektům, které působí pouze v tomto členském státě, by měli být rovněž vyňati z mechanismu určování z toho důvodu, že jejich činnosti jsou omezené a mají nedostatečný přeshraniční dopad.

(79) Digitální transformace v oblasti finančních služeb přinesla nebývalou míru využívání a spoléhání se na služby IKT. Jelikož se stalo nemyslitelným poskytovat finanční služby bez využití cloudových služeb, softwarových řešení a služeb souvisejících s daty, stal se finanční ekosystém Unie ze své podstaty závislým na některých službách IKT poskytovaných poskytovateli služeb IKT. Někteří z těchto poskytovatelů, inovátoři ve vývoji a používání technologií založených na IKT, hrají při poskytování finančních služeb významnou úlohu nebo jsou již do hodnotového řetězce finančních služeb začleněni. Získali tak zásadní postavení pro stabilitu a integritu finančního systému Unie. Tato rozšířená závislost na službách poskytovaných kritickými poskytovateli služeb IKT z řad třetích stran ve spojení se vzájemnou závislostí informačních systémů různých účastníků trhu vytváří přímé a potenciálně závažné riziko pro systém finančních služeb Unie a pro kontinuitu poskytování finančních služeb, pokud by byli kritičtí poskytovatelé služeb IKT z řad třetích stran ovlivněni provozními narušeními nebo závažnými kybernetickými incidenty. Kybernetické incidenty mají charakteristickou schopnost množit se a šířit se v celém finančním systému výrazně rychleji než jiné druhy rizika monitorované ve finančním sektoru a mohou se rozšířit napříč odvětvími i za zeměpisnými hranicemi. Mají potenciál stát se systémovou krizí, pokud došlo k narušení důvěry ve finanční systém v důsledku narušení funkcí podporujících reálnou ekonomiku nebo značných finančních ztrát, které dosáhly úrovně, kterou finanční systém není schopen zvládnout nebo která vyžaduje zavedení rozsáhlých opatření pro absorpci otřesů. Aby se zabránilo těmto scénářům, a tím i ohrožení finanční stability a integrity Unie, je nezbytné zajistit sbližování postupů dohledu týkajících se rizika v oblasti IKT spojeného s třetími stranami ve finančním sektoru, zejména prostřednictvím nových pravidel umožňujících dohled Unie nad kritickými poskytovateli služeb IKT z řad třetích stran.

(80) Rámec dohledu do značné míry závisí na míře spolupráce mezi hlavním orgánem dohledu a kritickým poskytovatelem služeb IKT z řad třetích stran, který poskytuje finančním subjektům služby ovlivňující nabídku finančních služeb. Úspěšný dohled závisí mimo jiné na schopnosti hlavního orgánu dohledu účinně provádět úkoly v oblasti sledování a kontroly s cílem posoudit pravidla, kontroly a procesy používané kritickými poskytovateli služeb IKT z řad třetích stran a posoudit potenciální kumulativní dopad jejich činností na finanční stabilitu a integritu finančního systému. Zároveň je zásadní, aby se kritičtí poskytovatelé služeb IKT z řad třetích stran řídili doporučeními hlavního orgánu dohledu a zabývali se jeho obavami. Vzhledem k tomu, že nedostatečná spolupráce kritického poskytovatele služeb IKT z řad třetích stran poskytujícího služby, jež ovlivňují nabídku finančních služeb, jako je odmítnutí přístupu do jeho prostor nebo poskytnutí informací, by v konečném důsledku zbavila hlavní orgán dohledu jeho základních nástrojů pro posuzování rizika v oblasti IKT spojeného s třetími stranami a mohla by mít nepříznivý dopad na finanční stabilitu a integritu finančního systému, je rovněž nezbytné stanovit přiměřený sankční režim.

(81) V této souvislosti by potřebu hlavního orgánu dohledu ukládat penále s cílem přimět kritické poskytovatele služeb IKT z řad třetích stran k dodržování povinností týkajících se transparentnosti a přístupu stanovených v tomto nařízení neměly ohrozit obtíže způsobené vymáháním těchto penále ve vztahu ke kritickým poskytovatelům služeb IKT z řad třetích stran usazeným ve třetích zemích. V zájmu zajištění vymahatelnosti těchto sankcí a umožnění rychlého zavedení postupů, které respektují práva kritických poskytovatelů služeb IKT z řad třetích stran na obhajobu v souvislosti s mechanismem určování a vydáváním doporučení, by tito kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří poskytují finančním subjektům služby ovlivňující nabídku finančních služeb, měli být povinni udržovat přiměřenou obchodní přítomnost v Unii. Vzhledem k povaze dohledu a neexistenci srovnatelných ujednání v jiných jurisdikcích neexistují žádné vhodné alternativní mechanismy zajišťující tento cíl prostřednictvím účinné spolupráce s orgány dohledu ve finančním sektoru ve třetích zemích v souvislosti se sledováním dopadu digitálních provozních rizik představovaných systémovými poskytovateli služeb IKT z řad třetích stran, kteří jsou považováni za kritické poskytovatele služeb IKT z řad třetích stran usazené ve třetích zemích. S cílem nadále poskytovat svoje služby IKT finančním subjektům v Unii by poskytovatel služeb IKT z řad třetích stran usazený ve třetí zemi, který byl určen jako kritický podle tohoto nařízení, měl do 12 měsíců od takového určení přijmout veškerá nezbytná opatření k tomu, aby zabezpečil svoje začlenění v Unii, a to založením dceřiného podniku, jak je uvedeno v *acquis* Unie, konkrétně ve směrnici Evropského parlamentu a Rady 2013/34/EU[1].

[1] Směrnice Evropského parlamentu a Rady 2013/34/EU ze dne 26. června 2013 o ročních účetních závěrkách, konsolidovaných účetních závěrkách a souvisejících zprávách některých forem podniků, o změně směrnice Evropského parlamentu a Rady 2006/43/ES a o zrušení směrnic Rady 78/660/EHS a 83/349/EHS (Úř. věst. L 182, 29.6.2013, s. 19).

(82) Požadavek na založení dceřiného podniku v Unii by neměl kritickému poskytovateli služeb IKT z řad třetích stran bránit v poskytování služeb IKT a související technické podpory ze zařízení a infrastruktury nacházejících se mimo Unii. Toto nařízení neukládá povinnost lokalizace údajů, neboť nevyžaduje uchovávání nebo zpracování údajů v Unii.

(83) Kritičtí poskytovatelé služeb IKT z řad třetích stran by měli mít možnost poskytovat služby IKT odkudkoli na světě, nikoli nezbytně nebo výhradně z prostor nacházejících se v Unii. Činnosti v oblasti dohledu by měly být nejprve prováděny v prostorách nacházejících se v Unii a prostřednictvím interakce se subjekty nacházejícími se v Unii, včetně dceřiných podniků založených kritickými poskytovateli služeb IKT z řad třetích stran podle tohoto nařízení. Tato opatření v rámci Unie by však mohla být nedostatečná k tomu, aby hlavnímu orgánu dohledu umožnila plně a účinně plnit jeho povinnosti podle tohoto nařízení. Hlavní orgán dohledu by proto měl mít rovněž možnost vykonávat své příslušné pravomoci dohledu ve třetích zemích. Výkon těchto pravomocí ve třetích zemích by měl hlavnímu orgánu dohledu umožnit přezkoumat zařízení, z nichž jsou služby IKT nebo služby technické podpory kritickým poskytovatelem služeb IKT z řad třetích stran skutečně poskytovány nebo spravovány, a měl by hlavnímu orgánu dohledu poskytnout komplexní a provozní pochopení řízení rizika v oblasti IKT kritického poskytovatele služeb IKT z řad třetích stran. Možnost, aby hlavní orgán dohledu jakožto agentura Unie vykonával pravomoci mimo území Unie, by měla být řádně vymezena odpovídajícími podmínkami, zejména souhlasem dotčeného kritického poskytovatele služeb IKT z řad třetích stran. Podobně by měly být o výkonu činností hlavního orgánu dohledu na území třetí země informovány relevantní orgány této země a neměly by proti němu mít námitky. K zajištění účinného provádění, a aniž jsou dotčeny příslušné pravomoci orgánů Unie a členských států, je však třeba tyto pravomoci rovněž plně zakotvit v ujednáních o správní spolupráci uzavíraných s relevantními orgány dotčené třetí země. Toto nařízení by proto mělo evropským orgánům dohledu umožnit uzavírat ujednání o správní spolupráci s relevantními orgány třetích zemí, které by jinak neměly vytvářet právní závazky vůči Unii a jejím členským státům.

(84) Pro usnadnění komunikace s hlavním orgánem dohledu a zajištění odpovídajícího zastoupení by kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří jsou součástí skupiny, měli určit jednu právnickou osobu jako své koordinační místo.

(85) Rámec dohledu se netýká pravomoci členských států provádět vlastní úkoly v oblasti dohledu nebo sledování, pokud jde o poskytovatele služeb IKT z řad třetích stran, kteří nejsou podle tohoto nařízení určeni jako kritičtí, ovšem kteří jsou považováni za významné na vnitrostátní úrovni.

(86) Aby se využilo 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 rizika v oblasti IKT. Měl by mu pomáhat nový podvýbor (Fórum dohledu), který bude provádět přípravné práce jak pro individuální rozhodnutí určená kritickým poskytovatelům služeb IKT z řad třetích stran, tak pro vydávání kolektivních doporučení, zejména ohledně porovnávání testování programů dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran, a současně bude identifikovat osvědčené postupy pro řešení otázek rizika koncentrace IKT.

(87) Aby se zajistilo, že na úrovni Unie bude na kritické poskytovatele služeb IKT z řad třetích stran dohlíženo přiměřeně a účinně, toto nařízení stanoví, že jako hlavní orgán dohledu by mohl být určen kterýkoli ze tří evropských orgánů dohledu. Individuální přidělení kritického poskytovatele služeb IKT z řad třetích stran jednomu ze tří evropských orgánů dohledu by mělo být výsledkem posouzení převahy finančních subjektů působících ve finančních sektorech, za něž má tento evropský orgán dohledu odpovědnost. Tento přístup by měl vést k vyváženému rozdělení úkolů a povinností mezi tři evropské orgány dohledu v souvislosti s výkonem funkcí dohledu a měl by co nejlépe využívat lidské zdroje a technické odborné znalosti, které jsou k dispozici v každém ze tří evropských orgánů dohledu.

(88) Hlavním orgánům dohledu by měly být uděleny nezbytné pravomoci k provádění šetření a kontrol v prostorách a na místech kritických poskytovatelů služeb IKT z řad třetích stran, aby získaly úplné a aktualizované informace. Tyto pravomoci by měly hlavnímu orgánu dohledu umožnit reálně pochopit druh, rozměr a dopad rizika v oblasti IKT spojeného s třetími stranami pro finanční subjekty a konečně i pro finanční systém Unie. Pověření evropských orgánů dohledu úlohou hlavního dohledu je nutným předpokladem k pochopení a řešení systémového rozměru rizika v oblasti IKT ve finančním sektoru. Vliv kritických poskytovatelů služeb IKT z řad třetích stran na finanční sektor Unie a potenciální problémy způsobené souvisejícím rizikem koncentrace IKT si žádají přijetí kolektivního přístupu na úrovni Unie. Souběžné provádění několika auditů a přístupových práv realizované ze strany početných příslušných orgánů samostatně, s nízkou či žádnou vzájemnou koordinací by orgánům dohledu ve finančním sektoru bránilo získat úplný a komplexní přehled o riziku v oblasti IKT spojeném s třetími stranami v Unii a současně by rovněž pro kritické poskytovatele služeb IKT z řad třetích stran vytvářelo nadbytečnost, zatížení a složitost, pokud by se na ně tyto četné požadavky sledování a kontroly vztahovaly.

(89) Vzhledem k významnému dopadu určení za kritického poskytovatele by toto nařízení mělo zajistit, aby práva kritických poskytovatelů služeb IKT z řad třetích stran byla dodržována po celou dobu provádění rámce dohledu. Před tím, než budou tito poskytovatelé určeni jako kritičtí poskytovatelé, by měli mít například právo předložit hlavnímu orgánu dohledu odůvodněné prohlášení obsahující veškeré relevantní informace pro účely posouzení týkajícího se jejich určení. Vzhledem k tomu, že hlavnímu orgánu dohledu by měla být svěřena pravomoc předkládat doporučení ohledně rizika v oblasti IKT a vhodných nápravných prostředků, včetně práva nesouhlasit s některými smluvními ujednáními, která v konečném důsledku dopadají na stabilitu finančního subjektu či finančního systému, kritičtí poskytovatelé služeb IKT z řad třetích stran by rovněž měli mít možnost podat před dokončením těchto doporučení vysvětlení, pokud jde o očekávaný dopad řešení navrhovaných v doporučeních na zákazníky, kteří jsou subjekty, jež nespadají do oblasti působnosti tohoto nařízení, a navrhnout řešení s cílem zmírnit rizika. Kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří s doporučeními nesouhlasí, by rovněž měli mít možnost předložit odůvodněné vysvětlení svého záměru doporučení neuznat. Není-li takové odůvodněné vysvětlení předloženo nebo je-li považováno za nedostatečné, měl by hlavní orgán dohledu vydat veřejné oznámení, v němž stručně popíše záležitost týkající se nesouladu.

(90) Příslušné orgány by měly do svých funkcí, pokud jde o obezřetnostní dohled nad finančními subjekty, náležitě zahrnout úkol ověřování věcného dodržování doporučení vydaných hlavním orgánem dohledu. Příslušné orgány by měly mít možnost požadovat, aby finanční subjekty přijaly dodatečná opatření k řešení rizik identifikovaných v doporučeních hlavního orgánu dohledu, a měly by za tímto účelem včas vydávat oznámení. Pokud hlavní orgán dohledu vydá doporučení kritickým poskytovatelům služeb IKT z řad třetích stran, nad nimiž je vykonáván dohled podle směrnice (EU).../...[+], měly by mít příslušné orgány možnost dobrovolně a před přijetím dalších opatření konzultovat příslušné orgány podle uvedené směrnice s cílem podpořit koordinovaný přístup k jednání s dotčenými kritickými poskytovateli služeb IKT z řad třetích stran.

(91) Výkon dohledu by se měl řídit třemi provozními zásadami, jejichž cílem je zajistit: a) úzkou koordinaci mezi evropskými orgány dohledu v jejich úlohách hlavního orgánu dohledu prostřednictvím společné sítě dohledu, b) soulad s rámcem stanoveným směrnicí (EU).../...[+] (prostřednictvím dobrovolné konzultace se subjekty na základě uvedené směrnice s cílem zabránit zdvojování opatření zaměřených na kritické poskytovatele služeb IKT z řad třetích stran a c) uplatňování náležité péče s cílem minimalizovat potenciální riziko narušení služeb poskytovaných kritickými poskytovateli služeb IKT z řad třetích stran zákazníkům, kteří jsou subjekty nespadajícími do oblasti působnosti tohoto nařízení.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

(92) Rámec dohledu by neměl nahrazovat ani žádným způsobem či podílem zastupovat povinnost finančních subjektů samostatně řídit rizika spojená s poskytovateli služeb IKT z řad třetích stran, včetně povinnosti průběžně sledovat smluvní ujednání uzavřená s kritickými poskytovateli služeb IKT z řad třetích stran. Obdobně by rámec dohledu neměl ovlivňovat úplnou odpovědnost finančních subjektů za dodržování a splnění všech právních povinností stanovených v tomto nařízení a v příslušném právu v oblasti finančních služeb.

(93) Aby se předešlo zdvojením a přesahům, neměly by příslušné orgány samostatně přijímat žádná opatření zaměřená na sledování rizik kritických poskytovatelů služeb ICT z řad třetích stran a měly by v tomto ohledu spoléhat pouze na příslušné posouzení hlavním orgánem dohledu. Veškerá opatření by se v každém případě měla předem koordinovat a odsouhlasit s hlavním orgánem dohledu v kontextu provádění úkolů v rámci dohledu.

(94) Aby se podpořilo sbližování na mezinárodní úrovni, pokud jde o využívání osvědčených postupů při přezkumu a sledování řízení digitálního rizika poskytovatelů služeb IKT z řad třetích stran, měly by být evropské orgány dohledu vybízeny k uzavírání dohod o spolupráci s relevantními orgány dohledu a regulačními orgány třetích zemí.

(95) Aby se využilo zvláštních kompetencí, technických dovedností a odborných znalostí pracovníků specializujících se na operační riziko a riziko v oblasti IKT v rámci příslušných orgánů, tří evropských orgánů dohledu a na dobrovolném základě i příslušných orgánů podle směrnice (EU) .../...[+], měl by hlavní orgán dohledu čerpat z vnitrostátních schopností a znalostí v oblasti dohledu a vytvořit specializované kontrolní týmy pro jednotlivé kritické poskytovatele služeb IKT z řad třetích stran, a to seskupením meziodvětvových týmů na podporu příprav i provádění dohledových činností, včetně všeobecných šetření a kontrol kritických poskytovatelů služeb IKT z řad třetích stran na místě, jakož i veškerých nezbytných následných opatření.

(96) Zatímco náklady vyplývající z úkolů v oblasti dohledu by byly plně financovány z poplatků vybíraných od kritických poskytovatelů služeb IKT z řad třetích stran, je pravděpodobné, že evropským orgánům dohledu vzniknou před spuštěním rámce dohledu náklady na zavedení specializovaných systémů IKT podporujících budoucí dohled, neboť specializované systémy IKT by musely být vyvinuty a zavedeny předem. Toto nařízení proto stanoví model hybridního financování, v jehož rámci by byl rámec dohledu jako takový plně financován z poplatků, zatímco rozvoj systémů IKT evropských orgánů dohledu by byl financován z příspěvků Unie a příslušných vnitrostátních orgánů.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

(97) Příslušné orgány by měly mít všechny požadované kontrolní, vyšetřovací a sankční pravomoci, aby zajistily řádný výkon svých povinností podle tohoto nařízení. V zásadě by měly zveřejňovat oznámení o uložených správních sankcích. Finanční subjekty a poskytovatelé služeb IKT z řad třetích stran mohou být usazeni v různých členských státech a podléhat dohledu různých příslušných orgánů, a proto by uplatňování tohoto nařízení mělo být na jedné straně usnadněno úzkou spoluprací mezi relevantními příslušnými orgány, včetně ECB, pokud jde o zvláštní úkoly, které jí svěřuje nařízení (EU) č. 1024/2013, a na straně druhé konzultacemi s evropskými orgány dohledu prostřednictvím vzájemné výměny informací a poskytování pomoci v souvislosti s příslušnou činností dohledu.

(98) Za účelem další kvantifikace a kvalifikace kritérií pro určení poskytovatelů služeb IKT z řad třetích stran za kritické poskytovatele a harmonizace poplatků souvisejících s dohledem by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU s cílem doplnit toto nařízení tím, že se dále upřesní systémový dopad, který by mělo selhání nebo výpadek provozu poskytovatele služeb IKT z řad třetích stran na finanční subjekty, kterým poskytuje služby IKT, počet globálních systémově významných institucí (G-SVI) nebo jiných systémově významných institucí (J-SVI), jež využívají daného poskytovatele služeb IKT z řad třetích stran, počet poskytovatelů služeb IKT z řad třetích stran působících na daném trhu, náklady na migraci dat a pracovních úkolů v oblasti IKT při přechodu k jinému poskytovateli služeb IKT z řad třetích stran, jakož i výše 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[1]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci by Evropský parlament a Rada měly obdržet veškeré dokumenty současně s odborníky z členských států a jejich odborníci by měli mít automaticky přístup na zasedání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

[1] Úř. věst. L 123, 12.5.2016, s. 1.

(99) Konzistentní harmonizaci požadavků stanovených tímto nařízením by měly zajišťovat regulační technické normy. Evropské orgány dohledu by jako orgány disponující vysoce odbornými znalostmi měly vypracovat návrhy regulačních technických norem, které neobsahují politická rozhodnutí, a měly by je předložit Komisi. Regulační technické normy by měly být vypracovány v oblastech řízení rizika v oblasti IKT, hlášení závažných incidentů souvisejících s IKT, testování, jakož i ve vztahu ke klíčovým požadavkům na řádné sledování rizika v oblasti IKT spojeného s třetími stranami. Komise a evropské orgány dohledu by měly zajistit, aby tyto normy a požadavky mohly všechny finanční subjekty uplatňovat způsobem, který je přiměřený jejich velikosti a celkovému rizikovému profilu a povaze, rozsahu a složitosti jejich služeb, činností a operací. Komisi by měla být svěřena pravomoc přijímat tyto regulační technické normy prostřednictvím aktů v přenesené pravomoci podle článku 290 Smlouvy o fungování EU a v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

(100) Aby se usnadnila srovnatelnost hlášení o závažných incidentech souvisejících s IKT a závažných provozních nebo bezpečnostních incidentech spojených s platbami a rovněž zajistila transparentnost smluvních ujednání pro používání služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran, měly by evropské orgány dohledu vypracovat návrhy prováděcích technických norem, jimiž se stanoví standardizované vzory, formuláře a postupy, které budou finanční subjekty používat pro hlášení závažných incidentů souvisejících s IKT a závažných provozních nebo bezpečnostních incidentů spojených s platbami, a rovněž standardizované vzory pro registr informací. Při vypracovávání těchto norem by evropské orgány dohledu měly zohlednit velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací. Komisi by měla být svěřena pravomoc přijímat tyto prováděcí technické normy podle článku 291 Smlouvy o fungování EU a v souladu s článkem 15 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

(101) Protože již byly další požadavky specifikovány akty v přenesené pravomoci a prováděcími akty vycházejícími z technických regulačních a prováděcích technických norem v nařízeních Evropského parlamentu a Rady (ES) č. 1060/2009[1], (EU) č. 648/2012[2], (EU) č. 600/2014[3] a (EU) č. 909/2014[4], 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 rizika v oblasti IKT.

---

1 Nařízení Evropského parlamentu a Rady (ES) č. 1060/2009 ze dne 16. září 2009 o ratingových agenturách (Úř. věst. L 302, 17.11.2009, s. 1).

2 Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1).

3 Nařízení Evropského parlamentu a Rady (EU) č. 600/2014 ze dne 15. května 2014 o trzích finančních nástrojů a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 173, 12.6.2014, s. 84).

4 Nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnic 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012 (Úř. věst. L 257, 28.8.2014, s. 1).

(102) Jelikož toto nařízení, společně se směrnicí Evropského parlamentu a Rady (EU) .../...[1] +, obsahuje konsolidaci ustanovení o řízení rizika v oblasti IKT z několika 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 a nařízení Evropského parlamentu a Rady (EU) 2016/1011[2], je třeba za účelem zajištění úplné konzistentnosti tato nařízení změnit tak, aby se vyjasnilo, že použitelná ustanovení o riziku v oblasti IKT jsou uvedena v tomto nařízení.

(103) V důsledku toho je třeba upravit oblast působnosti příslušných článků o operačním riziku, na jejichž základě zmocnění uvedená v nařízeních (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 (EU) č. 909/2014 a (EU) 2016/1011 umožnila přijetí aktů v přenesené pravomoci a prováděcích aktů, tak aby byla do tohoto nařízení převzata všechna ustanovení týkající se aspektů digitální provozní odolnosti, jež jsou nyní součástí uvedených nařízení.

---

[1] Směrnice Evropského parlamentu a Rady (EU) .../..., kterou se mění směrnice 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341, pokud jde o digitální provozní odolnost ve finančním sektoru (Úř. věst. L ...., ..., s. ...).

\+ Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 42/22 (2020/0268(COD)).

[2] 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).

(104) Potenciální systémové kybernetické riziko spojené s využíváním infrastruktur IKT, které umožňují provoz platebních systémů a poskytování činností zpracování plateb, by mělo být na úrovni Unie řádně řešeno prostřednictvím harmonizovaných pravidel digitální odolnosti. Za tímto účelem by Komise měla urychleně posoudit potřebu přezkumu oblasti působnosti tohoto nařízení a zároveň uvést tento přezkum do souladu s výsledkem komplexního přezkumu plánovaného podle směrnice (EU) 2015/2366. Četné rozsáhlé útoky v posledním desetiletí ukazují, že jsou platební systémy vystavené kybernetickým hrozbám. Platební systémy a činnosti zpracování plateb získaly díky ústřednímu postavení v řetězci platebních služeb a prokázání silného propojení s celkovým finančním systémem zásadní význam pro fungování finančních trhů Unie. Kybernetické útoky na tyto systémy mohou způsobit závažná narušení provozu s přímým dopadem na klíčové ekonomické funkce jako usnadnění plateb a nepřímým dopadem na související ekonomické procesy. Dokud nebude na úrovni Unie zaveden harmonizovaný režim a dohled nad provozovateli platebních systémů a zpracovateli, mohou se členské státy za účelem uplatňování podobných tržních postupů inspirovat požadavky na digitální provozní odolnost stanovenými v tomto nařízení při uplatňování pravidel na provozovatele platebních systémů a zpracovatele, nad nimiž je vykonáván dohled v rámci jejich vlastní jurisdikce.

(105) Jelikož cíle tohoto nařízení, totiž dosažení vysoké úrovně digitální provozní odolnosti u regulovaných finančních subjektů, nemůže být dosaženo uspokojivě členskými státy, jelikož je nutná harmonizace různých pravidel v unijním a vnitrostátním právu, ale spíše jej z důvodu rozsahu a účinků tohoto nařízení 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.

(106) Evropský inspektor ochrany údajů byl konzultován v souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725[1] a dne 10. května 2021 vydal své stanovisko[2],

PŘIJALY TOTO NAŘÍZENÍ:

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

[2] Úř. věst. C 229, 15.6.2021, s. 16.

# Kapitola I
# Obecná ustanovení

*Článek 1*

*Předmět*

1. Za účelem dosažení vysoké společné úrovně digitální provozní odolnosti stanoví toto nařízení následující jednotné požadavky týkající se bezpečnosti sítí a informačních systémů podporujících obchodní procesy finančních subjektů:

   a) požadavky vztahující se na finanční subjekty týkající se:

      i) řízení rizika v oblasti informačních a komunikačních technologií (IKT);

      ii) hlášení závažných incidentů souvisejících s IKT a dobrovolné oznamování významných kybernetických hrozeb příslušným orgánům;

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

      iv) testování digitální provozní odolnosti;

v) sdílení operativních a jiných informací souvisejících s kybernetickými hrozbami a zranitelnostmi;

vi) opatření pro řádné řízení rizika v oblasti IKT spojeného s třetími stranami;

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

c) pravidla pro stanovení a fungování rámce dohledu nad kritickými poskytovateli 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 základní nebo důležité subjekty podle vnitrostátních předpisů provádějících článek 3 směrnice (EU) .../...[+] se toto nařízení pro účely článku 4 uvedené směrnice považuje za odvětvový právní akt Unie.

3. Tímto nařízením není dotčena odpovědnost členských států, pokud jde o základní funkce státu týkající se veřejné bezpečnosti, obrany a národní bezpečnosti v souladu s právem Unie.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

*Článek 2*

*Oblast působnosti*

1. Aniž jsou dotčeny odstavce 3 a 4, vztahuje se toto nařízení na tyto subjekty:

a) úvěrové instituce;

b) platební instituce, včetně platebních institucí vyňatých podle směrnice (EU) 2015/2366;

c) poskytovatele služeb informování o účtu;

d) instituce elektronických peněz, včetně institucí elektronických peněz vyňatých podle směrnice 2009/110/ES;

e) investiční podniky;

f) poskytovatele služeb souvisejících s kryptoaktivy, kterým bylo uděleno povolení podle nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 („nařízení o trzích s kryptoaktivy“), a vydavatele tokenů vázaných na aktiva;

g) centrální depozitáře cenných papírů;

h) ústřední protistrany;

i) obchodní systémy;

j) registry obchodních údajů;

k) správce alternativních investičních fondů;

l) správcovské společnosti;

m) poskytovatele služeb hlášení údajů;

n) pojišťovny a zajišťovny;

o) zprostředkovatele pojištění, zprostředkovatele zajištění a zprostředkovatele doplňkového pojištění;

p) instituce zaměstnaneckého penzijního pojištění;

q) ratingové agentury;

r) správce kritických referenčních hodnot;

s) poskytovatele služeb skupinového financování;

t) registry sekuritizací;

u) poskytovatele služeb IKT z řad třetích stran.

2. Subjekty uvedené v odst. 1 písm. a) až t) jsou pro účely tohoto nařízení souhrnně nazývány „finančními subjekty“.

3. Toto nařízení se nevztahuje na:

a) správce alternativních investičních fondů podle čl. 3 odst. 2 směrnice 2011/61/EU;

b) pojišťovny a zajišťovny podle článku 4 směrnice 2009/138/ES;

c) instituce zaměstnaneckého penzijního pojištění, které provozují penzijní plány, které dohromady nemají více než 15 účastníků;

d) fyzické nebo právnické osoby vyňaté podle článků 2 a 3 směrnice 2014/65/EU;

e) zprostředkovatele pojištění, zprostředkovatele zajištění a zprostředkovatele doplňkového pojištění, kteří jsou mikropodniky, malými nebo středními podniky;

f) žirové instituce poštovních úřadů podle čl. 2 odst. 5 bodu 3 směrnice 2013/36/EU.

4. Členské státy mohou z oblasti působnosti tohoto nařízení vyloučit subjekty uvedené v čl. 2 odst. 5 bodech 4 až 23 směrnice 2013/36/EU, které se nacházejí na jejich území. Pokud členský stát této možnosti využije, uvědomí o tom i o veškerých následných změnách Komisi. Komise tyto informace zveřejní na svých internetových stránkách nebo jinými snadno dostupnými prostředky.

*Článek 3*

*Definice*

Pro účely tohoto nařízení se rozumí:

1) „digitální provozní odolností“ schopnost finančního subjektu budovat, zajišťovat a revidovat svoji provozní integritu a spolehlivost prostřednictvím zajištění, ať již přímo, či nepřímo s využitím služeb poskytovaných poskytovateli služeb IKT z řad třetích stran, veškerých schopností souvisejících s IKT nezbytných k řešení otázek bezpečnosti sítí a informačních systémů, které finanční subjekt používá a které přispívají k nepřetržitému poskytování finančních služeb a k jejich kvalitě, mimo jiné i během narušení;

2) „sítí a informačním systémem“ síť a informační systém ve smyslu čl. 6 bodu 1 směrnice (EU) .../...[+];

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

3) „původním systémem IKT“ systém IKT, který dosáhl konce svého životního cyklu (konec životnosti), který není vhodný pro modernizaci nebo opravy z technologických nebo obchodních důvodů nebo který již není podporován svým dodavatelem nebo poskytovatelem služeb IKT z řad třetích stran, ale který je stále používán a podporuje funkce finančního subjektu;

4) „bezpečností sítí a informačních systémů“ bezpečnost sítí a informačních systémů ve smyslu čl. 6 bodu 2 směrnice (EU) .../...[+];

5) „rizikem v oblasti IKT“ veškeré rozumně rozpoznatelné okolnosti související s používáním sítí a informačních systémů, které, pokud by k nim došlo, mohou narušit bezpečnost sítí a informačních systémů, jakéhokoli na technologiích závislého nástroje nebo postupu, operací a procesů nebo poskytování služeb vznikem nepříznivých dopadů v digitálním nebo fyzickém prostředí;

6) „informačním aktivem“ soubor informací, v hmotné i nehmotné formě, které je potřeba chránit;

7) „aktivem v oblasti IKT“ softwarové nebo hardwarové aktivum v síti a informačních systémech používané finančním subjektem;

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

8) „incidentem souvisejícím s IKT“ jediná událost nebo řada propojených událostí, které finanční subjekt neplánoval a které ohrožují bezpečnost sítí a informačních systémů a mají nepříznivý dopad na dostupnost, hodnověrnost, integritu nebo důvěrnost údajů nebo na služby, které finanční subjekt poskytuje;

9) „provozním nebo bezpečnostním incidentem souvisejícím s platbami“ jediná událost nebo řada propojených událostí, které finanční subjekty uvedené v čl. 2 odst. 1 písm. a) až d) neplánovaly a které mají nepříznivý dopad na dostupnost, hodnověrnost, integritu nebo důvěrnost údajů souvisejících s platbami nebo na služby související s platbami, které finanční subjekt poskytuje, a to bez ohledu na to, zda souvisí s IKT či nikoli;

10) „závažným incidentem souvisejícím s IKT“ incident související s IKT, který má velký nepříznivý dopad na síť a informační systémy využívané k zajištění zásadních nebo důležitých funkcí finančního subjektu;

11) „závažným provozním nebo bezpečnostním incidentem souvisejícím s platbami“ provozní nebo bezpečnostní incident související s platbami, který má velký nepříznivý dopad na poskytované služby související s platbami;

12) „kybernetickou hrozbou“ kybernetická hrozba ve smyslu čl. 2 bodu 8 nařízení (EU) 2019/881;

13) „významnou kybernetickou hrozbou“ kybernetická hrozba, jejíž technické vlastnosti naznačují, že by mohla vést k závažnému incidentu souvisejícímu s IKT nebo k závažnému provoznímu nebo bezpečnostnímu incidentu souvisejícímu s platbami;

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

15) „operativními informacemi o hrozbách“ informace, které byly shromážděny, zpracovány, analyzovány, interpretovány nebo rozšířeny tak, aby poskytovaly nezbytné souvislosti pro rozhodování a umožňovaly relevantní a dostatečné pochopení s cílem zmírnit dopad incidentu souvisejícího s IKT nebo kybernetické hrozby, včetně technických údajů o kybernetickém útoku, osobách odpovědných za útok a jejich *modu operandi* a motivaci;

16) „zranitelností“ slabina, citlivost nebo chyba aktiva, systému, procesu nebo kontroly, jichž může být využito;

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

18) „rizikem v oblasti IKT spojeným s třetími stranami“ riziko pro finanční subjekt v oblasti IKT, které může vzniknout v souvislosti s jeho využíváním služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran nebo jejich subdodavateli, a to i prostřednictvím dohod o externím zajištění služeb;

19) „poskytovatelem služeb IKT z řad třetích stran“ podnik poskytující služby IKT;

20) „poskytovatelem služeb IKT v rámci skupiny“ podnik, který je součástí finanční skupiny a poskytuje služby IKT převážně finančním subjektům v rámci téže skupiny nebo finančním subjektům v rámci téhož institucionálního systému ochrany, včetně jejich mateřským podniků, dceřiných podniků nebo poboček či dalších subjektů, které mají stejného majitele nebo jsou pod jeho kontrolou;

21) „službami IKT“ digitální a datové služby poskytované prostřednictvím systémů IKT průběžně jednomu nebo více interním nebo externím uživatelům, včetně hardwaru jako služby a hardwarových služeb, které zahrnují poskytování technické podpory prostřednictvím aktualizací softwaru nebo firmwaru poskytovatelem hardwaru, s výjimkou tradičních analogových telefonních služeb;

22) „zásadní nebo důležitou funkcí“ funkce, jejíž narušení by významně narušilo finanční výkonnost finančního subjektu nebo řádný průběh nebo kontinuitu jeho služeb a činností 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 platného práva v oblasti finančních služeb;

23) „kritickým poskytovatelem služeb IKT z řad třetích stran“ poskytovatel služeb IKT z řad třetích stran určený jako kritický v souladu s článkem 31;

24) „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 který uzavřel smluvní ujednání s finančním subjektem na poskytování služeb IKT;

25) „dceřiným podnikem“ dceřiný podnik ve smyslu čl. 2 bodu 10 a článku 22 směrnice 2013/34/EU;

26) „skupinou“ skupina ve smyslu čl. 2 bodu 11 směrnice 2013/34/EU;

27) „mateřským podnikem“ mateřský podnik ve smyslu čl. 2 bodu 9 a článku 22 směrnice 2013/34/EU;

28) „subdodavatelem IKT usazeným ve třetí zemi“ subdodavatel IKT, který je právnickou osobou usazenou ve třetí zemi a který 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;

29) „rizikem koncentrace IKT“ expozice vůči jednomu či několika propojeným kritickým poskytovatelům služeb IKT z řad třetích stran vytvářející takovou míru závislosti na těchto poskytovatelích, že jejich nedostupnost, selhání nebo jiná nedostatečnost mohou potenciálně ohrozit schopnost finančního subjektu poskytovat zásadní nebo důležité funkce nebo způsobit, že utrpí jinou újmu, včetně vysokých ztrát, nebo ohrozit finanční stabilitu celé Unie;

30) „vedoucím orgánem“ vedoucí orgán ve smyslu čl. 4 odst. 1 bodu 36 směrnice 2014/65/EU, čl. 3 odst. 1 bodu 7 směrnice 2013/36/EU, čl. 2 odst. 1 písm. s) směrnice Evropského parlamentu a Rady 2009/65/ES[1], čl. 2 odst. 1 bodu 45 nařízení (EU) č. 909/2014, čl. 3 odst. 1 bodu 20 nařízení (EU) 2016/1011 a příslušného ustanovení nařízení o trzích s kryptoaktivy nebo rovnocenné osoby, které skutečně řídí subjekt nebo zastávají klíčové funkce podle příslušného unijního nebo vnitrostátního práva;

[1] Směrnice Evropského parlamentu a Rady 2009/65/ES ze dne 13. července 2009 o koordinaci právních a správních předpisů týkajících se subjektů kolektivního investování do převoditelných cenných papírů (SKIPCP) (Úř. věst. L 302, 17.11.2009, s. 32).

31) „úvěrovou institucí“ úvěrová instituce ve smyslu čl. 4 odst. 1 bodu 1 nařízení Evropského parlamentu a Rady (EU) č. 575/2013[1];

32) „úvěrovou institucí vyňatou podle směrnice 2013/36/EU“ subjekt uvedený v čl. 2 odst. 5 bodech 4 až 23 směrnice 2013/36/EU;

33) „investičním podnikem“ investiční podnik ve smyslu čl. 4 odst. 1 bodu 1 směrnice 2014/65/EU;

34) „malým a nepropojeným investičním podnikem“ investiční podnik, který splňuje podmínky stanovené v čl. 12 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2019/2033[2];

35) „platební institucí“ platební instituce ve smyslu čl. 4 bodu 4 směrnice (EU) 2015/2366;

36) „platební institucí vyňatou podle směrnice (EU) 2015/2366“ platební instituce vyňatá podle čl. 32 odst. 1 směrnice (EU) 2015/2366;

37) „poskytovatelem služeb informování o účtu“ poskytovatel služeb informování o účtu ve smyslu čl. 33 odst. 1 směrnice (EU) 2015/2366;

---

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

2 Nařízení Evropského parlamentu a Rady (EU) 2019/2033 ze dne 27. listopadu 2019 o obezřetnostních požadavcích na investiční podniky a o změně nařízení (EU) č. 1093/2010, (EU) č. 575/2013, (EU) č. 600/2014 a (EU) č. 806/2014 (Úř. věst. L 314, 5.12.2019, s. 1).

38) „institucí elektronických peněz“ instituce elektronických peněz ve smyslu čl. 2 bodu 1 směrnice 2009/110/ES;

39) „institucí elektronických peněz vyňatou podle směrnice 2009/110/ES“ instituce elektronických peněz, na niž se podle čl. 9 odst. 1 směrnice 2009/110/ES vztahuje výjimka;

40) „ústřední protistranou“ ústřední protistrana ve smyslu čl. 2 bodu 1 nařízení (EU) č. 648/2012;

41) „registrem obchodních údajů“ registr obchodních údajů ve smyslu čl. 2 bodu 2 nařízení (EU) č. 648/2012;

42) „centrálním depozitářem cenných papírů“ centrální depozitář cenných papírů ve smyslu čl. 2 odst. 1 bodu 1 nařízení (EU) č. 909/2014;

43) „obchodním systémem“ obchodní systém ve smyslu čl. 4 odst. 1 bodu 24 směrnice 2014/65/EU;

44) „správcem alternativních investičních fondů“ správce alternativních investičních fondů ve smyslu čl. 4 odst. 1 písm. b) směrnice 2011/61/EU;

45) „správcovskou společností“ správcovská společnost ve smyslu čl. 2 odst. 1 písm. b) směrnice 2009/65/ES;

46) „poskytovatelem služeb hlášení údajů“ poskytovatel služeb hlášení údajů ve smyslu nařízení (EU) č. 600/2014, uvedený v čl. 2 odst. 1 bodech 34 až 36 daného nařízení;

47) „pojišťovnou“ pojišťovna ve smyslu čl. 13 bodu 1 směrnice 2009/138/ES;

48) „zajišťovnou“ zajišťovna ve smyslu čl. 13 bodu 4 směrnice 2009/138/ES;

49) „zprostředkovatelem pojištění“ zprostředkovatel pojištění ve smyslu čl. 2 odst. 1 bodu 3 směrnice Evropského parlamentu a Rady (EU) 2016/97[1];

50) „zprostředkovatelem doplňkového pojištění“ zprostředkovatel doplňkového pojištění ve smyslu čl. 2 odst. 1 bodu 4 směrnice (EU) 2016/97;

51) „zprostředkovatelem zajištění“ zprostředkovatel zajištění ve smyslu čl. 2 odst. 1 bodu 5 směrnice (EU) 2016/97;

52) „institucí zaměstnaneckého penzijního pojištění“ instituce zaměstnaneckého penzijního pojištění ve smyslu čl. 6 bodu 1 směrnice (EU) 2016/2341;

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2016/97 ze dne 20. ledna 2016 o distribuci pojištění (Úř. věst. L 26, 2.2.2016, s. 19).

53) „malou institucí zaměstnaneckého penzijního pojištění“ instituce zaměstnaneckého penzijního pojištění, která provozuje penzijní plány, které dohromady mají méně než 100 účastníků;

54) „ratingovou agenturou“ ratingová agentura ve smyslu čl. 3 odst. 1 písm. b) nařízení (ES) č. 1060/2009;

55) „poskytovatelem služeb souvisejících s kryptoaktivy“ poskytovatel služeb souvisejících s kryptoaktivy ve smyslu příslušného ustanovení nařízení o trzích s kryptoaktivy;

56) „vydavatelem tokenů vázaných na aktiva“ vydavatel tokenů vázaných na aktiva ve smyslu příslušného ustanovení nařízení o trzích s kryptoaktivy;

57) „správcem kritických referenčních hodnot“ správce kritických referenčních hodnot ve smyslu čl. 3 odst. 1 bodu 25 nařízení E (EU) 2016/1011;

58) „poskytovatelem služeb skupinového financování“ poskytovatel služeb skupinového financování ve smyslu čl. 2 odst. 1 písm. e) nařízení Evropského parlamentu a Rady (EU) 2020/1503[1];

59) „registrem sekuritizací“ registr sekuritizací ve smyslu čl. 2 bodu 23 nařízení Evropského parlamentu a Rady (EU) 2017/2402[2];

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2020/1503 ze dne 7. října 2020 o evropských poskytovatelích služeb skupinového financování pro podniky a o změně nařízení (EU) 2017/1129 a směrnice (EU) 2019/1937 (Úř. věst. L 347, 20.10.2020, s. 1).

[2] Nařízení Evropského parlamentu a Rady (EU) 2017/2402 ze dne 12. prosince 2017, kterým se stanoví obecný rámec pro sekuritizaci a vytváří se zvláštní rámec pro jednoduchou, transparentní a standardizovanou sekuritizaci a kterým se mění směrnice 2009/65/ES, 2009/138/ES, 2011/61/EU a nařízení (ES) č. 1060/2009 a (EU) č. 648/2012 (Úř. věst. L 347, 28.12.2017, s. 35).

60) „mikropodnikem“ finanční subjekt jiný než obchodní systém, ústřední protistrana, registr obchodních údajů nebo centrální depozitář cenných papírů, který zaměstnává méně než 10 osob a jehož roční obrat nebo celková roční bilanční suma nepřekračuje 2 miliony EUR;

61) „hlavním orgánem dohledu“ evropský orgán dohledu jmenovaný v souladu s čl. 31 odst. 1 písm. b) tohoto nařízení;

62) „společným výborem“ výbor uvedený v článku 54 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010;

63) „malým podnikem“ finanční subjekt, který zaměstnává nejméně 10 osob, avšak méně než 50 osob, a jehož roční obrat nebo celková roční bilanční suma překračuje 2 miliony EUR, avšak nepřekračuje 10 milionů EUR;

64) „středním podnikem“ finanční subjekt, který není malým podnikem a zaměstnává méně než 250 osob a jehož roční obrat nepřekračuje 50 milionů EUR nebo jehož roční bilanční suma nepřekračuje 43 milionů EUR;

65) „veřejným orgánem“ jakýkoli ústřední orgán nebo jiný subjekt veřejné správy, včetně národních centrálních bank.

*Článek 4*

*Zásada proporcionality*

1. Finanční subjekty uplatňují pravidla stanovená v kapitole II v souladu se zásadou proporcionality a s přihlédnutím ke své velikosti a celkovému rizikovému profilu a povaze, rozsahu a složitosti svých služeb, činností a operací.

2. Kromě toho je uplatňování kapitol III, IV a V oddílu I finančními subjekty přiměřené jejich velikosti a celkovému rizikovému profilu a povaze, rozsahu a složitosti jejich služeb, činností a operací, jak je konkrétně stanoveno v příslušných pravidlech uvedených kapitol.

3. Příslušné orgány zváží uplatňování zásady proporcionality finančními subjekty při přezkumu soudržnosti rámce pro řízení rizika v oblasti IKT na základě zpráv předložených na žádost příslušných orgánů podle čl. 6 odst. 5 a čl. 16 odst. 2.

# Kapitola II
# Řízení rizika v oblasti IKT

## ODDÍL I

*Článek 5*

*Řízení a organizace*

1. Finanční subjekty mají zaveden interní řídicí a kontrolní rámec, který zajistí účinné a obezřetné řízení rizika v oblasti IKT v souladu s čl. 6 odst. 4 s cílem dosáhnout vysoké úrovně digitální provozní odolnosti.

2. Vedoucí orgán finančního subjektu stanoví a schvaluje veškerá opatření související s rámcem pro řízení rizika v oblasti IKT podle čl. 6 odst. 1, dohlíží na jejich provádění a odpovídá za něj.

   Pro účely prvního pododstavce vedoucí orgán:

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

   b) zavádí postupy a strategie, jejichž cílem je zajistit zachování přísných norem v oblasti dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů;

c) stanoví jasné úlohy a povinnosti pro všechny funkce související s IKT a zavádí vhodné mechanismy řízení s cílem zajistit účinnou a včasnou komunikaci, spolupráci a koordinaci mezi uvedenými funkcemi;

d) nese celkovou odpovědnost za stanovení a schválení strategie digitální provozní odolnosti podle čl. 6 odst. 8, včetně stanovení přiměřené přípustné odchylky rizika v oblasti IKT u finančního subjektu podle čl. 6 odst. 8 písm. b);

e) schvaluje provádění politiky zachování provozu IKT finančního subjektu a plány reakce a obnovy v oblasti IKT uvedené v čl. 11 odst. 1 a 3, které mohou být přijaty jako zvláštní konkrétní politika tvořící nedílnou součást celkové politiky zachování provozu a plánu reakce a obnovy finančního subjektu, dohlíží na ně a pravidelně je přezkoumává;

f) schvaluje a pravidelně přezkoumává plány interních auditů IKT, které finanční subjekt vypracovává, audity IKT a jejich podstatné změny;

g) přiděluje a pravidelně přezkoumává odpovídající rozpočtové prostředky na pokrytí potřeb finančního subjektu v oblasti digitální provozní odolnosti s ohledem na všechny typy zdrojů, včetně relevantních programů zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti uvedených v čl. 13 odst. 6 a dovedností v oblasti IKT pro všechny zaměstnance;

h) schvaluje a pravidelně přezkoumává strategii finančního subjektu pro režimy využívání služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran;

i) na úrovni podniku zavede kanály pro oznamování, které mu umožní být řádně informován:

i) o ujednáních o využívání služeb IKT uzavřených s poskytovateli služeb IKT z řad třetích stran;

ii) o veškerých relevantních plánovaných podstatných změnách týkajících se poskytovatelů služeb IKT z řad třetích stran;

iii) o potenciálním dopadu těchto změn na zásadní nebo důležité funkce, které jsou předmětem těchto ujednání, včetně shrnutí analýzy rizik s cílem posoudit dopad těchto změn, a alespoň o závažných incidentech souvisejících s IKT a jejich dopadu, jakož i o opatřeních týkajících se reakce a obnovy a o nápravných opatřeních.

3. Finanční subjekty, jiné než mikropodniky, vytvoří funkci s cílem sledovat ujednání o využívání služeb IKT uzavřená s poskytovateli z řad třetích stran nebo pověří jednoho vedoucího pracovníka 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 rizika v oblasti IKT a jeho dopadů na fungování finančního subjektu, mimo jiné pravidelným absolvováním specifického školení úměrného riziku v oblasti IKT, jež je předmětem řízení.

## ODDÍL II

*Článek 6*

*Rámec pro řízení rizika v oblasti IKT*

1. Finanční subjekty mají spolehlivý, ucelený a dobře zdokumentovaný rámec pro řízení rizika v oblasti IKT jako součást svého celkového systému řízení rizika, který jim umožňuje řešit toto riziko rychle, účinně a komplexně a zajistit vysokou míru digitální provozní odolnosti.

2. Rámec pro řízení rizika v oblasti IKT obsahuje přinejmenším strategie, politiky, postupy, protokoly a nástroje IKT, jež jsou nezbytné pro řádnou a přiměřenou ochranu všech informačních aktiv a aktiv v oblasti IKT, včetně počítačového softwaru, hardwaru, serverů a rovněž všech relevantních fyzických součástí a infrastruktur, jako jsou místnosti, datová centra a citlivé určené prostory, aby byla zajištěna vhodná ochrana všech informačních aktiv a aktiv v oblasti IKT před riziky, včetně poškození a neoprávněného přístupu nebo použití.

3. Finanční subjekty v souladu se svým rámcem pro řízení rizika v oblasti IKT minimalizují dopad rizika v oblasti IKT zaváděním vhodných strategií, politik, postupů, protokolů a nástrojů. Poskytují úplné a aktualizované informace o riziku v oblasti IKT a o svém rámci pro řízení rizika v oblasti IKT na žádost příslušných orgánů.

4. Finanční subjekty, jiné než mikropodniky, pověří odpovědností za řízení a kontrolu rizika v oblasti IKT kontrolní funkci a zajistí odpovídající úroveň nezávislosti této kontrolní funkce, aby nedocházelo ke střetům zájmů. Finanční subjekty zajistí náležité oddělení a nezávislost vedoucích funkcí, kontrolních funkcí a interních auditních funkcí v oblasti rizika IKT podle modelu tří linií obrany nebo interního modelu řízení a kontroly rizika.

5. Rámec pro řízení rizika v oblasti IKT se zdokumentuje a reviduje alespoň jednou ročně nebo pravidelně v případě mikropodniků 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 sledování. Zpráva o přezkumu rámce pro řízení rizika v oblasti IKT se na žádost předkládá příslušnému orgánu.

6. Rámec pro řízení rizika v oblasti IKT finančních subjektů, jiných než mikropodniky, podléhá pravidelnému internímu auditu prováděnému auditory v souladu s plánem auditu finančních subjektů. Tito auditoři mají dostatečné znalosti, dovednosti a odborné znalosti, pokud jde o riziko v oblasti IKT, jakož i přiměřenou nezávislost. Četnost a zaměření auditů IKT odpovídají riziku finančního subjektu v oblasti IKT.

7. Na základě závěrů z interního auditu zavedou finanční subjekty formální následný postup, včetně pravidel pro včasné ověření a nápravu kritických zjištění auditu IKT.

8. Rámec pro řízení rizika v oblasti IKT zahrnuje strategii digitální provozní odolnosti, v níž se stanoví způsob jeho uplatňování. Za tímto účelem zahrnuje strategie digitální provozní odolnosti metody řešení rizika v oblasti IKT a plnění specifických cílů v oblasti IKT, a to formou:

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

   b) stanovení přípustné odchylky rizika v oblasti IKT podle ochoty finančního subjektu podstupovat riziko a analýzy tolerance dopadů narušení v oblasti IKT;

   c) stanovení jasných cílů v oblasti bezpečnosti informací, včetně klíčových ukazatelů výkonnosti a klíčových ukazatelů k měření rizika;

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

e) uvedení různých mechanismů zavedených za účelem detekce incidentů souvisejících s IKT, prevence jejich dopadů a ochrany před nimi;

f) doložení stávající situace v oblasti digitální provozní odolnosti na základě počtu hlášených závažných incidentů souvisejících s IKT a účinnosti preventivních opatření;

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

h) nastínění komunikační strategie v případě incidentů souvisejících s IKT, jejichž zveřejnění je vyžadováno v souladu s článkem 14.

9. Finanční subjekty mohou v kontextu strategie digitální provozní odolnosti uvedené v odstavci 8 definovat ucelenou strategii více dodavatelů IKT, a to na úrovni skupiny nebo subjektu, v níž budou uvedeny klíčové závislosti na poskytovatelích služeb IKT z řad třetích stran a vysvětleny důvody kombinovaného využívání poskytovatelů služeb IKT z řad třetích stran.

10. Finanční subjekty mohou v souladu s unijními a vnitrostátními odvětvovými právními předpisy externě zadat úkoly ověřování souladu s požadavky na řízení rizika v oblasti IKT podnikům uvnitř skupiny nebo externím podnikům. V případě takového externího zadání nese za ověřování souladu s požadavky na řízení rizika v oblasti IKT i nadále plnou odpovědnost finanční subjekt.

*Článek 7*

*Systémy, protokoly a nástroje IKT*

Za účelem řešení a řízení rizika v oblasti IKT finanční subjekty používají a udržují aktualizované systémy, protokoly a nástroje IKT, které jsou:

a) přiměřené rozsahu operací podporujících provádění jejich činností v souladu se zásadou proporcionality uvedenou v článku 4;

b) spolehlivé;

c) vybaveny dostatečnou kapacitou ke správnému zpracování dat potřebných k výkonu činností a včasnému poskytování služeb a k realizaci vysokých objemů objednávek, zpráv nebo transakcí podle potřeby, a to i v případě zavádění nové technologie;

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

*Článek 8*

*Identifikace*

1. Jako součást rámce pro řízení rizika v oblasti IKT uvedeného v čl. 6 odst. 1 finanční subjekty identifikují, klasifikují a náležitě zdokumentují veškeré obchodní funkce, úlohy a povinnosti podporované IKT, informační aktiva a aktiva v oblasti IKT podporující tyto funkce a jejich úlohy a závislosti ve vztahu k rizikům v oblasti IKT. Finanční subjekty podle potřeby a alespoň jednou ročně přezkoumají přiměřenost této klasifikace a veškeré příslušné dokumentace.

2. Finanční subjekty nepřetržitě identifikují všechny zdroje rizika v oblasti IKT, zejména rizika vzájemné expozice s jinými finančními subjekty, a vyhodnocují kybernetické hrozby a zranitelnosti IKT relevantní pro jejich obchodní funkce podporované IKT, informační aktiva a aktiva v oblasti IKT. Finanční subjekty pravidelně, přinejmenším však jednou ročně, revidují scénáře rizik, které jsou pro ně relevantní.

3. Finanční subjekty, jiné než mikropodniky, vyhodnocují rizika po každé velké změně v infrastruktuře sítě a informačního systému a v procesech nebo postupech ovlivňujících jejich podnikové funkce podporované IKT, informační aktiva či aktiva v oblasti IKT.

4. Finanční subjekty identifikují všechna informační aktiva a aktiva v oblasti IKT, včetně těch na vzdálených pracovištích, síťové zdroje a hardwarové vybavení a evidují ta, která jsou považovaná za kritická. Evidují konfiguraci informačních aktiv a aktiv v oblasti IKT a propojení a vzájemné závislosti různých informačních aktiv a aktiv v oblasti IKT.

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

6. Pro účely odstavců 1, 4 a 5 vedou finanční subjekty příslušné soupisy a pravidelně je aktualizují pokaždé, když dojde k jakékoli velké změně podle odstavce 3.

7. Finanční subjekty jiné než mikropodniky pravidelně, přinejmenším však jednou ročně, provádějí zvláštní posouzení rizika v oblasti IKT u všech původních systémů IKT, a to vždy před propojením a po propojení technologií, aplikací nebo systémů.

*Článek 9*

*Ochrana a prevence*

1. Pro účely odpovídající ochrany systémů IKT a s ohledem na organizaci opatření reakce finanční subjekty nepřetržitě sledují a kontrolují bezpečnost a fungování systémů a nástrojů IKT a minimalizují dopad rizika v oblasti IKT na systémy IKT prostřednictvím zavedení vhodných nástrojů, politik a postupů v oblasti bezpečnosti IKT.

2. Finanční subjekty navrhují, opatřují a uplatňují politiky, postupy, protokoly a nástroje v oblasti bezpečnosti IKT, jejichž účelem je zajistit odolnost, kontinuitu provozu a dostupnost systémů IKT, zejména těch, které podporují zásadní nebo důležité funkce, a udržet vysoké standardy dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů během jejich uchovávání, používání i přenosu.

3. K dosažení cílů uvedených v odstavci 2 využívají finanční subjekty řešení a procesy IKT, které jsou vhodné v souladu s článkem 4. Tato řešení a procesy IKT:

   a) zajišťují bezpečnost prostředků pro přenos dat;

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

c) předcházejí narušení dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů a jejich ztrátě;

d) zajišťují ochranu údajů před riziky vyplývajícími ze špatné správy údajů, včetně nekvalitní správy, rizik souvisejících se zpracováním a chyb způsobených lidským faktorem.

4. Jako součást rámce pro řízení rizika v oblasti IKT uvedeného v čl. 6 odst. 1 finanční subjekty:

a) vypracují a zdokumentují politiku zabezpečení informací vymezující pravidla na ochranu dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů, informačních aktiv a aktiv v oblasti IKT, případně včetně uvedených aktiv jejich zákazníků;

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

c) uplatňují politiky omezující fyzický nebo logický přístup k informačním aktivům a aktivům v oblasti IKT na minimum nezbytné pro výkon oprávněných a schválených funkcí a činností a za tímto účelem vytvoří soubor politik, postupů a kontrol, který se zabývá přístupovými právy, a zajistí jejich řádnou správu;

d) zavedou politiky a protokoly pro silné ověřovací mechanismy založené na příslušných normách a systémech speciálních kontrol a opatření na ochranu kryptografických klíčů, jimiž jsou zašifrována data, na základě výsledků schválené klasifikace dat a procesů posuzování rizika v oblasti IKT;

e) zavedou zdokumentované politiky, postupy a kontroly pro řízení změn IKT, včetně změn softwarových, hardwarových a firmwarových komponentů, systémů nebo parametrů 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 komplexní zdokumentované politiky pro dočasné opravy a aktualizace.

Pro účely prvního pododstavce písm. b) finanční subjekty navrhnou infrastrukturu připojení k síti umožňující jeho okamžité přerušení nebo segmentaci s cílem minimalizovat šíření krize a zabránit jejímu vzniku, zejména u vzájemně propojených finančních procesů.

Pro účely prvního pododstavce písm. e) jsou postupy řízení změn v oblasti IKT schvalovány příslušnými liniemi vedení a platí pro ně specifické protokoly.

*Článek 10*

*Detekce*

1. Finanční subjekty mají zavedeny mechanismy včasné detekce neobvyklých aktivit podle článku 17, včetně problémů s fungováním sítě IKT a incidentů souvisejících s IKT, a mechanismy identifikace potenciálních významných kritických míst.

   Všechny detekční mechanismy uvedené v prvním pododstavci se pravidelně testují v souladu s článkem 25.

2. Detekční mechanismy uvedené v odstavci 1 umožňují vícestupňovou kontrolu, stanoví prahové hodnoty a kritéria výstrah pro spuštění a zahájení postupů reakce na incidenty související s IKT, mimo jiné automatické výstražné mechanismy pro příslušné pracovníky odpovědné za reakce na incidenty související s IKT.

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

4. Poskytovatelé služeb hlášení údajů kromě toho zavedou systémy umožňující účinně kontrolovat úplnost obchodních zpráv, zjišťovat chybějící údaje a zjevné chyby a požadovat nové zaslání těchto zpráv.

*Článek 11*

*Reakce a obnova*

1. Jako součást rámce pro řízení rizika v oblasti IKT uvedeného v čl. 6 odst. 1 a na základě požadavků na identifikaci uvedených v článku 8 finanční subjekty zavedou ucelenou politiku zachování provozu IKT, která může být přijata jako specifická politika tvořící nedílnou součást celkové politiky zachování provozu finančního subjektu.

2. Finanční subjekty uplatňují politiku zachování provozu IKT prostřednictvím specializovaných, vhodných a zdokumentovaných úprav, plánů, postupů a mechanismů zaměřených na:

   a) zajištění kontinuity zásadních nebo důležitých funkcí finančního subjektu;

   b) rychlou, vhodnou a účinnou reakci na všechny incidenty související s IKT a jejich vyřešení, a to tak, aby byly omezeny škody a byla prioritně obnovena činnost a aktivována opatření na obnovu;

   c) 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 12;

d) odhad předběžných dopadů, škod a ztrát;

e) zavedení opatření v oblasti komunikace a krizového řízení, která zajistí předání aktualizovaných informací všem příslušným interním zaměstnancům a externím zainteresovaným stranám podle článku 14 a jejich oznámení příslušným orgánům v souladu s článkem 19.

3. Jako součást rámce pro řízení rizika v oblasti IKT uvedeného v čl. 6 odst. 1 finanční subjekty uplatňují související plány reakce a obnovy v oblasti IKT, které u finančních subjektů, jiných než mikropodniky, podléhají nezávislému internímu auditu.

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 celkové politiky zachování provozu provádějí finanční subjekty analýzu dopadu na činnost, pokud jde o jejich expozice vůči závažným narušením činnosti. V rámci analýzy dopadu na činnost finanční subjekty posoudí potenciální dopad závažných narušení činnosti pomocí kvantitativních a kvalitativních kritérií, případně s využitím interních a externích dat a analýzy scénářů. Analýza dopadu na činnost zohlední, jak zásadní jsou určené a zmapované obchodní funkce, podpůrné procesy, závislosti na třetích stranách a informační aktiva a jejich vzájemné závislosti. Finanční subjekty zajistí, aby aktiva v oblasti IKT a služby IKT byly navrhovány a využívány v plném souladu s analýzou dopadu na činnost, zejména s ohledem na odpovídající zajištění redundance všech zásadních složek.

6. V rámci svého komplexního řízení rizika v oblasti IKT finanční subjekty:

a) alespoň jednou ročně testují plány zachování provozu IKT a plány reakce a obnovy v oblasti IKT v souvislosti se systémy IKT podporujícími všechny funkce, jakož i v případě jakýchkoli podstatných změn systémů IKT podporujících zásadní nebo důležité funkce;

b) testují plány krizové komunikace zavedené podle článku 14.

Pro účely prvního pododstavce písm. 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 12.

Finanční subjekty pravidelně přezkoumávají svoji politiku zachování provozu IKT a plány reakce a obnovy v oblasti IKT, přičemž zohlední výsledky testů provedených v souladu s prvním pododstavcem a doporučeními vyplývajícími z auditních kontrol nebo přezkumů provedených orgány dohledu.

7. Finanční subjekty, jiné než mikropodniky, zavedou funkci řízení krizí, jež v případě aktivace jejich plánů zachování provozu IKT nebo plánů reakce a obnovy v oblasti IKT stanoví mimo jiné jednoznačné postupy pro řízení interní a externí krizové komunikace podle článku 14.

8. Finanční subjekty vedou snadno dostupné záznamy činnosti před výpadky a během výpadků po aktivaci plánů zachování provozu IKT a plánů reakce a obnovy v oblasti IKT.

9. Centrální depozitáři cenných papírů poskytnou příslušným orgánům kopie výsledků testů zachování provozu IKT nebo podobných cvičení.

10. Finanční subjekty, jiné než mikropodniky, oznamují příslušným orgánům na jejich žádost odhad souhrnných ročních nákladů a ztrát způsobených závažnými incidenty souvisejícími s IKT.

11. V souladu s článkem 16 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 vypracují evropské orgány dohledu prostřednictvím společného výboru do ... [18 měsíců ode dne vstupu tohoto nařízení v platnost] společné pokyny pro odhad souhrnných ročních nákladů a ztrát uvedených v odstavci 10.

*Článek 12*

*Politiky a postupy zálohování, postupy a metody obnovy*

1. Pro účely zajištění obnovy systémů IKT a dat s minimální odstávkou, omezenými výpadky fungování a ztrátami finanční subjekty jako součást svého rámce pro řízení rizika v oblasti IKT vypracují a zdokumentují:

   a) politiky a postupy zálohování uvádějící rozsah dat, která se zálohují, a minimální frekvenci zálohování, a to na základě významu informací nebo úrovně důvěrnosti dat;

   b) postupy a metody obnovy.

2. Finanční subjekty zřídí záložní systémy, které lze aktivovat v souladu s politikami a postupy zálohování, jakož i postupy a metodami obnovy provozu. Aktivace záložních systémů nesmí ohrozit bezpečnost sítí a informačních systémů ani dostupnost, hodnověrnost, integritu nebo důvěrnost údajů. Pravidelně se provádí testování postupů zálohování a postupů a metod obnovy.

3. Při obnově zálohových dat pomocí vlastních systémů finanční subjekty použijí systémy IKT, které jsou fyzicky a logicky odděleny od zdrojového systému IKT. Systémy IKT jsou bezpečně chráněny před jakýmkoli neoprávněným přístupem nebo poškozením IKT a podle potřeby umožňují včasnou obnovu služeb s využitím datových a systémových záloh.

V případě ústředních protistran plány obnovy umožňují obnovit všechny obchody k okamžiku přerušení, aby ústřední protistrana mohla nadále s jistotou fungovat a dokončit vypořádání ve stanovený den.

Poskytovatelé služeb hlášení údajů navíc udržují přiměřené zdroje a mají k dispozici záložní zařízení a zařízení k obnově provozu, aby mohly kdykoli nabízet a udržovat své služby.

4. Finanční subjekty, jiné než mikropodniky, udržují rezervní kapacity IKT vybavené náležitými zdroji, schopnostmi a funkcemi pro zajištění potřeb jejich činnosti. Mikropodniky posuzují potřebu zachovat tyto nadbytečné kapacity IKT na základě svého rizikového profilu.

5. Centrální depozitáři cenných papírů provozují alespoň jedno sekundární místo zpracování vybavené náležitými zdroji, schopnostmi, funkcemi a personálem pro zajištění potřeb jejich činnosti.

   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 nebo důležitých funkcí stejně jako primární místo, nebo poskytovat úroveň služeb nezbytnou k zajištění provádění zásadních operací finančního subjektu v rámci cílů pro obnovu;

   c) je ihned přístupné pro pracovníky 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 provádějí nezbytné kontroly, včetně veškerých násobných kontrol a sesouhlasení dat s cílem zajistit nejvyšší možnou úroveň integrity dat. Tyto kontroly se provádějí rovněž při obnově dat od externích zainteresovaných stran, aby byla zajištěna konzistentnost všech dat v obou systémech.

*Článek 13*

*Poučení a rozvoj*

1. Finanční subjekty disponují prostředky a pracovníky, aby mohly shromažďovat informace o zranitelnostech 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 incidentech souvisejících s IKT poté, co závažný incident související s IKT naruší jejich hlavní činnosti, přičemž analyzují příčiny narušení a určí potřebná zlepšení operací IKT nebo v rámci politiky zachování provozu IKT uvedené v článku 11.

Finanční subjekty, jiné než mikropodniky, na žádost sdělí příslušným orgánům změny, které byly provedeny v návaznosti na přezkumy incidentů souvisejících s IKT uvedené v prvním pododstavci.

Přezkumy po incidentech souvisejících s IKT podle prvního pododstavce stanoví, zda byly dodrženy zavedené postupy a zda byla přijatá opatření účinná, a to i ve vztahu k:

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

b) kvalitě a rychlosti provádění forenzní analýzy, je-li to považováno za vhodné;

c) efektivitě eskalace incidentů v rámci finančního subjektu;

d) efektivitě interní a externí komunikace.

3. Poučení vyvozená z testování digitální provozní odolnosti provedeného v souladu s články 26 a 27 a ze skutečných incidentů souvisejících s IKT, zejména kybernetických útoků, a dále z problémů v souvislosti s aktivací plánů zachování provozu IKT a plánů reakce a obnovy v oblasti IKT a relevantních informací vyměňovaných s protistranami a vyhodnocovaných během přezkumů orgány dohledu se náležitě a průběžně začleňují do postupu posuzování rizika v oblasti IKT. Tato zjištění tvoří základ pro odpovídající přezkumy příslušných složek rámce pro řízení rizik v oblasti IKT uvedeného v čl. 6 odst. 1.

4. Finanční subjekty sledují účinnost uplatňování své strategie digitální provozní odolnosti podle čl. 6 odst. 8. Evidují vývoj rizika v oblasti IKT v čase, analyzují četnost, druhy, rozsah a vývoj incidentů souvisejících s IKT, zejména kybernetických útoků a jejich vzorců, aby bylo možné pochopit míru expozice vůči riziku v oblasti IKT, zejména ve vztahu k zásadním nebo důležitým funkcím, 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 zaměstnanců programy zvyšování povědomí o bezpečnosti v oblasti IKT a školení o digitální provozní odolnosti. Tyto programy a školení se vztahují na všechny zaměstnance a na vedoucí pracovníky a musí mít úroveň složitosti úměrnou výkonu jejich funkcí. Finanční subjekty případně zahrnou do svých příslušných školicích programů rovněž poskytovatele služeb IKT z řad třetích stran v souladu s čl. 30 odst. 2 písm. i).

7. Finanční subjekty, jiné než mikropodniky, průběžně sledují relevantní technologický vývoj, mimo jiné s cílem pochopit možný dopad zavádění nových technologií na požadavky na bezpečnost IKT a digitální provozní odolnost. Drží krok s nejnovějšími postupy řízení rizika v oblasti IKT, aby účinně bojovaly se stávajícími či novými formami kybernetických útoků.

*Článek 14*

*Komunikace*

1. Jako součást rámce pro řízení rizika v oblasti IKT uvedeného v čl. 6 odst. 1 finanční subjekty zavedou krizové komunikační plány umožňující odpovědné informování klientů, protistran a případně veřejnosti alespoň o závažných incidentech souvisejících s IKT nebo zranitelnostech.

2. Jako součást rámce pro řízení rizika v oblasti IKT finanční subjekty uplatňují komunikační strategie pro interní zaměstnance a externí zainteresované strany. Komunikační politiky pro zaměstnance zohledňují nutnost rozlišovat mezi pracovníky podílejícími se na řízení rizika v oblasti IKT, zejména pracovníky odpovědnými za reakci a obnovu, a pracovníky, které je nutné informovat.

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

*Článek 15*

*Další harmonizace nástrojů, metod, postupů a politik řízení rizika v oblasti IKT*

Evropské orgány dohledu prostřednictvím společného výboru a za konzultace s Agenturou Evropské unie pro kybernetickou bezpečnost (ENISA) vypracují společné návrhy regulačních technických norem s cílem:

a) dále upřesnit prvky, které mají být začleněny do strategií, politik, postupů, protokolů a nástrojů zabezpečení IKT uvedených v čl. 9 odst. 2 v zájmu zajištění bezpečnosti sítí, zavedení vhodných ochranných opatření proti vniknutí a zneužití údajů, zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů, včetně kryptografických technik, a zaručení přesného a rychlého přenosu dat bez vážných narušení a zbytečných prodlev;

b) dále rozvinout složky kontrol správy přístupových práv uvedených v čl. 9 odst. 4 písm. c) a související politiku v oblasti lidských zdrojů stanovící přístupová práva, postupy udělování a odebírání těchto práv, sledování neobvyklého chování v souvislosti s rizikem v oblasti IKT pomocí vhodných ukazatelů, včetně ukazatelů vzorců, doby, aktivit IT a neznámých zařízení při používání sítě;

c) dále rozvinout mechanismy uvedené v čl. 10 odst. 1 umožňující rychle detekovat neobvyklé aktivity a kritéria uvedená v čl. 10 odst. 2 pro spuštění procesů detekce a reakce v případě incidentů souvisejících s IKT;

d) dále upřesnit složky politiky zachování provozu IKT uvedené v čl. 11 odst. 1;

e) dále upřesnit testování plánů zachování provozu IKT podle čl. 11 odst. 6, aby se zajistilo, že toto testování řádně zohledňuje scénáře, za nichž se kvalita poskytování zásadních nebo důležitých funkcí zhoršuje na nepřijatelnou úroveň nebo toto poskytování selhává, a potenciální dopad platební neschopnosti či jiných selhání jakéhokoli poskytovatele služeb IKT z řad třetích stran a v příslušných případech politická rizika v jurisdikcích příslušných poskytovatelů;

f) dále upřesnit složky plánů reakce a obnovy v oblasti IKT uvedených v čl. 11 odst. 3;

g) dále upřesnit obsah a formát zprávy o přezkumu rámce pro řízení rizika v oblasti IKT podle čl. 6 odst. 5.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu zohlední velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací, přičemž náležitě zohlední veškeré specifické rysy vyplývající z odlišné povahy činností v různých odvětvích finančních služeb.

Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [12 měsíců ode dne vstupu tohoto nařízení 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. 1094/2010 a (EU) č. 1095/2010.

*Článek 16*

*Zjednodušený rámec pro řízení rizika v oblasti IKT*

1. Články 5 až 15 tohoto nařízení se nepoužijí na malé a nepropojené investiční podniky, platební instituce vyňaté podle směrnice (EU) 2015/2366, instituce vyňaté podle směrnice 2013/36/EU, u nichž se členské státy rozhodly neuplatnit možnost uvedenou v čl. 2 odst. 4 tohoto nařízení, instituce elektronických peněz vyňaté podle směrnice 2009/110/ES a malé instituce zaměstnaneckého penzijního pojištění.

Aniž je dotčen první pododstavec, subjekty uvedené v prvním pododstavci:

a) zavedou a udržují spolehlivý a zdokumentovaný rámec pro řízení rizika v oblasti IKT, který podrobně popisuje mechanismy a opatření zaměřené na rychlé, účinné a komplexní řízení rizika v oblasti IKT, včetně ochrany příslušných fyzických součástí a infrastruktur;

b) průběžně sledují bezpečnost a fungování všech systémů IKT;

c) minimalizují dopad rizika v oblasti IKT používáním spolehlivých, odolných a aktualizovaných systémů, protokolů a nástrojů IKT, které jsou vhodné pro podporu výkonu jejich činností a poskytování služeb a které odpovídajícím způsobem chrání dostupnost, hodnověrnost, integritu a důvěrnost údajů v síti a informačních systémech;

d) umožní rychlou identifikaci a detekci zdrojů rizik a anomálií v síti a informačních systémech a urychlené řešení incidentů souvisejících s IKT;

e) určí klíčové závislosti na poskytovatelích služeb IKT z řad třetích stran;

f) zajistí zachování provozu zásadních nebo důležitých funkcí prostřednictvím plánů zachování provozu a opatření v oblasti reakce a obnovy, které zahrnují alespoň opatření týkající se zálohování a obnovy;

g) pravidelně testují plány a opatření uvedené v písmenu f), jakož i účinnost kontrol prováděných v souladu s písmeny a) a c);

h) podle potřeby provedou příslušné provozní závěry vyplývající z testů uvedených v písmenu g) a z analýzy po incidentu do postupu posuzování rizik v oblasti IKT a v souladu s potřebami a rizikovým profilem v oblasti IKT vypracují pro zaměstnance a vedení programy zvyšování povědomí o bezpečnosti v oblasti IKT a školení týkající se digitální provozní odolnosti.

2. Rámec pro řízení rizika v oblasti IKT uvedený v odst. 1 druhém pododstavci písm. a) je zdokumentován a přezkoumáván pravidelně a při výskytu závažných incidentů souvisejících s IKT v souladu s pokyny pro dohled. Je průběžně zdokonalován na základě zkušeností z jeho provádění a sledování. Zpráva o přezkumu rámce pro řízení rizika v oblasti IKT se na žádost poskytne příslušnému orgánu.

3. Evropské orgány dohledu prostřednictvím společného výboru a za konzultace s ENISA vypracují společné návrhy regulačních technických norem s cílem:

a) dále upřesnit prvky, které mají být zahrnuty do rámce pro řízení rizika v oblasti IKT uvedeného v odst. 1 druhém pododstavci písm. a);

b) dále upřesnit prvky týkající se systémů, protokolů a nástrojů k minimalizaci dopadu rizika v oblasti IKT uvedeného v odst. 1 druhém pododstavci písm. c) v zájmu zajištění bezpečnosti sítí, zavedení vhodných ochranných opatření proti vniknutí a zneužití dat a zachování dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů;

c) dále upřesnit prvky plánů zachování provozu IKT uvedené v odst. 1 druhém pododstavci písm. f);

d) dále upřesnit pravidla týkající se testování plánů zachování provozu a zajistit účinnost kontrol uvedených v odst. 1 druhém pododstavci písm. g) a zabezpečit, aby toto testování řádně zohlednilo scénáře, v nichž se kvalita poskytování zásadní nebo důležité funkce zhorší na nepřijatelnou úroveň nebo selže;

e) dále upřesnit obsah a formát zprávy o přezkumu rámce pro řízení rizika v oblasti IKT podle odstavce 2.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu zohlední velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací.

Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [12 měsíců ode dne vstupu tohoto nařízení 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. 1094/2010 a (EU) č. 1095/2010.

# Kapitola III

# Řízení, klasifikace a hlášení incidentů souvisejících s IKT

*Článek 17*

*Proces řízení incidentů souvisejících s IKT*

1. Finanční subjekty vymezí, zavedou a uplatňují proces řízení incidentů souvisejících s IKT za účelem detekce, řízení a hlášení incidentů souvisejících s IKT.

2. Finanční subjekty zaznamenávají veškeré incidenty související s IKT a závažné kybernetické hrozby. 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, zdokumentování a řešení jejich hlavních příčin, a zabránilo se tak výskytu těchto incidentů.

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

a) zavede ukazatele včasného varování;

b) stanoví postupy k identifikaci, sledování, evidenci, kategorizaci a klasifikaci incidentů souvisejících s IKT podle jejich priority a závažnosti a podle toho, jak zásadní jsou zasažené služby v souladu s kritérii vymezenými v čl. 18 odst. 1;

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

d) stanoví plány komunikace pro zaměstnance, externí zainteresované strany a média podle článku 14 a pro informování klientů, postupy interní eskalace, včetně stížností klientů souvisejících s IKT, a případně rovněž pro poskytování informací finančním subjektům jednajícím jako protistrany;

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

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

*Článek 18*

*Klasifikace incidentů souvisejících s IKT a kybernetických hrozeb*

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

   a) počet nebo význam dotčených klientů nebo finančních protistran a případně výše nebo počet transakcí dotčených incidentem souvisejícím s IKT, a zda incident související s IKT poškodil dobrou pověst;

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

   c) územní rozsah, pokud jde o oblasti dotčené incidentem souvisejícím s IKT, zejména má-li incident dopad na více než dva členské státy;

   d) ztráty údajů, které incident související s IKT způsobil, pokud jde o dostupnost, hodnověrnost, integritu nebo důvěrnost údajů;

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

   f) ekonomický dopad incidentu souvisejícího s IKT, zejména přímé a nepřímé náklady a ztráty, v absolutním i relativním vyjádření.

2. Finanční subjekty klasifikují kybernetické hrozby jako závažné na základě toho, jak zásadní jsou ohrožené služby, včetně transakcí a operací finančních subjektů, jaký je počet nebo význam klientů nebo finančních protistran a územní rozsah ohrožených oblastí.

3. Evropské orgány dohledu prostřednictvím společného výboru a za konzultace s ECB a ENISA vypracují společné návrhy regulačních technických norem, v nichž jsou dále upřesněna:

   a) kritéria stanovená v odstavci 1, včetně prahových hodnot významnosti pro stanovení závažných incidentů souvisejících s IKT, nebo případně závažných provozních či bezpečnostních incidentů souvisejících s platbami, na něž se vztahuje povinnost hlášení podle čl. 19 odst. 1;

   b) kritéria, která příslušné orgány použijí pro účely posouzení relevantnosti závažných incidentů souvisejících s IKT, nebo případně závažných provozních či bezpečnostních incidentů souvisejících s platbami, pro příslušné orgány v jiných členských státech, a údaje v hlášeních závažných incidentů souvisejících s IKT, nebo případně závažných provozních či bezpečnostních incidentů souvisejících s platbami, které budou sdíleny s dalšími příslušnými orgány podle čl. 19 odst. 6 a 7;

   c) kritéria stanovená v odstavci 2 tohoto článku, včetně vysokých prahových hodnot významnosti pro určování závažných kybernetických hrozeb.

4. Evropské orgány dohledu při vypracování společných návrhů regulačních technických norem podle odstavce 3 tohoto článku přihlédnou ke kritériím vymezeným v čl. 4 odst. 2, jakož i k mezinárodním normám, pokynům a specifikacím vypracovaným a zveřejněným ENISA, včetně případných specifikací pro jiná hospodářská odvětví. Pro účely uplatňování kritérií stanovených v čl. 4 odst. 2 evropské orgány dohledu řádně zváží, zda je třeba, aby mikropodniky a malé a střední podniky mobilizovaly dostatečné zdroje a schopnosti k zajištění rychlého řešení incidentů souvisejících s IKT.

Evropské orgány dohledu předloží tyto společné návrhy regulačních technických norem Komisi do ... [12 měsíců ode dne vstupu tohoto nařízení v platnost].

Na Komisi je přenesena pravomoc doplnit toto nařízení přijetím regulačních technických norem uvedených v odstavci 3 v souladu s články 10 až 14 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

*Článek 19*

*Hlášení závažných incidentů souvisejících s IKT*
*a dobrovolné oznamování významných kybernetických hrozeb*

1. Finanční subjekty hlásí závažné incidenty související s IKT relevantním příslušným orgánům uvedeným v článku 46 v souladu s odstavcem 4 tohoto článku.

Pokud finanční subjekt podléhá dohledu více než jednoho vnitrostátního příslušného orgánu uvedeného v článku 46, určí členské státy jediný příslušný orgán jako relevantní příslušný orgán odpovědný za výkon funkcí a povinností stanovených v tomto článku.

Úvěrové instituce klasifikované v souladu s čl. 6 odst. 4 nařízení (EU) č. 1024/2013 jako významné hlásí závažné incidenty související s IKT relevantnímu vnitrostátnímu příslušnému orgánu určenému v souladu s článkem 4 směrnice 2013/36/EU, který danou zprávu neprodleně předává ECB.

Pro účely prvního pododstavce finanční subjekty vypracují pomocí vzorů uvedených v článku 20 na základě shromáždění a analýzy všech relevantních informací prvotní oznámení a zprávy uvedené v odstavci 4 tohoto článku a předloží je příslušnému orgánu. V případě, že z technických důvodů není možné předložit prvotní oznámení za použití uvedeného vzoru, předají finanční subjekty oznámení příslušnému orgánu alternativními prostředky.

Prvotní oznámení a zprávy uvedené v odstavci 4 obsahují veškeré informace nezbytné k tomu, aby příslušný orgán stanovil významnost závažného incidentu souvisejícího s IKT a posoudil možné přeshraniční dopady.

Aniž je dotčeno hlášení finančního subjektu relevantnímu příslušnému orgánu podle prvního pododstavce, členské státy mohou dále určit, že některé nebo všechny finanční subjekty podají prvotní oznámení a všechny zprávy uvedené v odstavci 4 tohoto článku za použití vzorů uvedených v článku 20 příslušným orgánům nebo týmům pro reakce na počítačové bezpečnostní incidenty (dále jen „týmy CSIRT“) určeným nebo zřízeným v souladu se směrnicí (EU) .../...[+].

2. Finanční subjekty mohou relevantnímu příslušnému orgánu dobrovolně oznamovat významné kybernetické hrozby, pokud se domnívají, že hrozba je relevantní pro finanční systém, uživatele služeb nebo klienty. Relevantní příslušný orgán může tyto informace poskytnout jiným relevantním orgánům uvedeným v odstavci 6.

Úvěrové instituce klasifikované v souladu s čl. 6 odst. 4 nařízení (EU) č. 1024/2013 jako významné mohou dobrovolně oznamovat významné kybernetické hrozby relevantnímu vnitrostátnímu příslušnému orgánu určenému v souladu s článkem 4 směrnice 2013/36/EU, který dané oznámení neprodleně předává ECB.

Členské státy mohou stanovit, že finanční subjekty mohou dobrovolné oznámení podle prvního pododstavce rovněž předat týmům CSIRT určeným nebo zřízeným v souladu se směrnicí (EU).../...[+].

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

3. Dojde-li k závažnému incidentu souvisejícímu s IKT a má-li tento incident dopad na finanční zájmy klientů, finanční subjekty bez zbytečného prodlení, jakmile se o incidentu dozvědí, informují své klienty o tomto závažném incidentu souvisejícím s IKT a o veškerých opatřeních přijatých ke zmírnění nepříznivých dopadů tohoto incidentu.

V případě významné kybernetické hrozby informují finanční subjekty případně své klienty, kteří by mohli být hrozbou dotčeni, o vhodných ochranných opatřeních, která mohou tito klienti případně přijmout.

4. Finanční subjekty ve lhůtách stanovených v souladu s čl. 20 prvním pododstavcem písm. a) bodem 2 předloží relevantnímu příslušnému orgánu:

a) prvotní oznámení;

b) průběžnou zprávu po prvotním oznámení uvedeném v písmeni a), jakmile se stav původního incidentu významným způsobem změní nebo jakmile se na základě nových dostupných informací změní řešení závažného incidentu souvisejícího s IKT, po níž případně následují aktualizovaná oznámení pokaždé, když je k dispozici příslušná aktualizace stavu, jakož i na zvláštní žádost 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.

5. Finanční subjekty mohou v souladu s unijními a vnitrostátními odvětvovými právními předpisy externě zadat zajištění povinného hlášení podle tohoto článku poskytovateli služeb z řad třetích stran. V případě takového externího zadání nese za plnění požadavku hlášení incidentů i nadále plnou odpovědnost finanční subjekt.

6. Po obdržení prvotního oznámení a každé zprávy podle odstavce 4 poskytne příslušný orgán včas podrobnosti o závažném incidentu souvisejícím s IKT těmto příjemcům, a to na základě jejich příslušných pravomocí:

a) EBA, ESMA či EIOPA;

b) ECB v případě finančních subjektů uvedených v čl. 2 odst. 1 písm. a), b) a d);

c) příslušným orgánům, jednotným kontaktním místům nebo týmům CSIRT určeným nebo zřízeným v souladu se směrnicí (EU) …/…[+];

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

d) orgánům příslušným k řešení krize uvedeným v článku 3 směrnice 2014/59/EU a Jednotnému výboru pro řešení krizí, pokud jde o subjekty uvedené v čl. 7 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 806/2014[1] a subjekty a skupiny uvedené v čl. 7 odst. 4 písm. b) a odst. 5 nařízení (EU) č. 806/2014, pokud se tyto podrobnosti týkají incidentů, které představují riziko pro zajištění zásadních funkcí ve smyslu čl. 2 odst. 1 bodu 35 směrnice 2014/59/EU, a

e) jiným relevantním veřejným orgánům podle vnitrostátního práva.

7. Po obdržení informací v souladu s odstavcem 6 EBA, ESMA nebo EIOPA a ECB za konzultace s ENISA a ve spolupráci s relevantním příslušným orgánem posoudí, zda je závažný incident související s IKT relevantní pro příslušné orgány v jiných členských státech. Na základě tohoto posouzení EBA, ESMA nebo EIOPA co nejdříve zašle odpovídající oznámení relevantním příslušným orgánům v jiných členských státech. ECB informuje o veškerých záležitostech relevantních 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.

---

[1] 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).

8. Oznámením, které má učinit ESMA podle odstavce 7 tohoto článku, není dotčena odpovědnost příslušného orgánu za urychlené předání podrobností o závažném incidentu souvisejícím s IKT relevantnímu orgánu v hostitelském členském státě, pokud centrální depozitář cenných papírů vykonává v hostitelském členském státě významnou přeshraniční činnost, daný závažný incident související s IKT bude mít pravděpodobně závažné důsledky pro finanční trhy hostitelského členského státu a pokud existují ujednání o spolupráci mezi příslušnými orgány týkající se dohledu nad finančními subjekty.

*Článek 20*

*Harmonizace obsahu a vzorů hlášení*

Evropské orgány dohledu prostřednictvím společného výboru a za konzultace s ENISA a ECB vypracují:

a) společné návrhy regulačních technických norem za účelem:

   i) stanovení obsahu hlášení závažných incidentů souvisejících s IKT s cílem zohlednit kritéria stanovená v čl. 18 odst. 1 a zahrnout další prvky, jako jsou podrobnosti pro stanovení relevantnosti hlášení pro ostatní členské státy a zda se jedná o závažný provozní nebo bezpečnostní incident související s platbami, či nikoli;

ii) stanovení lhůt pro prvotní oznámení a pro každou zprávu podle čl. 19 odst. 4;

iii) vymezení obsahu oznámení o významných kybernetických hrozbách.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu zohlední velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací, a to zejména s cílem zajistit, aby pro účely tohoto pododstavce písm. a) bodu ii) mohly různé lhůty případně odrážet specifika finančních sektorů, aniž je dotčeno zachování jednotného přístupu k hlášení incidentů souvisejících s IKT podle tohoto nařízení a podle směrnice (EU) .../...[+]. Evropské orgány dohledu případně poskytnou odůvodnění, pokud se odchylují od přístupů přijatých v souvislosti s uvedenou směrnicí;

b) společné návrhy prováděcích technických norem s cílem vytvořit standardní formuláře, vzory a postupy, které finanční subjekty použijí k hlášení závažného incidentu souvisejícího s IKT a k oznámení významné kybernetické hrozby.

Evropské orgány dohledu předloží společné návrhy regulačních technických norem uvedené v prvním pododstavci písm. a) a společné návrhy prováděcích technických norem uvedené v prvním pododstavci písm. b) Komisi do ... [18 měsíců ode dne vstupu tohoto nařízení v platnost].

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

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

Komisi je svěřena pravomoc přijímat společné prováděcí technické normy uvedené v prvním pododstavci písm. b) v souladu s článkem 15 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

*Článek 21*

*Centralizace hlášení závažných incidentů souvisejících s IKT*

1. Evropské orgány dohledu prostřednictvím společného výboru a za konzultace 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. Ve společné zprávě se analyzují možnosti usnadnění toku hlášení incidentů souvisejících s IKT, snížení nákladů a podpory tematických analýz s cílem zlepšení sbližování dohledu.

2. Společná zpráva uvedená v odstavci 1 obsahuje alespoň tyto prvky:

   a) předpoklady pro vytvoření jednotného centra EU;

b) přínosy, omezení a rizika, včetně rizik spojených s vysokou koncentrací citlivých informací;

c) nezbytné schopnosti pro zajištění interoperability s ohledem na jiné relevantní systémy podávání zpráv;

d) prvky provozního řízení;

e) podmínky členství;

f) technická úprava přístupu finančních subjektů a vnitrostátních příslušných orgánů k jednotnému centru EU;

g) předběžné posouzení finančních nákladů, které s sebou ponese vytvoření provozní platformy podporující jednotné centrum EU, včetně nezbytných odborných znalostí.

3. Evropské orgány dohledu předloží zprávu uvedenou v odstavci 1 Komisi, Evropskému parlamentu a Radě do ... [24 měsíců ode dne vstupu tohoto nařízení v platnost].

*Článek 22*

*Zpětná vazba orgánu dohledu*

1. Aniž jsou dotčeny technické vstupy, poradenství nebo náprava a následná navazující činnost, které mohou v souladu s vnitrostátním právem případně poskytnout týmy CSIRT podle směrnice (EU) …/…[+], příslušný orgán po obdržení prvotního oznámení a každé zprávy podle čl. 19 odst. 4 potvrdí jejich přijetí a může, je-li to možné, finančnímu subjektu zavčas poskytnout náležitou a přiměřenou zpětnou vazbu nebo obecné pokyny, zejména poskytnutím veškerých relevantních anonymizovaných informací a operativních informací o podobných hrozbách, a může projednat nápravu uplatněnou na úrovni daného finančního subjektu a možnosti, jak minimalizovat a zmírnit nepříznivý dopad na finanční sektor. Aniž je dotčena zpětná vazba orgánů dohledu, finanční subjekty jsou i nadále plně odpovědné za řešení incidentů souvisejících s IKT hlášených podle čl. 19 odst. 1 a za jejich důsledky.

2. Evropské orgány dohledu každoročně anonymizovaně a souhrnně informují prostřednictvím společného výboru o závažných incidentech souvisejících s IKT, o nichž obdržely podrobné informace od příslušných orgánů v souladu s čl. 19 odst. 6, přičemž uvedou alespoň počet závažných incidentů souvisejících s IKT, jejich povahu a dopad na provoz finančních subjektů nebo klientů, přijatá nápravná opatření a vzniklé náklady.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

Evropské orgány dohledu vydávají varování a statistiky na vysoké úrovni na podporu posuzování hrozeb a zranitelností v oblasti IKT.

*Článek 23*

*Provozní nebo bezpečnostní incidenty související s platbami týkající se úvěrových institucí, platebních institucí, poskytovatelů služeb informování o účtu a institucí elektronických peněz*

Požadavky stanovené v této kapitole se v případech, kdy se týkají úvěrových institucí, platebních institucí, poskytovatelů služeb informování o účtu a institucí elektronických peněz, vztahují rovněž na provozní nebo bezpečnostní incidenty související s platbami a na závažné provozní nebo bezpečnostní incidenty související s platbami.

# Kapitola IV
# Testování digitální provozní odolnosti

*Článek 24*

*Obecné požadavky na provádění testování digitální provozní odolnosti*

1. Pro účely posuzování připravenosti na řešení incidentů souvisejících s IKT, identifikace slabých míst, vad a nedostatků v digitální provozní odolnosti a rychlého zavedení nápravných opatření finanční subjekty jiné než mikropodniky při zohlednění kritérií vymezených v čl. 4 odst. 2 vytvoří, udržují a aktualizují spolehlivý a ucelený program testování digitální provozní odolnosti jakožto nedílnou součást rámce pro řízení rizika v oblasti IKT uvedeného v článku 6.

2. Tento program testování digitální provozní odolnosti obsahuje celou řadu hodnocení, testů, metodik, postupů a nástrojů, které se použijí v souladu s články 25 a 26.

3. Při provádění programu testování digitální provozní odolnosti uvedeného v odstavci 1 tohoto článku finanční subjekty, jiné než mikropodniky, uplatňují přístup založený na posouzení rizik, přičemž zohlední kritéria vymezená v čl. 4 odst. 2 tím, že řádně zohlední vývoj rizika v oblasti IKT, jakákoli specifická rizika, jimž je či jimž by mohl být vystaven dotyčný finanční subjekt, význam informačních aktiv a poskytovaných služeb a rovněž jakékoli jiné faktory, které finanční subjekt považuje za vhodné.

4. Finanční subjekty, jiné než mikropodniky, 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, jiné než mikropodniky, vytvoří postupy a politiky pro stanovení priorit, klasifikaci a nápravu všech problémů zjištěných při provádění testů a vytvoří interní metodiky ověřování, jejichž prostřednictvím kontrolují, zda všechny zjištěné slabiny, nedostatky či vady byly plně odstraněny.

6. Finanční subjekty, jiné než mikropodniky, zajistí, aby byly alespoň jednou ročně provedeny vhodné testy všech systémů a aplikací IKT podporujících zásadní nebo důležité funkce.

*Článek 25*

*Testování nástrojů a systémů IKT*

1. Program testování digitální provozní odolnosti uvedený v článku 24 stanoví v souladu s kritérii vymezenými v čl. 4 odst. 2 provedení vhodných testů, jako jsou hodnocení a zjišťování zranitelnosti, analýzy otevřených zdrojů, posouzení bezpečnosti sítě, analýzy nedostatků, přezkumy fyzické bezpečnosti, dotazníky a antivirová softwarová řešení, v případě proveditelnosti přezkumy zdrojových kódů, testy založené na scénářích, testování kompatibility, testování výkonu, testování mezi koncovými body a penetrační testování.

2. Centrální depozitáři cenných papírů a ústřední protistrany provádějí hodnocení zranitelnosti před každým použitím či opakovaným použitím nových nebo stávajících aplikací nebo prvků infrastruktury a služeb IKT podporujících zásadní nebo důležité funkce finančního subjektu.

3. Mikropodniky provádějí testy uvedené v odstavci 1 tak, že kombinují přístup založený na posouzení rizik se strategickým plánováním testování IKT, přičemž náležitě zváží potřebu zachovat vyvážený přístup mezi rozsahem zdrojů a dobou, kterou je třeba věnovat testování IKT podle tohoto článku, na jedné straně a naléhavostí, druhem rizika, tím, jak zásadní jsou informační aktiva a poskytované služby, jakož i veškerými dalšími relevantními faktory, včetně schopnosti finančního subjektu podstupovat zvážená rizika na straně druhé.

*Článek 26*

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

1. Finanční subjekty, jiné než subjekty uvedené v čl. 16 odst. 1 prvním pododstavci a jiné než mikropodniky, které jsou určeny v souladu s odst. 8 třetím pododstavcem tohoto článku, provádějí alespoň jednou za tři roky pokročilé testování s využitím penetračního testování na základě hrozeb. Na základě rizikového profilu finančního subjektu a s přihlédnutím k provozním okolnostem může příslušný orgán v případě potřeby požádat finanční subjekt, aby tuto četnost snížil nebo zvýšil.

2. Každý penetrační test na základě hrozeb pokrývá některé nebo všechny zásadní nebo důležité funkce finančního subjektu a provádí se za provozu na systémech skutečně využívaných k zajištění těchto funkcí.

   Finanční subjekty identifikují všechny relevantní základní systémy, procesy a technologie IKT podporující zásadní nebo důležité funkce a služby IKT, včetně těch, které podporují zásadní nebo důležité funkce a jsou dodávané externě či nasmlouvané s poskytovateli služeb IKT z řad třetích stran.

   Finanční subjekty posoudí, které zásadní nebo důležité funkce je třeba zahrnout do penetračního testování na základě hrozeb. Výsledek tohoto posouzení určí přesný rozsah penetračního testování na základě hrozeb a musí být potvrzen příslušnými orgány.

3. Pokud jsou do rozsahu penetračního testování na základě hrozeb zahrnuti poskytovatelé služeb IKT z řad třetích stran, přijme finanční subjekt nezbytná opatření a záruky k zajištění účasti těchto poskytovatelů služeb IKT z řad třetích stran na penetračním testování na základě hrozeb a po celou dobu si ponechá plnou odpovědnost za zajištění souladu s tímto nařízením.

4. Aniž je dotčen odst. 2 první a druhý pododstavec, pokud lze důvodně očekávat, že účast poskytovatelů služeb IKT z řad třetích stran na penetračním testování na základě hrozeb, jak je uvedena v odstavci 3, bude mít nepříznivý dopad na kvalitu nebo bezpečnost služeb, které poskytovatel služeb IKT z řad třetích stran poskytuje zákazníkům, kteří jsou subjekty mimo oblast působnosti tohoto nařízení, nebo na důvěrnost údajů souvisejících s takovými službami, finanční subjekt a poskytovatel služeb IKT z řad třetích stran se mohou písemně dohodnout, že poskytovatel služeb IKT z řad třetích stran uzavře smluvní ujednání přímo s externím subjektem provádějícím testování, aby bylo pod vedením jednoho vybraného finančního subjektu provedeno společné penetrační testování na základě hrozeb zahrnující několik finančních subjektů (dále jen „společné testování“), pro něž poskytovatel služeb IKT z řad třetích stran poskytuje služby IKT.

   Toto společné testování se vztahuje na příslušný rozsah služeb IKT, které podporují zásadní nebo důležité funkce a jsou zadány příslušnému poskytovateli služeb IKT z řad třetích stran finančními subjekty. Společné testování se považuje za penetrační testování na základě hrozeb, které provádějí finanční subjekty účastnící se společného testování.

Počet finančních subjektů účastnících se společného testování musí být náležitě kalibrován s ohledem na složitost a druhy dotčených služeb.

5. Finanční subjekty ve spolupráci s poskytovateli služeb IKT z řad třetích stran a dalšími zúčastněnými stranami, včetně subjektů provádějících testování, avšak s výjimkou příslušných orgánů, použijí účinné kontroly v rámci řízení rizik, aby zmírnily rizika jakéhokoliv případného dopadu na data, poškození aktiv a narušení zásadních nebo důležitých funkcí, služeb nebo operací u vlastního finančního subjektu, jeho protistran nebo celého finančního sektoru.

6. Na konci testování a po schválení zpráv a plánů nápravných opatření finanční subjekt a v příslušných případech externí subjekt provádějící testování předloží orgánu určenému v souladu s odstavcem 9 nebo 10 souhrn příslušných zjištění, plánů nápravných opatření a dokumentaci prokazující, že penetrační testování na základě hrozeb bylo provedeno v souladu s požadavky.

7. Orgány vydají finančním subjektům osvědčení o provedeném testu v souladu s požadavky, což doloží dokumentací, aby mohly příslušné orgány tyto penetrační testy na základě hrozeb vzájemně uznávat. Finanční subjekt o osvědčení, souhrnu příslušných zjištění a plánech nápravných opatření informuje relevantní příslušný orgán.

   Aniž je dotčeno toto osvědčení, finanční subjekty jsou vždy plně odpovědné za dopady testů uvedených v odstavci 4.

8. Finanční subjekty najímají subjekty provádějící testování pro účely provádění penetračního testování na základě hrozeb v souladu s článkem 27. Pokud finanční subjekty používají pro účely provádění penetračního testování na základě hrozeb interní subjekty, musí provedení vždy jednoho ze tří testů zadat externímu subjektu provádějícímu testování.

Úvěrové instituce, které jsou klasifikovány jako významné v souladu s čl. 6 odst. 4 nařízení (EU) č. 1024/2013, používají pouze externí subjekty provádějící testování v souladu s čl. 27 odst. 1 písm. a) až e).

Příslušné orgány určí finanční subjekty, které jsou povinny provádět penetrační testování na základě hrozeb, s přihlédnutím ke kritériím stanoveným v čl. 4 odst. 2, a to na základě posouzení:

a) faktorů souvisejících s dopady, zejména toho, jak rozsáhlý je dopad služeb, které finanční subjekt poskytuje, a činností, které provádí, na finanční sektor;

b) případných hledisek finanční stability, včetně systémové povahy finančního subjektu na unijní nebo případně vnitrostátní úrovni;

c) konkrétního rizikového profilu v oblasti IKT, úrovně vyspělosti finančního subjektu v oblasti IKT nebo dotčených technologických prvků.

9. Členské státy mohou určit jediný veřejný orgán ve finančním sektoru, který bude na vnitrostátní úrovni odpovědný za záležitosti související s penetračním testováním na základě hrozeb ve finančním sektoru, a svěří mu za tímto účelem veškeré pravomoci a úkoly.

10. Není-li určen veřejný orgán podle odstavce 9 tohoto článku, a aniž je dotčena pravomoc určit finanční subjekty, které mají provádět penetrační testování na základě hrozeb, může příslušný orgán pověřit výkonem některých nebo všech úkolů uvedených v tomto článku a v článku 27 jiný vnitrostátní orgán ve finančním sektoru.

11. Evropské orgány dohledu po dohodě s ECB vypracují v souladu s rámcem TIBER–EU společné návrhy regulačních technických norem, který dále upřesní:

a) kritéria, která se použijí pro účely uplatňování odst. 8 druhého pododstavce;

b) požadavky a normy, kterými se řídí využívání interních subjektů provádějících testování;

c) požadavky týkající se:

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

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

iii) výsledků a fáze ukončení testování a nápravy;

d) druh spolupráce v oblasti dohledu a jinou relevantní spolupráci, která je zapotřebí k provádění penetračního testování na základě hrozeb a pro usnadnění vzájemného uznávání těchto testů, pokud jde o finanční subjekty působící ve více než jednom členském státě, aby byla umožněna náležitá úroveň zapojení orgánů dohledu a flexibilní uplatňování, které zohlední specifičnosti finančních pododvětví nebo místních finančních trhů.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu náležitě zohlední veškeré specifické aspekty vyplývající z odlišné povahy činností v různých odvětvích finančních služeb.

Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [18 měsíců ode dne vstupu tohoto nařízení 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. 1094/2010 a (EU) č. 1095/2010.

*Článek 27*

*Požadavky na subjekty provádějící penetrační testování na základě hrozeb*

1. Finanční subjekty využijí k penetračnímu testování na základě hrozeb pouze subjekty provádějící testování, které:

   a) jsou nejvhodnější a mají nejlepší pověst;

   b) disponují technickými a organizačními schopnostmi a prokáží specifické znalosti v oblasti operativních informací o hrozbách, penetračního testování a testování metodou „červeného týmu“;

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

   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 kryty příslušným pojištěním odpovědnosti za škody při výkonu povolání, včetně rizik pochybení a nedbalosti.

2. Finanční subjekty využívající interní subjekty provádějící testování zajistí, aby kromě požadavků uvedených v odstavci 1 byly splněny i tyto podmínky:

a) toto využití bylo schváleno relevantním příslušným orgánem nebo jediným veřejným orgánem určeným v souladu s čl. 26 odst. 9 a 10;

b) relevantní příslušný orgán ověřil, že daný finanční subjekt vyčlenil dostatečné zdroje a zajistil, aby během fáze návrhu a provádění testu nedocházelo ke střetům zájmů, a

c) poskytovatel operativních informací o hrozbách je externí subjekt, který není součástí daného finančního subjektu.

3. Finanční subjekty zajistí, aby ve smlouvách uzavřených s externími subjekty provádějícími testování byla požadována řádná správa výsledků penetračního testování na základě hrozeb a aby jakékoli související zpracování údajů, včetně jakéhokoli vypracování, uložení, agregace, návrhu, hlášení, sdělení nebo zničení neohrozilo finanční subjekt.

# Kapitola V
# Řízení rizika v oblasti IKT spojeného s třetími stranami

## ODDÍL I
## HLAVNÍ ZÁSADY SPRÁVNÉHO ŘÍZENÍ RIZIKA V OBLASTI IKT SPOJENÉHO S TŘETÍMI STRANAMI

*Článek 28*

*Obecné zásady*

1. Finanční subjekty řídí riziko v oblasti IKT spojené s třetími stranami jako nedílnou součást rizika v oblasti IKT ve svém rámci pro řízení rizika v oblasti IKT uvedeném v čl. 6 odst. 1 podle těchto zásad:

   a) 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 platného práva v oblasti finančních služeb;

b) řízení rizika v oblasti IKT spojeného s třetími stranami provádějí finanční subjekty s ohledem na zásadu proporcionality a na:

i) povahu, rozsah, složitost a význam závislostí v oblasti IKT,

ii) rizika vyplývající ze smluvních ujednání o využívání služeb IKT uzavřených s poskytovateli služeb IKT z řad třetích stran se zohledněním toho, jak zásadní či důležité jsou příslušné služby, procesy nebo funkce a jaký je potenciální dopad na kontinuitu a dostupnost finančních služeb a činností na individuální úrovni i na úrovni skupiny.

2. Jakožto součást svého rámce pro řízení rizika v oblasti IKT finanční subjekty, jiné než subjekty uvedené v čl. 16 odst. 1 prvním pododstavci a jiné než mikropodniky, přijmou a pravidelně přezkoumávají strategii pro riziko v oblasti IKT spojené s třetími stranami, přičemž případně zohlední strategii více dodavatelů uvedenou v čl. 6 odst. 9. Strategie pro riziko v oblasti IKT spojené s třetími stranami obsahuje zásady využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran a uplatňuje se na individuálním a případně subkonsolidovaném či konsolidovaném základě. Vedoucí orgán na základě posouzení celkového rizikového profilu finančního subjektu a rozsahu a složitosti obchodních služeb pravidelně přezkoumává rizika identifikovaná v souvislosti se smluvními ujednáními o využívání služeb IKT podporujících zásadní nebo důležité funkce.

3. Jakožto součást svého rámce pro řízení rizika v oblasti IKT finanční subjekty na úrovni subjektu a na subkonsolidované a konsolidované úrovni vedou a aktualizují registr informací s ohledem na všechna smluvní ujednání o využívání služeb IKT poskytovaných poskytovateli služeb IKT z řad třetích stran.

Smluvní ujednání uvedená v prvním pododstavci se řádně zdokumentují, přičemž se rozlišuje mezi těmi, která se týkají služeb IKT podporujících zásadní nebo důležité funkce a těmi, která se jich netýkají.

Finanční subjekty alespoň jednou ročně nahlásí příslušným orgánům počet nových ujednání o využívání služeb IKT, kategorie poskytovatelů služeb IKT z řad třetích stran, druh smluvních ujednání a poskytované služby a funkce IKT.

Finanční subjekt zpřístupní příslušnému orgánu na jeho žádost 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 jakémkoli plánovaném smluvním ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce, jakož i v případě, že se některá funkce stane zásadní nebo důležitou.

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

a) posoudí, zda se smluvní ujednání týká využívání služeb IKT podporujících 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 toto smluvní ujednání může přispívat k zesílení rizika koncentrace IKT uvedeného v článku 29;

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.

5. Finanční subjekty smí uzavírat smluvní ujednání pouze s poskytovateli služeb IKT z řad třetích stran, kteří splňují příslušné normy v oblasti bezpečnosti informací. Pokud se tato smluvní ujednání týkají zásadních nebo důležitých funkcí, finanční subjekty před uzavřením ujednání náležitě zváží, zda poskytovatelé služeb IKT z řad třetích stran uplatňují nejaktuálnější a nejkvalitnější normy bezpečnosti informací.

6. Finanční subjekty při výkonu práv na přístup, kontrolu a audit u poskytovatele služeb IKT z řad třetích stran předem na základě přístupu založeného na posouzení rizik stanoví četnost auditů a kontrol, jakož i 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.

   Pokud se smluvní ujednání uzavřená s poskytovateli služeb IKT z řad třetích stran o využívání služeb IKT týkají technicky velmi složitých otázek, finanční subjekt ověří, že interní nebo externí auditoři nebo skupina auditorů disponují odpovídajícími dovednostmi a znalostmi pro účinné provedení příslušných auditů a posouzení.

7. Finanční subjekty zajistí, aby smluvní ujednání o využívání služeb IKT bylo možné ukončit za kterékoli z těchto okolností:

a) poskytovatel služeb IKT z řad třetích stran zásadním způsobem poruší platné právní předpisy nebo smluvní podmínky;

b) sledováním rizika v oblasti IKT spojeného 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) v rámci celkového řízení rizika v oblasti IKT poskytovatele služeb IKT z řad třetích stran jsou zjištěna slabá místa, a to zejména s ohledem na zajištění dostupnosti, hodnověrnosti, integrity a důvěrnosti údajů, ať již osobních či jiných citlivých údajů, nebo jiných než osobních údajů;

d) příslušný orgán již nedokáže dále efektivně dohlížet na finanční subjekt v důsledku podmínek příslušného smluvního ujednání nebo okolností s ním souvisejících.

8. U služeb IKT podporujících zásadní nebo důležité funkce zavedou finanční subjekty strategie ukončení smluvního vztahu. Strategie ukončení smluvního vztahu zohlední rizika, jež mohou vzniknout na úrovni poskytovatelů služeb IKT z řad třetích stran, zejména jejich případné selhání, snížení kvality poskytovaných služeb a funkcí IKT, jakékoli narušení činnosti v důsledku nevhodného či chybného poskytování služeb IKT nebo jakéhokoli vážného rizika vznikajícího v souvislosti s řádným a nepřetržitým poskytováním příslušné služby IKT, nebo v případě ukončení smluvních ujednání s poskytovateli služeb IKT z řad třetích stran za kterékoli z okolností uvedených v odstavci 7.

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 splňovat kritéria vymezená v čl. 4 odst. 2, musí být dostatečně otestovány a pravidelně přezkoumávány.

Finanční subjekty identifikují alternativní řešení a vypracují plány přechodu, které jim umožní odebrání nasmlouvaných služeb IKT a příslušných dat od poskytovatele služeb IKT z řad třetích stran a jejich bezpečný a integrovaný přenos k alternativnímu poskytovateli, nebo jejich začlenění v rámci vlastní organizace.

Finanční subjekty mají zavedena vhodná opatření pro nepředvídané události, aby byl zachován provoz, pokud by nastaly okolnosti uvedené v prvním pododstavci.

9. Evropské orgány dohledu vypracují prostřednictvím společného výboru návrhy prováděcích technických norem, které stanoví standardní vzory pro účely registru informací uvedeného v odstavci 3, včetně informací společných všem smluvním ujednáním o využívání služeb IKT. Evropské orgány dohledu předloží tyto návrhy prováděcích technických norem Komisi do ... [12 měsíců ode dne vstupu tohoto nařízení v platnost].

Komisi je svěřena pravomoc přijímat prováděcí technické normy uvedené v prvním pododstavci v souladu s článkem 15 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

10. Evropské orgány dohledu vypracují prostřednictvím společného výboru návrhy regulačních technických norem, které dále upřesní podrobný obsah politiky uvedené v odstavci 2 ve vztahu ke smluvním ujednáním o využívání služeb IKT podporujících zásadní nebo důležité funkce, poskytovaných poskytovateli služeb IKT z řad třetích stran.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu zohlední velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací. Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [12 měsíců ode dne vstupu tohoto nařízení 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. 1094/2010 a (EU) č. 1095/2010.

*Článek 29*

*Předběžné posouzení rizika koncentrace IKT na úrovni subjektu*

1. Finanční subjekty při identifikaci a posuzování rizik uvedených v čl. 28 odst. 4 písm. c) rovněž zohlední, zda by plánované uzavření smluvního ujednání souvisejícího se službami IKT podporujícími zásadní nebo důležité funkce způsobilo jakoukoli z těchto situací:

   a) uzavření smlouvy s poskytovatelem služeb IKT z řad třetích stran, kterou není snadné nahradit; nebo

   b) uzavření více smluvních ujednání týkajících se poskytování služeb IKT podporujících zásadní nebo důležité funkce se stejným poskytovatelem služeb IKT z řad třetích stran nebo s úzce propojenými poskytovateli služeb IKT z řad třetích stran.

   Finanční subjekty zváží přínosy a náklady alternativních řešení, například využití jiných poskytovatelů služeb IKT z řad třetích stran, 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 zásadní nebo důležité funkce možnost, aby poskytovatel služeb IKT z řad třetích stran zajišťoval služby IKT podporující zásadní nebo důležitou funkci prostřednictvím subdodávek od jiných poskytovatelů služeb IKT z řad třetích stran, finanční subjekty zváží výhody a rizika, jež mohou vzniknout v souvislosti s tímto využitím subdodavatele IKT, zejména je-li tento subdodavatel IKT usazen ve třetí zemi.

Týkají-li se smluvní ujednání služeb IKT podporujících zásadní nebo důležité funkce, finanční subjekty řádně zváží ustanovení insolvenčního práva, která se uplatní v případě úpadku poskytovatele služeb IKT z řad třetích stran, jakož i veškerá omezení, jež mohou vzniknout při naléhavé obnově dat finančního subjektu.

Pokud jsou smluvní ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce uzavřena s poskytovatelem služeb IKT z řad třetích stran usazeným ve třetí zemi, zváží finanční subjekty kromě aspektů uvedených v druhém pododstavci rovněž dodržování pravidel Unie pro ochranu údajů a účinné vymáhání práva v dané třetí zemi.

Pokud smluvní ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce stanoví subdodávky, finanční subjekty posoudí, zda a jak mohou potenciální dlouhé nebo složité subdodavatelské řetězce ovlivnit jejich schopnost plně sledovat nasmlouvané funkce a schopnost příslušných orgánů provádět v tomto ohledu účinný dohled nad finančním subjektem.

*Článek 30*

*Hlavní smluvní ustanovení*

1. Práva a povinnosti finančního subjektu a poskytovatele služeb IKT z řad třetích stran jsou jasně rozděleny a stanoveny písemně. Úplná smlouva zahrnuje dohody o úrovni služeb a je vyhotovena v jednom písemném dokumentu, který musí být dostupný stranám v papírové podobě, nebo v podobě dokumentu v jiném formátu, který lze stáhnout, je trvalý a přístupný.

2. Smluvní ujednání o využívání služeb IKT obsahují přinejmenším tyto prvky:

   a) srozumitelný a úplný popis všech funkcí a služeb IKT dodávaných poskytovatelem služeb IKT z řad třetích stran s uvedením, zda je povoleno zajišťování služeb IKT podporujících 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 mají být nasmlouvané nebo subdodavatelem zajišťované funkce a služby IKT poskytovány a kde mají být zpracovávána data, včetně místa jejich uchovávání, a povinnost poskytovatele služeb IKT z řad třetích stran oznámit finančnímu subjektu předem, plánuje-li změnu těchto míst;

c) ustanovení týkající se dostupnosti, hodnověrnosti, integrity a důvěrnosti, pokud jde o ochranu údajů, včetně osobních údajů;

d) 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 poskytovatele služeb IKT z řad třetích stran nebo v případě ukončení smluvních ujednání;

e) popis úrovně služeb, včetně aktualizací a revizí;

f) povinnost poskytovatele služeb IKT z řad třetích stran poskytnout finančnímu subjektu pomoc bez dodatečných nákladů nebo za náklady, které jsou stanoveny ex ante, dojde-li k incidentu v oblasti IKT, který souvisí se službou IKT poskytovanou finančnímu subjektu;

g) povinnost poskytovatele služeb IKT z řad třetích stran plně spolupracovat s příslušnými orgány a s orgány příslušnými k řešení krize finančního subjektu, včetně osob jimi jmenovaných;

h) práva na ukončení smlouvy a související minimální výpovědní lhůty pro ukončení smluvních ujednání v souladu s očekáváními příslušných orgánů a orgánů příslušných k řešení krize;

i) podmínky pro účast poskytovatele služeb IKT z řad třetích stran na programech zvyšování povědomí o bezpečnosti v oblasti IKT a školeních o digitální provozní odolnosti finančních subjektů v souladu s čl. 13 odst. 6.

3. Smluvní ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce zahrnují kromě prvků uvedených v odstavci 2 alespoň:

a) úplný popis úrovně služeb, včetně jejich aktualizací a revizí, a přesné kvalitativní i kvantitativní výkonnostní cíle v rámci sjednaných úrovní služeb umožňující účinné sledování služeb IKT finančním subjektem a neprodlené přijetí vhodných kroků k nápravě, nejsou-li sjednané úrovně služeb splněny;

b) výpovědní lhůty a povinnosti hlášení poskytovatele služeb IKT z řad třetích stran finančnímu subjektu, včetně oznámení jakéhokoli vývoje, který by mohl mít významný dopad na schopnost poskytovatele služeb IKT z řad třetích stran účinně poskytovat služby IKT podporující zásadní nebo důležité funkce v souladu se sjednanými úrovněmi služeb;

c) povinnosti poskytovatele služeb IKT z řad třetích stran uplatňovat a testovat plány zachování provozu a mít bezpečnostní opatření, nástroje a politiky v oblasti IKT, jež zajistí odpovídající úroveň bezpečnosti poskytování služeb finančním subjektem v souladu s jeho regulačním rámcem;

d) povinnost poskytovatele služeb IKT z řad třetích stran účastnit se penetračního testování na základě hrozeb finančního subjektu a plně na něm spolupracovat, jak je uvedeno v článcích 26 a 27;

e) právo nepřetržitě sledovat výsledky poskytovatele služeb IKT z řad třetích stran, které zahrnuje:

   i) neomezené právo na přístup, kontrolu a audit vykonávané finančním subjektem nebo určenou třetí stranou a příslušným orgánem a právo pořizovat kopie příslušné dokumentace na místě, pokud jsou zásadní z hlediska provozu poskytovatele služeb IKT z řad třetích stran, přičemž účinný výkon těchto práv nesmí být znemožňován či omezován jinými smluvními ujednáními nebo prováděcími politikami;

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

iii) povinnost poskytovatele služeb IKT z řad třetích stran plně spolupracovat při kontrolách na místě a auditech prováděných příslušnými orgány, hlavním orgánem dohledu, finančním subjektem nebo určenou třetí stranou, a

iv) povinnost poskytnout podrobnosti o rozsahu, postupech, které je třeba uplatňovat, a četnosti těchto kontrol a auditů;

f) strategie ukončení smluvního vztahu, zejména stanovení povinného přiměřeného přechodného období:

i) během kterého bude poskytovatel služeb IKT z řad třetích stran za účelem snížení rizika výpadku u finančního subjektu nebo zajištění účinného řešení a restrukturalizace nadále poskytovat příslušné funkce nebo služby IKT;

ii) umožňujícího finančnímu subjektu přejít k jinému poskytovateli služeb IKT z řad třetích stran, nebo přistoupit k vlastnímu řešení odpovídajícímu složitosti poskytované služby.

Odchylně od písmene e) se poskytovatel služeb IKT z řad třetích stran a finanční subjekt, který je mikropodnikem, mohou dohodnout, že práva finančního subjektu na přístup, kontrolu a audit mohou být přenesena na nezávislou třetí stranu určenou poskytovatelem služeb IKT z řad třetích stran a že finanční subjekt může od této třetí strany kdykoli požadovat informace a ujištění o výkonu poskytovatele služeb IKT z řad třetích stran.

4. Finanční subjekty a poskytovatelé služeb IKT z řad třetích stran při vyjednávání o smluvních ujednáních zváží použití standardních smluvních doložek vypracovaných veřejnými orgány pro konkrétní služby.

5. Evropské orgány dohledu vypracují prostřednictvím společného výboru návrhy regulačních technických norem k dalšímu upřesnění prvků uvedených v odst. 2 písm. a), které musí finanční subjekt určit a posoudit při subdodávkách služeb IKT podporujících zásadní nebo důležité funkce.

Při vypracovávání těchto návrhů regulačních technických norem evropské orgány dohledu zohlední velikost a celkový rizikový profil finančního subjektu a povahu, rozsah a složitost jeho služeb, činností a operací.

Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [18 měsíců ode dne vstupu tohoto nařízení 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. 1094/2010 a (EU) č. 1095/2010.

## ODDÍL II

## RÁMEC DOHLEDU NAD KRITICKÝMI POSKYTOVATELI SLUŽEB IKT Z ŘAD TŘETÍCH STRAN

*Článek 31*

*Určení kritických poskytovatelů služeb IKT z řad třetích stran*

1. Evropské orgány dohledu prostřednictvím společného výboru a na základě doporučení fóra dohledu zřízeného podle čl. 32 odst. 1:

   a) určí poskytovatele služeb IKT z řad třetích stran, kteří jsou kritičtí pro finanční subjekty, a to na základě posouzení, v jehož rámci zohlední kritéria podle odstavce 2;

b) jmenují hlavním orgánem dohledu pro jednotlivé kritické poskytovatele služeb IKT z řad třetích stran evropský orgán dohledu, který je v souladu s nařízeními (EU) č. 1093/2010, (EU) č. 1094/2010 nebo (EU) č. 1095/2010 odpovědný za finanční subjekty, jež mají dohromady největší podíl celkových aktiv z hodnoty celkových aktiv všech finančních subjektů, které využívají služeb příslušného kritického poskytovatele služeb IKT z řad třetích stran, jak je doloženo souhrnem jednotlivých účetních závěrek daných finančních subjektů.

2. Určení uvedené v odst. 1 písm. a) vychází ze všech následujících kritérií ve vztahu ke službám IKT poskytovaným poskytovatelem služeb IKT z řad třetích stran:

a) systémový dopad na stabilitu, kontinuitu nebo kvalitu poskytování finančních služeb v případě, že bude příslušný poskytovatel služeb IKT z řad třetích stran čelit rozsáhlému provoznímu výpadku poskytování svých služeb, přičemž se zohlední počet finančních subjektů a celková hodnota aktiv finančních subjektů, kterým příslušný poskytovatel služeb IKT z řad třetích stran poskytuje své služby;

b) systémová povaha či význam finančních subjektů, které spoléhají na příslušného poskytovatele služeb IKT z řad třetích stran, na základě posouzení podle následujících parametrů:

i) počet globálních systémově významných institucí (G-SVI) nebo jiných systémově významných institucí (J-SVI), které spoléhají na daného poskytovatele služeb IKT z řad třetích stran;

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

c) spoléhání finančních subjektů na služby dodávané příslušným poskytovatelem služeb IKT z řad třetích stran v souvislosti se zásadními nebo důležitými funkcemi finančních subjektů, které v konečném důsledku zahrnují zapojení stejného poskytovatele služeb IKT z řad třetích stran bez ohledu na to, zda finanční subjekty využívají tyto služby přímo či nepřímo prostřednictvím subdodavatelských ujednání;

d) míra nahraditelnosti poskytovatele služeb IKT z řad třetích stran s přihlédnutím k těmto parametrům:

i) nedostatek, i částečný, reálných alternativ vzhledem k omezenému počtu poskytovatelů služeb IKT z řad třetích stran aktivně působících na konkrétním trhu, podíl příslušného poskytovatele služeb IKT z řad třetích stran na trhu nebo technická složitost či sofistikovanost služeb, též v souvislosti s jakoukoli chráněnou technologií, nebo specifické vlastnosti organizace či činnosti poskytovatele služeb IKT z řad třetích stran;

ii) potíže související s částečnou či úplnou migrací relevantních dat a pracovních úkolů při přechodu od příslušného poskytovatele služeb IKT z řad třetích stran k jinému poskytovateli služeb IKT z řad třetích stran buď kvůli vysokým finančním nákladům, času nebo jiným zdrojům, jež může proces migrace vyžadovat, nebo kvůli zvýšenému riziku v oblasti IKT či jiným operačním rizikům, jimž může být finanční subjekt během této migrace vystaven.

3. Je-li poskytovatel služeb IKT z řad třetích stran součástí skupiny, kritéria uvedená v odstavci 2 se uplatňují na služby IKT poskytované danou skupinou jako celkem.

4. Kritičtí poskytovatelé služeb IKT z řad třetích stran, kteří jsou součástí skupiny, určí jednu právnickou osobu jako koordinátora, aby bylo zajištěno odpovídající zastoupení a komunikace s hlavním orgánem dohledu.

5. Hlavní orgán dohledu oznámí poskytovateli služeb IKT z řad třetích stran výsledek posouzení vedoucího k určení podle odst. 1 písm. a). Do šesti týdnů ode dne oznámení může poskytovatel služeb IKT z řad třetích stran předložit hlavnímu orgánu dohledu odůvodněné prohlášení s veškerými relevantními informacemi pro účely posouzení. Hlavní orgán dohledu odůvodněné prohlášení zváží a může požádat o předložení doplňujících informací do 30 kalendářních dnů od jeho obdržení.

Poté, co byl některý poskytovatel služeb IKT z řad třetích stran určen jako kritický, evropské orgány dohledu prostřednictvím společného výboru oznámí tuto skutečnost a počáteční datum, od kterého se na něj budou vztahovat činnosti v oblasti dohledu, tomuto poskytovateli. Toto počáteční datum nastane do jednoho měsíce po oznámení. O tom, že byl určen jako kritický, informuje daný poskytovatel služeb IKT z řad třetích stran finanční subjekty, kterým poskytuje služby.

6. Komisi je svěřena pravomoc přijmout do ... [18 měsíců ode dne vstupu tohoto nařízení v platnost] akt v přenesené pravomoci v souladu s článkem 57, kterým toto nařízení doplní dalším upřesněním kritérií uvedených v odstavci 2 tohoto článku.

7. Určování podle odst. 1 písm. a) se neuskuteční, dokud Komise nepřijme akt v přenesené pravomoci podle odstavce 6.

8. Určování podle odst. 1 písm. a) se nevztahuje na:

   i) finanční subjekty poskytující služby IKT jiným finančním subjektům;

   ii) poskytovatele služeb IKT z řad třetích stran, kteří podléhají rámci dohledu stanovenému pro účely podpory úkolů uvedených v čl. 127 odst. 2 Smlouvy o fungování EU;

   iii) poskytovatele služeb IKT v rámci skupiny;

iv) poskytovatele služeb IKT z řad třetích stran, kteří poskytují služby IKT pouze v jednom členském státě finančním subjektům, jež působí pouze v daném členském státě.

9. Evropské orgány dohledu prostřednictvím společného výboru vypracují, zveřejní a každoročně aktualizují seznam kritických poskytovatelů služeb IKT z řad třetích stran na úrovni Unie.

10. Příslušné orgány pro účely odst. 1 písm. a) každoročně a na agregovaném základě zašlou zprávy podle čl. 28 odst. 3 třetího pododstavce fóru dohledu vytvořenému v souladu s článkem 32. Fórum dohledu posoudí na základě informací obdržených od příslušných orgánů závislost finančních subjektů na třetích stranách poskytujících služby IKT.

11. Poskytovatelé služeb IKT z řad třetích stran, kteří nejsou uvedeni na seznamu podle odstavce 9, mohou požádat o to, aby byli určeni jakožto kritičtí podle odst. 1 písm. a).

Poskytovatel služeb IKT z řad třetích stran pro účely prvního pododstavce předloží odůvodněnou žádost EBA, ESMA nebo EIOPA, které prostřednictvím společného výboru rozhodnou, zda tohoto poskytovatele služeb IKT z řad třetích stran určí jakožto kritického podle odst. 1 písm. a).

Rozhodnutí uvedené ve druhém pododstavci se přijme a oznámí dotčenému poskytovateli služeb IKT z řad třetích stran do šesti měsíců od obdržení žádosti.

12. Finanční subjekty mohou využívat služby poskytovatele služeb IKT z řad třetích stran usazeného ve třetí zemi, který byl určen za kritického podle odst. 1 písm. a), pouze pokud tento poskytovatel založí dceřiný podnik v Unii do 12 měsíců od daného určení.

13. Kritický poskytovatel služeb IKT z řad třetích stran uvedený v odstavci 12 oznámí hlavnímu orgánu dohledu jakékoli změny ve struktuře vedení svého dceřiného podniku založeného v Unii.

*Článek 32*

*Struktura rámce dohledu*

1. Společný výbor v souladu s čl. 57 odst. 1 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 vytvoří fórum dohledu jako podvýbor pro účely podpory pracovních úkolů společného výboru a hlavního orgánu dohledu podle čl. 31 odst. 1 písm. b), co se týče rizika v oblasti IKT spojeného s třetími stranami ve všech finančních odvětvích. Fórum dohledu připravuje návrhy společných stanovisek a společných aktů společného výboru v této oblasti.

   Fórum dohledu pravidelně jedná o relevantním vývoji v oblasti rizika a zranitelností v oblasti IKT a podporuje soudržný přístup ke sledování rizika v oblasti IKT spojeného s třetími stranami na úrovni Unie.

2. Fórum dohledu provede každý rok společné posouzení výsledků a zjištění dohledových činností prováděných pro všechny kritické poskytovatele služeb IKT z řad třetích stran 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 rizika mezi odvětvími.

3. Fórum dohledu předloží komplexní referenční hodnoty pro kritické poskytovatele služeb IKT z řad třetích stran, které společný výbor schválí jako společná stanoviska evropských orgánů dohledu v souladu s čl. 56 prvním pododstavcem nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010.

4. Fórum dohledu tvoří:

   a) předsedové evropských orgánů dohledu;

   b) jeden zástupce na vysoké úrovni z řad stávajících zaměstnanců relevantního příslušného orgánu uvedeného v článku 46 z každého členského státu;

   c) výkonní ředitelé jednotlivých evropských orgánů dohledu a po jednom zástupci z Komise, ESRB, ECB a ENISA jako pozorovatelé;

   d) případně jeden další zástupce příslušného orgánu uvedeného v článku 46 z každého členského státu jako pozorovatel;

e) případně jakožto pozorovatel jeden zástupce příslušných orgánů určených nebo zřízených v souladu se směrnicí (EU) …/…[+], které jsou odpovědné za dohled nad zásadním nebo důležitým subjektem podléhajícím uvedené směrnici, který byl určen jako kritický poskytovatel služeb IKT z řad třetích stran.

Fórum dohledu může ve vhodných případech požádat o radu nezávislé odborníky jmenované v souladu s odstavcem 6.

5. Každý členský stát určí relevantní příslušný orgán, z řad jehož zaměstnanců je určen zástupce na vysoké úrovni podle odst. 4 prvního pododstavce písm. b), a informuje o tom hlavní orgán dohledu.

Evropské orgány dohledu zveřejní na svých internetových stránkách seznam zástupců na vysoké úrovni z řad stávajících zaměstnanců relevantních příslušných orgánů určených členskými státy.

6. Nezávislé odborníky uvedené v odst. 4 druhém pododstavci jmenuje fórum dohledu ze skupiny odborníků vybraných na základě veřejného a transparentního postupu výběru uchazečů.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

Tito nezávislí odborníci jsou jmenováni na základě svých odborných znalostí v oblasti finanční stability, digitální provozní odolnosti a otázek bezpečnosti IKT. Jednají nezávisle a objektivně ve výlučném zájmu Unie jako celku a nevyžadují ani nepřijímají pokyny od orgánů či institucí Unie, od vlád členských států ani od jiných veřejných či soukromých subjektů.

7. V souladu s článkem 16 nařízení (EU) č. 1093/2010, (EU) č. 1094/2010 a (EU) č. 1095/2010 evropské orgány dohledu do ... [18 měsíců ode dne vstupu tohoto nařízení v platnost] vydají pro účely tohoto oddílu pokyny pro spolupráci mezi evropskými orgány dohledu a příslušnými orgány týkající se podrobných postupů a podmínek pro rozdělování a výkon úkolů mezi příslušnými orgány a evropskými orgány dohledu a podrobností o výměně informací, jež příslušné orgány potřebují k zajištění dodržování doporučení podle čl. 35 odst. 1 písm. d) určených kritickým poskytovatelům služeb IKT z řad třetích stran.

8. Požadavky stanovenými v tomto oddíle není dotčeno uplatňování směrnice (EU) .../...[+] ani dalších předpisů Unie týkajících se dohledu nad poskytovateli cloudových služeb.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

9. Evropské orgány dohledu prostřednictvím společného výboru a na základě přípravných prací realizovaných fórem dohledu každoročně předkládají Evropskému parlamentu, Radě a Komisi zprávu o uplatňování tohoto oddílu.

*Článek 33*

*Úkoly hlavního orgánu dohledu*

1. Hlavní orgán dohledu jmenovaný v souladu s čl. 31 odst. 1 písm. b) vykonává dohled nad přidělenými kritickými poskytovateli služeb IKT z řad třetích stran a je pro účely všech záležitostí souvisejících s dohledem hlavním kontaktním místem pro tyto kritické poskytovatele služeb IKT z řad třetích stran.

2. Pro účely odstavce 1 hlavní orgán dohledu posoudí, zda jednotliví kritičtí poskytovatelé služeb IKT z řad třetích stran zavedli komplexní, jasná a účinná pravidla, postupy, mechanismy a ujednání pro řízení rizika v oblasti IKT, které mohou představovat pro finanční subjekty.

   Posouzení uvedené v prvním pododstavci se zaměří především na služby IKT poskytované kritickým poskytovatelem služeb IKT z řad třetích stran, které podporují zásadní nebo důležité funkce finančních subjektů. Je-li to nezbytné pro řešení všech relevantních rizik, toto posouzení se rozšíří na služby IKT podporující jiné než zásadní nebo důležité funkce.

3. Posouzení uvedené v odstavci 2 se vztahuje na:

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, jakož i schopnost nepřetržitě dodržovat vysoké standardy pro dostupnost, hodnověrnost, integritu a důvěrnost, údajů;

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

c) procesy řízení rizika, včetně politik pro řízení rizika v oblasti IKT, politiky zachování provozu IKT a plánů reakce a obnovy v oblasti IKT;

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

e) identifikaci, sledování a rychlé hlášení významných 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 služeb IKT daného kritického poskytovatele služeb IKT z řad třetích stran finančním subjektům.

4. Na základě posouzení uvedeného v odstavci 2 a v koordinaci se společnou sítí dohledu uvedenou v čl. 34 odst. 1 přijme hlavní orgán dohledu jasný, podrobný a odůvodněný individuální plán dohledu popisující roční cíle v oblasti dohledu a hlavní opatření v oblasti dohledu plánovaná pro každého kritického poskytovatele služeb IKT z řad třetích stran. Tento plán je každoročně předkládán kritickému poskytovateli služeb IKT z řad třetích stran.

Před přijetím plánu dohledu hlavní orgán dohledu předloží jeho návrh kritickému poskytovateli služeb IKT z řad třetích stran.

Po obdržení návrhu plánu dohledu může kritický poskytovatel služeb IKT z řad třetích stran do 15 kalendářních dnů předložit odůvodněné prohlášení dokládající očekávaný dopad na zákazníky, kteří jsou subjekty mimo oblast působnosti tohoto nařízení, a případně formulovat řešení ke zmírnění rizik.

5. Po přijetí ročních plánů dohledu uvedených v odstavci 4 a jejich oznámení kritickým poskytovatelům služeb IKT z řad třetích stran mohou příslušné orgány přijímat opatření týkající se takových kritických poskytovatelů služeb IKT z řad třetích stran pouze po dohodě s hlavním orgánem dohledu.

*Článek 34*

*Operativní koordinace mezi hlavními orgány dohledu*

1. Za účelem zajištění jednotného přístupu k dohledovým činnostem a umožnění koordinovaných obecných strategií dohledu a soudržných operativních přístupů a metodik práce tři hlavní orgány dohledu jmenované v souladu s čl. 31 odst. 1 písm. b) zřídí společnou síť dohledu, aby mohly mezi sebou koordinovat činnost v přípravných fázích a koordinovat provádění dohledu nad svými příslušnými kritickými poskytovateli služeb IKT z řad třetích stran, jakož i během jakýchkoli kroků, které může být nutno učinit podle článku 42.

2. Pro účely odstavce 1 vypracují hlavní orgány dohledu společný protokol o dohledu, který stanoví podrobné postupy pro provádění každodenní koordinace a pro zajištění rychlých výměn a reakcí. Protokol je pravidelně revidován tak, aby odrážel operativní potřeby, zejména vývoj praktických opatření v oblasti dohledu.

3. Hlavní orgány dohledu mohou příležitostně vyzvat ECB a ENISA, aby poskytly technické poradenství, sdílely praktické zkušenosti nebo se účastnily zvláštních koordinačních zasedání společné sítě dohledu.

*Článek 35*

*Pravomoci hlavního orgánu dohledu*

1. Pro účely plnění povinností stanovených v tomto oddíle má hlavní orgán dohledu tyto pravomoci, pokud jde o kritické poskytovatele služeb IKT z řad třetích stran:

   a) požádat o veškeré relevantní informace a dokumentaci podle článku 37;

   b) provádět obecná šetření podle článku 38 a kontroly podle článku 39;

   c) po dokončení činností dohledu požadovat zprávy, v nichž je uvedeno, jaké kroky či jakou nápravu učinili kritičtí poskytovatelé služeb IKT z řad třetích stran v souvislosti s doporučeními uvedenými v písmenu d) tohoto odstavce;

d) vydávat doporučení v oblastech uvedených v čl. 33 odst. 3, zejména pokud jde o:

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

ii) použití smluvních podmínek, včetně jejich technického provádění, za nichž kritičtí poskytovatelé služeb IKT z řad třetích stran poskytují tyto služby finančním subjektům a které hlavní orgán dohledu považuje za relevantní pro prevenci vzniku kritických míst, jejich rozšíření nebo pro minimalizaci možného systémového dopadu na celý finanční sektor Unie v případě rizika koncentrace IKT;

iii) veškeré plánované subdodávky, pokud se hlavní orgán dohledu domnívá, že další subdodávky, včetně subdodavatelských ujednání, která kritičtí poskytovatelé služeb IKT z řad třetích stran hodlají uzavřít s poskytovateli služeb IKT z řad třetích stran nebo se subdodavateli IKT usazenými ve třetí zemi, mohou představovat rizika pro poskytování služeb finančním subjektem nebo ohrozit finanční stabilitu, a to na základě posouzení informací shromážděných v souladu s články 37 a 38;

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

– plánovaný subdodavatel je poskytovatelem služeb IKT z řad třetích stran nebo subdodavatelem IKT usazeným ve třetí zemi;

– subdodávky se týkají zásadní nebo důležité funkce finančního subjektu, a

– hlavní orgán dohledu se domnívá, že využívání takových subdodávek představuje jasné a závažné riziko pro finanční stabilitu Unie nebo pro finanční subjekty, včetně schopnosti finančních subjektů plnit požadavky v oblasti dohledu.

Pro účely bodu iv) tohoto písmene předají poskytovatelé služeb IKT z řad třetích stran hlavnímu orgánu dohledu informace týkající se subdodávek a použijí k tomu šablonu uvedenou v čl. 41 odst. 1 písm. b).

2. Při výkonu pravomocí uvedených v tomto článku hlavní orgán dohledu:

a) zajišťuje pravidelnou koordinaci v rámci společné sítě dohledu, a zejména v příslušných případech usiluje o jednotné přístupy, pokud jde o dohled nad kritickými poskytovateli služeb IKT z řad třetích stran;

b) náležitě zohlední rámec stanovený směrnicí (EU) .../...[+] a v případě potřeby konzultuje s relevantními příslušnými orgány určenými nebo zřízenými v souladu s uvedenou směrnicí, aby se zabránilo zdvojování technických a organizačních opatření, která by se mohla podle uvedené směrnice vztahovat na kritické poskytovatele služeb IKT z řad třetích stran;

c) usiluje o co největší minimalizaci rizika narušení služeb poskytovaných kritickými poskytovateli služeb IKT z řad třetích stran zákazníkům, kteří nejsou subjekty spadajícími do oblasti působnosti tohoto nařízení.

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

Před vydáním doporučení v souladu s odst. 1 písm. d) poskytne hlavní orgán dohledu poskytovateli služeb IKT z řad třetích stran příležitost poskytnout do 30 kalendářních dnů relevantní informace dokládající očekávaný dopad na zákazníky, kteří nejsou subjekty spadajícími do oblasti působnosti tohoto nařízení, a případně navrhovat řešení ke zmírnění rizik.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

4. Hlavní orgán dohledu informuje společnou síť dohledu o výsledku výkonu pravomocí uvedených v odst. 1 písm. a) a b). Hlavní orgán dohledu předá zprávy uvedené v odst. 1 písm. c) bez zbytečného odkladu společné síti dohledu a příslušným orgánům finančních subjektů využívajících služby IKT daného kritického poskytovatele služeb IKT z řad třetích stran.

5. Kritičtí poskytovatelé služeb IKT z řad třetích stran v dobré víře spolupracují s hlavním orgánem dohledu a pomáhají mu při plnění jeho úkolů.

6. Pokud kritický poskytovatel služeb IKT z řad třetích stran zcela nebo částečně neučiní opatření, která jsou od něj vyžadována v souvislosti s výkonem pravomocí podle odst. 1 písm. a), b) a c), přijme hlavní orgán dohledu po uplynutí lhůty nejméně 30 kalendářních dnů ode dne, kdy kritický poskytovatel služeb IKT z řad třetích stran obdržel oznámení o příslušných opatřeních, rozhodnutí o uložení penále, aby kritického poskytovatele služeb IKT z řad třetích stran přiměl daná opatření dodržovat.

7. Penále uvedené v odstavci 6 se ukládá na denním základě, dokud není dosaženo souladu s danými opatřeními, avšak nejdéle po dobu šesti měsíců od vyrozumění kritického poskytovatele služeb IKT z řad třetích stran o rozhodnutí uložit penále.

8. Výše penále vypočítaná ode dne uvedeného v rozhodnutí o uložení penále činí až 1 % průměrného denního celosvětového obratu kritického poskytovatele služeb IKT z řad třetích stran za předchozí účetní období. Při stanovení výše penále zohlední hlavní orgán dohledu tato kritéria týkající se nedodržení opatření uvedených v odstavci 6:

   i) závažnost a délku trvání nedodržování opatření;

   ii) zda k nedodržení opatření došlo úmyslně nebo z nedbalosti;

   iii) míru spolupráce poskytovatele služeb IKT z řad třetích stran s hlavním orgánem dohledu.

   Pro účely prvního pododstavce vede hlavní orgán dohledu v zájmu zajištění jednotného přístupu konzultace se společnou sítí dohledu.

9. Penále mají správní povahu a jsou vymahatelná. 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 penále jsou příjmem souhrnného rozpočtu Evropské unie.

10. Hlavní orgán dohledu zveřejní každé uložené penále, ledaže by toto zveřejnění vážně ohrozilo finanční trhy nebo způsobilo zúčastněným stranám nepřiměřenou škodu.

11. Hlavní orgán dohledu před uložením penále podle odstavce 6 umožní zástupcům kritického poskytovatele služeb IKT z řad třetích stran, jehož se řízení týká, vyjádřit se k jeho zjištěním a svá rozhodnutí založí pouze na zjištěních, k nimž měl kritický poskytovatel služeb IKT z řad třetích stran, jehož se řízení týká, možnost se vyjádřit.

V průběhu řízení musí být plně respektováno právo účastníků řízení na obhajobu. Kritický poskytovatel služeb IKT z řad třetích stran, jehož se řízení týká, má právo nahlížet do spisu, 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 36*

*Výkon pravomocí hlavního orgánu dohledu mimo Unii*

1. Nelze-li cílů v oblasti dohledu dosáhnout na základě komunikace s dceřiným podnikem založeným pro účely čl. 31 odst. 12 nebo na základě výkonu činností dohledu v prostorách nacházejících se v Unii, může hlavní orgán dohledu vykonávat v jakýchkoli prostorách nacházejících se ve třetí zemi, které jsou kritickým poskytovatelem služeb IKT z řad třetích stran vlastněny nebo jakýmkoli způsobem využívány pro účely poskytování služeb finančním subjektům v Unii v souvislosti s jeho obchodními operacemi, funkcemi nebo službami, včetně jakýchkoli správních, obchodních nebo provozně kancelářských prostor, objektů, pozemků, budov nebo jiných nemovitostí, pravomoci uvedené v:

   a) čl. 35 odst. 1 písm. a) a

   b) čl. 35 odst. 1 písm. b), v souladu s čl. 38 odst. 2 písm. a), b) a d) a čl. 39 odst. 1 a odst. 2 písm. a).

   Pravomoci uvedené v prvním pododstavci mohou být vykonávány, pokud jsou splněny všechny tyto podmínky:

   i) hlavní orgán dohledu považuje provedení kontroly ve třetí zemi za nezbytné, aby mohl plně a účinně plnit své povinnosti podle tohoto nařízení;

ii) kontrola ve třetí zemi přímo souvisí s poskytováním služeb IKT finančním subjektům v Unii;

iii) dotčený kritický poskytovatel služeb IKT z řad třetích stran s provedením kontroly ve třetí zemi souhlasí a

iv) relevantní orgán dotčené třetí země byl hlavním orgánem dohledu oficiálně informován a nevznesl žádné námitky.

2. Aniž jsou dotčeny příslušné pravomoci orgánů Unie a členských států, uzavřou EBA, ESMA nebo EIOPA pro účely odstavce 1 ujednání o správní spolupráci s relevantním orgánem třetí země s cílem umožnit hladké provádění kontrol v dotčené třetí zemi ze strany hlavního orgánu dohledu a jeho určeného týmu pro účely jeho poslání v dané třetí zemi. Tato ujednání o spolupráci nezakládají právní závazky vůči Unii a jejím členským státům ani členským státům a jejich příslušným orgánům nebrání v uzavírání dvoustranných nebo mnohostranných ujednání s těmito třetími zeměmi a jejich relevantními orgány.

Tato ujednání o spolupráci stanoví alespoň tyto prvky:

a) postupy pro koordinaci činností dohledu prováděných podle tohoto nařízení a jakékoli obdobné sledování rizika v oblasti IKT spojeného s třetími stranami ve finančním sektoru prováděné relevantním orgánem dotčené třetí země, včetně podrobností pro předání souhlasu tohoto orgánu, který umožní hlavnímu orgánu dohledu a jeho určenému týmu provádět obecná šetření a kontroly na místě, jak je uvedeno v odst. 1 prvním pododstavci, na území, jež spadá do jeho jurisdikce;

b) mechanismus pro předávání veškerých relevantních informací mezi EBA, ESMA nebo EIOPA a relevantním orgánem dotčené třetí země, zejména v souvislosti s informacemi, které si může hlavní orgán dohledu vyžádat podle článku 37;

c) mechanismy, jejichž prostřednictvím bude relevantní orgán dotčené třetí země EBA, ESMA nebo EIOPA neprodleně oznamovat případy, kdy se má za to, že poskytovatel služeb IKT z řad třetích stran usazený ve třetí zemi, který byl určen za kritického v souladu s čl. 31 odst. 1 písm. a), porušil požadavky, které musí dodržovat podle použitelného práva dotčené třetí země při poskytování služeb finančním institucím v této třetí zemi, jakož i učiněná náprava a uplatněné sankce;

d) pravidelné předávání aktuálních informací o vývoji v oblasti regulace nebo dohledu, pokud jde o sledování rizika v oblasti IKT spojeného se třetími stranami u finančních institucí v dotčené třetí zemi;

e) podrobnosti umožňující v případě potřeby účast jednoho zástupce relevantního orgánu třetí země na kontrolách prováděných hlavním orgánem dohledu a určeným týmem.

3. Pokud není schopen provádět kontrolní činnosti uvedené v odstavcích 1 a 2 mimo Unii, hlavní orgán dohledu:

a) vykonává své pravomoci podle článku 35 na základě všech skutečností a dokumentů, které má k dispozici;

b) zdokumentuje a vysvětlí veškeré důsledky toho, že není schopen provádět plánované činnosti dohledu podle tohoto článku.

Možné důsledky uvedené v písmenu b) tohoto odstavce se zohlední v doporučeních hlavního orgánu dohledu vydaných podle čl. 35 odst. 1 písm. d).

*Článek 37*

*Žádost o informace*

1. Hlavní orgán dohledu může prostou žádostí nebo rozhodnutím požádat kritické poskytovatele služeb IKT z řad třetích stran, aby poskytly veškeré informace nezbytné pro výkon povinností hlavního orgánu dohledu podle tohoto nařízení, včetně všech relevantních obchodních nebo provozních dokladů, smluv, politik, dokumentace, 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 činností.

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

   a) odkáže 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) odkáže na tento článek jako na právní základ žádosti;

b) uvede účel žádosti;

c) upřesní, jaké informace jsou požadovány;

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

e) upozorní na penále stanovené v čl. 35 odst. 6, pokud budou požadované informace poskytnuty neúplné nebo pokud nebudou tyto informace poskytnuty ve lhůtě stanovené v písmenu d) tohoto odstavce;

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 a (EU) č. 1095/2010.

4. Zástupci kritických poskytovatelů služeb IKT z řad třetích stran jsou povinni požadované informace poskytnout. 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 předá kopii rozhodnutí o předložení informací příslušným orgánům finančních subjektů využívajících služeb příslušných kritických poskytovatelů služeb IKT z řad třetích stran a společné síti dohledu.

*Článek 38*

*Obecná šetření*

1. Aby mohl plnit své povinnosti podle tohoto nařízení, může hlavní orgán dohledu s pomocí společného kontrolního týmu uvedeného v čl. 40 odst. 1 provádět v případě potřeby šetření kritických poskytovatelů služeb IKT z řad třetích stran.

2. Hlavní orgán dohledu má pravomoc:

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

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

c) předvolat zástupce kritického poskytovatele služeb IKT z řad třetích stran a požádat jej o ústní nebo písemné vysvětlení skutečností nebo dokumentů, které se týkají předmětu a účelu šetření, a odpovědi zaznamenat;

d) vyslechnout jakoukoli jinou fyzickou nebo právnickou osobu, které 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 po předložení písemného pověření, v němž je uveden předmět a účel šetření.

V tomto pověření se rovněž uvede penále podle čl. 35 odst. 6, nebudou-li předloženy požadované záznamy, údaje, zdokumentované postupy nebo jakékoliv jiné materiály nebo odpovědi na otázky položené zástupcům poskytovatele služeb IKT z řad třetích stran, nebo nebudou-li úplné.

4. Zástupci kritických 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, penále stanovené v čl. 35 odst. 6, 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 zahájením šetření informuje příslušné orgány finančních subjektů využívajících služby IKT tohoto kritického poskytovatele služeb IKT z řad třetích stran o zamýšleném šetření a o totožnosti pověřených osob.

Hlavní orgán dohledu sdělí společné síti dohledu veškeré informace předané podle prvního pododstavce.

*Článek 39*

*Kontroly*

1. Aby mohl plnit své povinnosti podle tohoto nařízení, může hlavní orgán dohledu s pomocí společného kontrolního týmu uvedeného v čl. 40 odst. 1 vstupovat do všech prostor, na všechny pozemky nebo do všech budov využívaných k podnikatelské činnosti poskytovatelů služeb IKT z řad třetích stran, jako jsou jejich sídla, provozní střediska, druhotná pracoviště, a provádět v nich všechny nezbytné kontroly na místě a rovněž může provádět kontroly na dálku.

   Pro účely výkonu pravomocí uvedených v prvním pododstavci konzultuje hlavní orgán dohledu společnou síť dohledu.

2. Úředníci a jiné osoby zmocněné hlavním orgánem dohledu k provedení kontroly na místě mají pravomoc:

   a) vstupovat do všech takových prostor, na všechny pozemky a do všech budov využívaných k podnikatelské činnosti, a

   b) zapečetit veškeré takové podnikatelské prostory, účetní knihy nebo záznamy po dobu a v rozsahu, které jsou pro kontrolu nezbytné.

Úředníci a jiné osoby zmocněné hlavním orgánem dohledu své pravomoci vykonávají po předložení písemného pověření uvádějícího předmět a účel kontroly a penále podle čl. 35 odst. 6 pro případ, že se zástupci dotčených kritických poskytovatelů služeb IKT z řad třetích stran kontrole nepodrobí.

3. Hlavní orgán dohledu informuje s dostatečným předstihem před zahájením kontroly 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 používaných nebo přispívajících k poskytování služeb IKT 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, penále stanovené v čl. 35 odst. 6, 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 se kritický poskytovatel služeb IKT z řad třetích stran odmítá podrobit kontrole nařízené podle tohoto článku, hlavní orgán dohledu informuje kritického poskytovatele služeb IKT z řad třetích stran o důsledcích tohoto odmítnutí, včetně skutečnosti, že příslušné orgány dotčených finančních subjektů mohou od finančních subjektů vyžadovat, aby ukončily smluvní ujednání uzavřená s tímto kritickým poskytovatelem služeb IKT z řad třetích stran.

*Článek 40*

*Průběžný dohled*

1. Hlavnímu orgánu dohledu je při provádění činností dohledu, a zejména obecných šetření nebo kontrol, nápomocen společný kontrolní tým vytvořený pro každého kritického poskytovatele služeb IKT z řad třetích stran.

2. Společný kontrolní tým uvedený v odstavci 1 tvoří pracovníci:

   a) evropských orgánů dohledu;

   b) relevantních příslušných orgánů vykonávajících dohled nad finančními subjekty, jimž daný kritický poskytovatel služeb IKT z řad třetích stran poskytuje své služby;

   c) vnitrostátního příslušného orgánu uvedeného v čl. 32 odst. 4 písm. e), a to na dobrovolném základě;

   d) jednoho vnitrostátního příslušného orgánu z členského státu, v němž je kritický poskytovatel služeb IKT z řad třetích stran usazen, a to na dobrovolném základě.

Členové společného kontrolního týmu mají odborné znalosti v oboru IKT a v oblasti operačního rizika. Práci společného kontrolního týmu koordinuje určený pracovník hlavního orgánu dohledu („koordinátor hlavního orgánu dohledu“).

3. Hlavní orgán dohledu do tří měsíců po dokončení šetření nebo kontroly a po konzultaci s fórem dohledu přijme doporučení, která budou adresována kritickému poskytovateli služeb IKT z řad třetích stran podle pravomocí uvedených v článku 35.

4. Doporučení uvedená v odstavci 3 se neprodleně sdělí kritickému poskytovateli služeb IKT z řad třetích stran a příslušným orgánům finančních subjektů, jimž služby IKT poskytuje.

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

*Článek 41*

*Harmonizace podmínek umožňujících provádění činností dohledu*

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

   a) informace, jež mají být předloženy v žádosti o dobrovolnou účast poskytovatelem služeb IKT z řad třetích stran, jenž má být podle čl. 31 odst. 11 určen za kritického;

   b) obsah, strukturu a formát informací, jež mají poskytovatelé služeb IKT z řad třetích stran předložit, zpřístupnit nebo oznámit podle čl. 35 odst. 1, včetně šablony pro poskytování informací o ujednáních o subdodávkách;

   c) kritéria pro určení složení společného kontrolního týmu zajišťující vyváženou účast pracovníků evropských orgánů dohledu a relevantních příslušných orgánů, jejich určení, úkoly a organizaci práce;

   d) podrobnosti o vyhodnocení opatření přijatých kritickými poskytovateli služeb IKT z řad třetích stran na základě doporučení hlavního orgánu dohledu podle čl. 42 odst. 3 příslušnými orgány.

2. Evropské orgány dohledu předloží tyto návrhy regulačních technických norem Komisi do ... [18 měsíců ode dne vstupu tohoto nařízení v platnost].

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

*Článek 42*

*Následná opatření příslušných orgánů*

1. Kritičtí poskytovatelé služeb IKT z řad třetích stran do 60 kalendářních dnů od obdržení doporučení vydaných hlavním orgánem dohledu podle čl. 35 odst. 1 písm. d) buď oznámí hlavnímu orgánu dohledu svůj úmysl se těmito doporučeními řídit, nebo poskytnou odůvodněné vysvětlení, proč se těmito doporučeními řídit nebudou. Hlavní orgán dohledu tyto informace neprodleně předá příslušným orgánům dotčených finančních subjektů.

2. Hlavní orgán dohledu zveřejní, jestliže mu kritický poskytovatel služeb IKT z řad třetích stran neoznámí svůj úmysl podle odstavce 1 nebo jestliže nepovažuje vysvětlení poskytnuté kritickým poskytovatelem služeb IKT z řad třetích stran za dostatečné. Zveřejněné informace zahrnují totožnost kritického poskytovatele služeb IKT z řad třetích stran, jakož i informace o druhu a povaze porušení. Tyto informace se omezí na to, co je relevantní a přiměřené pro účely zajištění informovanosti veřejnosti, ledaže by jejich zveřejnění mohlo zúčastněným stranám způsobit nepřiměřenou škodu nebo by mohlo vážně ohrozit řádné fungování a integritu finančních trhů nebo stabilitu celého finančního systému Unie nebo jeho části.

   Hlavní orgán dohledu o tomto zveřejnění informuje poskytovatele služeb IKT z řad třetích stran.

3. Příslušné orgány informují příslušné finanční subjekty o rizicích identifikovaných v doporučeních adresovaných kritickým poskytovatelům služeb IKT z řad třetích stran v souladu s čl. 35 odst. 1 písm. d).

   Při řízení rizika v oblasti IKT spojeného se třetími stranami finanční subjekty zohlední rizika uvedená v prvním pododstavci.

4. Pokud se příslušný orgán domnívá, že finanční subjekt v rámci svého řízení rizika v oblasti IKT spojeného se třetími stranami nezohledňuje nebo dostatečně neřeší konkrétní rizika identifikovaná v doporučeních, upozorní finanční subjekt na možnost přijmout do 60 kalendářních dnů od tohoto upozornění rozhodnutí podle odstavce 6, pokud neexistují vhodná smluvní ujednání zaměřená na řešení těchto rizik.

5. Po obdržení zpráv uvedených v čl. 35 odst. 1 písm. c) a před přijetím rozhodnutí uvedeného v odstavci 6 tohoto článku mohou příslušné orgány dobrovolně konzultovat příslušné orgány určené nebo zřízené v souladu se směrnicí (EU) …/…[+], které jsou odpovědné za dohled nad zásadním nebo důležitým subjektem podléhajícím uvedené směrnici, který byl určen jako kritický poskytovatel služeb IKT z řad třetích stran.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

6. Příslušné orgány mohou jako krajní opatření v návaznosti na upozornění a případně konzultaci podle odstavců 4 a 5 tohoto článku přijmout v souladu s článkem 50 rozhodnutí vyžadující, aby finanční subjekty částečně či úplně dočasně přestaly využívat služby poskytované kritickým poskytovatelem služeb IKT z řad třetích stran, dokud daný kritický poskytovatel služeb IKT z řad třetích stran neodstraní rizika identifikovaná v jemu adresovaných doporučeních. Je-li to nezbytné, mohou finanční subjekty požádat, aby zcela či zčásti ukončily příslušná smluvní ujednání uzavřená s dotčenými kritickými poskytovateli služeb IKT z řad třetích stran.

7. Pokud kritický poskytovatel služeb IKT z řad třetích stran odmítne uznat doporučení, protože zaujal odlišný přístup od přístupu doporučeného hlavním orgánem dohledu, a tento odlišný přístup může mít nepříznivý dopad na velký počet finančních subjektů nebo na významnou část finančního sektoru a individuální varování vydaná příslušnými orgány nevedla k jednotným přístupům, jež by zmírnily potenciální riziko pro finanční stabilitu, může hlavní orgán dohledu po konzultaci s fórem dohledu vydat nezávazné a neveřejné stanovisko určené příslušným orgánům, aby případně podpořil jednotná a konvergentní následná opatření v oblasti dohledu.

8. Po obdržení zpráv uvedených v čl. 35 odst. 1 písm. c) příslušné orgány při přijímání rozhodnutí podle odstavce 6 tohoto článku zohlední druh a rozsah rizika, které kritický poskytovatel služeb IKT z řad třetích stran neodstranil, a rovněž závažnost porušení povinností, přičemž přihlédnou k těmto kritériím:

a) závažnosti a délce trvání porušení předpisů;

b) zda porušení předpisů odhalilo závažná slabá místa v postupech, řídicích systémech, řízení rizik a interních kontrolách 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 jiným způsobem přičíst;

d) zda k porušení předpisů došlo úmyslně nebo z nedbalosti;

e) zda pozastavení nebo ukončení smluvních ujednání představuje riziko pro kontinuitu činnosti finančního subjektu, bez ohledu na snahu finančního subjektu vyhnout se narušení poskytování svých služeb;

f) v příslušných případech, jak stanoví odstavec 5 tohoto článku, dobrovolně vyžádané stanovisko příslušných orgánů určených nebo zřízených v souladu se směrnicí (EU) …/…[+], které jsou odpovědné za dohled nad zásadním nebo důležitým subjektem podléhajícím uvedené směrnici, který byl určen jako kritický poskytovatel služeb IKT z řad třetích stran.

Příslušné orgány poskytnou finančním subjektům nezbytnou lhůtu, aby mohly upravit smluvní ujednání s kritickými poskytovateli služeb IKT z řad třetích stran, a zabránit tak nepříznivým dopadům na jejich digitální provozní odolnost a zavést strategie ukončení smluvního vztahu a plány přechodu uvedené v článku 28.

9. Rozhodnutí podle odstavce 6 tohoto článku se oznámí členům fóra dohledu uvedeného v čl. 32 odst. 4 písm. a) b) a c) a společné síti dohledu.

Kritičtí poskytovatelé služeb IKT z řad třetích stran, jichž se týkají rozhodnutí podle odstavce 6, plně spolupracují s dotčenými finančními subjekty, zejména v souvislosti s procesem pozastavení nebo ukončení jejich smluvních ujednání.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

10. Příslušné orgány pravidelně informují hlavní orgán dohledu o přístupech a opatřeních přijatých v rámci jejich úkolů v oblasti dohledu ve vztahu k finančním subjektům a rovněž o smluvních ujednáních uzavřených finančními subjekty v případech, kdy kritičtí poskytovatelé služeb IKT z řad třetích stran zcela či zčásti neuznaly doporučení hlavního orgánu dohledu.

11. Hlavní orgán dohledu může na žádost poskytnout další vysvětlení k vydaným doporučením, aby příslušným orgánům poskytl vodítko pro následná opatření.

*Článek 43*

*Poplatky za dohled*

1. Hlavní orgán dohledu účtuje v souladu s aktem v přenesené pravomoci uvedeným v odstavci 2 tohoto článku kritickým poskytovatelům služeb IKT z řad třetích stran poplatky, které plně pokrývají nezbytné výdaje hlavního orgánu dohledu v souvislosti s prováděním úkolů v oblasti dohledu podle tohoto nařízení, včetně náhrady veškerých nákladů, jež mohou vzniknout v důsledku práce vykonané společným kontrolním týmem uvedeným v článku 40, jakož i nákladů na poradenství poskytované nezávislými odborníky podle čl. 32 odst. 4 druhého pododstavce v souvislosti se záležitostmi spadajícími do působnosti činností přímého dohledu.

Výše poplatku účtovaného kritickému poskytovateli služeb IKT z řad třetích stran zahrnuje veškeré náklady spojené s plněním povinností stanovených v tomto oddíle a je úměrná jeho obratu.

2. Komisi je svěřena pravomoc přijmout do … [18 měsíců ode dne vstupu tohoto nařízení v platnost v souladu s článkem 57 akt v přenesené pravomoci, kterým toto nařízení doplní stanovením výše poplatků a způsobu jejich úhrady.

*Článek 44*

*Mezinárodní spolupráce*

1. Aniž je dotčen článek 36, EBA, ESMA a EIOPA mohou v souladu s článkem 33 nařízení (EU) č. 1093/2010, (EU) č. 1095/2010 a (EU) č. 1094/2010 pro účely posílení mezinárodní spolupráce ohledně rizika v oblasti IKT spojeného s třetími stranami v různých finančních sektorech uzavírat správní ujednání s regulačními orgány a orgány dohledu třetích zemí, a to zejména vypracováním osvědčených postupů pro přezkum postupů a kontrol souvisejících s řízením rizika v oblasti IKT, zmírňujících opatření a reakce na incidenty.

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, v níž se zaměří na vývoj rizika v oblasti IKT spojeného s třetími stranami a dopady na finanční stabilitu, integritu trhu, ochranu investorů a fungování vnitřního trhu.

# Kapitola VI
# Ujednání o sdílení informací

*Článek 45*

*Ujednání o sdílení operativních a jiných informací o kybernetických hrozbách*

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

   a) zaměřuje na zlepšení digitální provozní odolnosti finančních subjektů, zejména zvyšováním povědomí o kybernetických hrozbách, omezením nebo zabráněním možností šíření těchto hrozeb podporou obranných schopností, techniky detekce hrozeb, zmírňující strategie nebo fáze reakce a obnovy;

   b) odehrává v důvěryhodných komunitách finančních subjektů;

c) provádí prostřednictvím ujednání o sdílení informací chránících potenciálně citlivou povahu sdílených informací, která se řídí pravidly chování plně respektujícími důvěrnou povahu obchodních informací, ochranu osobních údajů v souladu s nařízením (EU) 2016/679 a dodržování pokynů týkajících se hospodářské soutěže.

2. Pro účely odst. 1 písm. c) se v ujednání o sdílení informací stanoví podmínky účasti a případně podrobnosti o zapojení veřejných orgánů a jejich možné způsobilosti k účasti na ujednáních o sdílení informací, o zapojení poskytovatelů služeb IKT z řad třetích stran a 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 o ukončení členství, jakmile vstoupí v platnost.

# Kapitola VII
# Příslušné orgány

*Článek 46*

*Příslušné orgány*

Aniž jsou dotčena ustanovení o rámci dohledu pro kritické třetí strany poskytující služby IKT uvedená v kapitole V oddílu II tohoto nařízení, dodržování povinností stanovených tímto nařízením zajišťují v souladu se svými pravomocemi udělenými na základě příslušných právních aktů tyto příslušné orgány:

a) v případě úvěrových institucí a institucí vyňatých podle směrnice 2013/36/EU příslušný orgán určený v souladu s článkem 4 uvedené směrnice a v případě úvěrových institucí, které byly klasifikovány jako významné v souladu s čl. 6 odst. 4 nařízení (EU) č. 1024/2013, ECB v souladu s pravomocemi a úkoly jí svěřenými uvedeným nařízením;

b) v případě platebních institucí, včetně platebních institucí vyňatých podle směrnice (EU) 2015/2366, institucí elektronických peněz, včetně institucí elektronických peněz vyňatých podle směrnice 2009/110/ES, a poskytovatelů služeb informování o účtu podle čl. 33 odst. 1 směrnice (EU) 2015/2366 příslušný orgán určený v souladu s článkem 22 směrnice (EU) 2015/2366;

c) v případě investičních podniků příslušný orgán určený v souladu s článkem 4 směrnice Evropského parlamentu a Rady (EU) 2019/2034[1];

d) v případě poskytovatelů služeb souvisejících s kryptoaktivy, kteří mají povolení podle nařízení o trzích s kryptoaktivy, a vydavatelů tokenů vázaných na aktiva příslušný orgán určený v souladu s příslušným ustanovením uvedeného nařízení;

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

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

---

[1] Směrnice Evropského parlamentu a Rady (EU) 2019/2034 ze dne 27. listopadu 2019 o obezřetnostním dohledu nad investičními podniky a o změně směrnic 2002/87/ES, 2009/65/ES, 2011/61/EU, 2013/36/EU, 2014/59/EU a 2014/65/EU (Úř. věst. L 314, 5.12.2019, s. 64).

g) v případě obchodních systémů příslušný orgán určený v souladu s článkem 67 směrnice 2014/65/EU a v případě poskytovatelů služeb hlášení údajů příslušný orgán ve smyslu čl. 2 odst. 1 bodu 18 nařízení (EU) č. 600/2014;

h) v případě registrů obchodních údajů příslušný orgán určený v souladu s článkem 22 nařízení (EU) č. 648/2012;

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

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

k) v případě pojišťoven a zajišťoven příslušný orgán určený v souladu s článkem 30 směrnice 2009/138/ES;

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

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

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

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

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

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

*Článek 47*

*Spolupráce se strukturami a orgány zřízenými směrnicí (EU) .../...*[+]

1. Aby se usnadnila spolupráce a umožnila výměna v oblasti dohledu mezi příslušnými orgány určenými podle tohoto nařízení a skupinou pro spolupráci zřízenou podle článku 14 směrnice (EU) …/…[+], mohou se evropské orgány dohledu a příslušné orgány podílet na činnosti skupiny pro spolupráci, pokud jde o záležitosti týkající se jejich činností dohledu ve vztahu k finančním subjektům. Evropské orgány dohledu a příslušné orgány mohou požádat o přizvání k účasti na činnosti skupiny pro spolupráci, pokud jde o záležitosti týkající se zásadních nebo důležitých subjektů podléhajících směrnici (EU) …/…[+], které byly rovněž určeny za kritické poskytovatele služeb IKT z řad třetích stran podle článku 31 tohoto nařízení.

2. Ve vhodných případech mohou příslušné orgány vést konzultace a sdílet informace s jednotnými kontaktními místy a týmy CSIRT určenými nebo zřízenými v souladu se směrnicí (EU) …/…[+].

---

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

3. Ve vhodných případech si mohou příslušné orgány vyžádat relevantní technické poradenství a pomoc příslušných orgánů určených nebo zřízených v souladu se směrnicí (EU) …/…[+] a uzavřít ujednání o spolupráci s cílem umožnit zavedení účinných mechanismů pro koordinaci rychlé reakce.

4. V ujednáních uvedených v odstavci 3 tohoto článku se mohou mimo jiné stanovit postupy pro koordinaci činností v oblasti dohledu a dozoru ve vztahu k zásadním nebo důležitým subjektům podléhajícím směrnici (EU) …/…[+], které byly určeny za kritické poskytovatele služeb IKT z řad třetích stran podle článku 31 tohoto nařízení, a to i za účelem provádění šetření a kontroly na místě v souladu s vnitrostátním právem, jakož i za účelem mechanismů pro výměnu informací mezi příslušnými orgány podle tohoto nařízení a příslušnými orgány určenými nebo zřízenými v souladu se zmíněnou směrnicí, což zahrnuje i přístup k informacím, o něž dané určené nebo zřízené orgány požádaly.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359(COD)).

*Článek 48*

*Spolupráce mezi orgány*

1. Příslušné orgány úzce spolupracují mezi sebou navzájem a případně s hlavním orgánem dohledu.

2. Příslušné orgány a hlavní orgán dohledu si včas vzájemně vymění veškeré relevantní informace týkající se kritických poskytovatelů služeb IK z řad třetích stran, které jsou nezbytné k tomu, aby mohly plnit své povinnosti podle tohoto nařízení, zejména pokud jde o zjištěná rizika, přístupy a opatření přijatá v rámci úkolů hlavního orgánu dohledu v oblasti dohledu.

*Článek 49*

*Meziodvětvová cvičení, komunikace a spolupráce ve finančním sektoru*

1. Evropské orgány dohledu mohou prostřednictvím společného výboru a ve spolupráci s příslušnými orgány, orgány příslušnými k řešení krize podle článku 3 směrnice 2014/59/EU, ECB, Jednotným výborem pro řešení krizí, pokud jde o informace týkající se subjektů spadajících do oblasti působnosti nařízení (EU) č. 806/2014, ESRB a případně ENISA vytvářet mechanismy umožňující sdílení osvědčených postupů ve finančních odvětvích, které zlepší znalost situace a určí společné kybernetické zranitelnosti 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 Unie v případě závažného přeshraničního incidentu souvisejících s IKT nebo související hrozby se systémovým dopadem na finanční sektor Unie jako celek.

   Tato cvičení mohou ve vhodných případech rovněž testovat závislosti finančního sektoru na jiných hospodářských odvětvích.

2. Příslušné orgány, evropské orgány dohledu a ECB při plnění svých povinností podle článků 47 až 54 vzájemně úzce spolupracují a vyměňují si informace. Úzce koordinují svůj dohled za účelem zjišťování případů porušení tohoto nařízení a jejich nápravy, vypracování a prosazování osvědčených postupů, usnadňování spolupráce, prosazování jednotnosti výkladu a poskytování hodnocení napříč jurisdikcemi v případě jakékoli neshody.

*Článek 50*

*Správní sankce a nápravná opatření*

1. Příslušné orgány mají všechny kontrolní, vyšetřovací a sankční pravomoci nezbytné 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, které příslušný orgán považuje za relevantní pro výkon svých povinností, a obdržet nebo pořídit jejich kopii;

b) provádět kontroly na místě nebo šetření, jež zahrnují mimo jiné možnost:

i) předvolat zástupce finančních subjektů a požádat je o ústní nebo písemné vysvětlení skutečností nebo dokumentů, které se týkají předmětu a účelu šetření, a odpovědi zaznamenat;

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

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

3. Aniž je dotčeno jejich právo ukládat trestní sankce podle článku 52, členské státy přijmou pravidla stanovící vhodné správní sankce a nápravná opatření pro případy porušení tohoto nařízení a zajistí jejich účinné uplatňování.

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

4. Členské státy svěří příslušným orgánům pravomoc k uplatňování alespoň následujících správních sankcí nebo nápravných opatření v případech porušení tohoto nařízení:

a) vydat příkaz požadující, aby fyzická nebo právnická osoba ukončily jednání porušující toto nařízení nebo aby takové jednání neopakovaly;

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

c) přijmout jakákoliv opatření, včetně opatření peněžité povahy, zajišťující, že finanční subjekty budou 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 prohlášení uvádějících totožnost fyzických či právnických osob a povahu jejich porušení.

5. Pokud se odst. 2 písm. c) a odstavec 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 51*

*Výkon pravomoci ukládat správní sankce a jiná nápravná opatření*

1. Příslušné orgány vykonávají pravomoc ukládat správní sankce a nápravná opatření podle článku 50 v souladu se svým vnitrostátním právním řádem v příslušných případech takto:

   a) přímo;

   b) ve spolupráci s jinými orgány;

c) na svou odpovědnost přenesením pravomoci na jiné orgány nebo

d) podáním návrhu příslušným soudním orgánům.

2. Příslušné orgány při určování druhu a úrovně správní sankce nebo nápravného opatření uloženého podle článku 50 zohledňují, do jaké míry bylo porušení způsobeno úmyslně nebo z nedbalosti, a všechny ostatní relevantní okolnosti, případně včetně:

a) významu, závažnosti a doby trvání porušení;

b) míry odpovědnosti fyzické nebo právnické osoby odpovědných za porušení;

c) finanční síly odpovědné fyzické nebo právnické osoby;

d) významu zisků nebo ztrát, kterých odpovědná fyzická nebo právnická osoba dosáhly 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 těmito osobami nebo ztrát, kterým se vyhnuly;

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

*Článek 52*

*Trestní sankce*

1. Členské státy se mohou rozhodnout, že nestanoví správní sankce nebo nápravná opatření za ta porušení, 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 se soudními orgány, orgány vedoucími trestní stíhání či jinými orgány činnými v trestním řízení v rámci své jurisdikce s cílem získat konkrétní informace týkající se trestního vyšetřování či řízení zahájeného pro porušení tohoto nařízení a poskytnout tyto informace ostatním příslušným orgánům a rovněž EBA, ESMA nebo EIOPA, aby mohly splnit svou povinnost spolupráce pro účely tohoto nařízení.

*Článek 53*

*Oznamovací povinnost*

Členské státy oznámí právní a správní předpisy k provedení této kapitoly, včetně případných relevantních trestněprávních ustanovení, Komisi a ESMA, EBA a EIOPA do … [24 měsíců ode dne vstupu tohoto nařízení v platnost]. Dále Komisi a ESMA, EBA a EIOPA neprodleně oznámí všechny jejich následné změny.

*Článek 54*

*Uveřejnění správních sankcí*

1. Příslušné orgány uveřejňují na svých oficiálních internetových stránkách bez zbytečného odkladu všechna rozhodnutí o uložení správní sankce, proti nimž není možné podat opravný prostředek, jakmile je subjektu, jemuž byla sankce uložena, toto rozhodnutí oznámeno.

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

3. Pokud se příslušný orgán na základě posouzení jednotlivých případů domnívá, že by uveřejnění totožnosti u právnických osob nebo totožnosti a osobních údajů u fyzických osob nebylo přiměřené, včetně rizik souvisejících s ochranou osobních údajů, že by ohrožovalo stabilitu finančních trhů nebo vedení probíhajícího vyšetřování trestného činu, nebo by 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 uveřejnění až do okamžiku, kdy pominou všechny důvody pro neuveřejnění;

   b) uveřejní je anonymně v souladu s vnitrostátním právem; nebo

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

4. V případě rozhodnutí uveřejnit správní sankci anonymně podle odst. 3 písm. b) může být uveřejnění 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 internetových 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 uveřejnění podle odstavců 1 až 4 zůstalo na jejich oficiálních internetových stránkách pouze po dobu nezbytně nutnou k zajištění souladu s tímto článkem. Toto období nepřesáhne pět let od daného uveřejnění.

*Článek 55*

*Profesní tajemství*

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

2. Povinnost zachovávat profesní 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 něž příslušné orgány přenesly své pravomoci, včetně auditorů a odborníků smluvně najatých těmito orgány.

3. Informace, na něž se vztahuje profesní tajemství, včetně výměny informací mezi příslušnými orgány podle tohoto nařízení a příslušnými orgány určenými nebo zřízenými v souladu se směrnicí (EU) .../...[+], nesmějí být sděleny žádné jiné osobě nebo orgánu, vyjma na základě ustanovení unijního či vnitrostátního práva.

[+] Úř. věst.: vložte prosím do textu číslo směrnice obsažené v dokumentu PE-CONS 32/22 (2020/0359 (COD)).

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 profesnímu 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.

*Článek 56*

*Ochrana údajů*

1. Evropské orgány dohledu a příslušné orgány mohou zpracovávat osobní údaje pouze tehdy, je-li to nezbytné pro účely plnění jejich příslušných povinností podle tohoto nařízení, zejména pro účely šetření, kontroly, žádosti o informace, komunikace, zveřejňování, hodnocení, ověřování, posuzování a vypracovávání plánů dohledu. Osobní údaje se zpracovávají v souladu s nařízením (EU) 2016/679 nebo případně nařízením (EU) 2018/1725.

2. Není-li v jiných odvětvových aktech stanoveno jinak, osobní údaje uvedené v odstavci 1 se uchovávají až do splnění příslušných povinností dohledu a v každém případě po dobu nejvýše 15 let, s výjimkou případů, kdy soudní řízení vyžaduje další uchovávání těchto údajů.

# Kapitola VIII
# Akty v přenesené pravomoci

*Článek 57*

*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. 31 odst. 6 a čl. 43 odst. 2 je svěřena Komisi na dobu pěti let od ... [12 měsíců ode dne vstupu tohoto nařízení v platnost]. Komise vypracuje zprávu o výkonu přenesení pravomoci nejpozději devět měsíců před koncem tohoto pětiletého období. 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. 31 odst. 6 a čl. 43 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. 31 odst. 6 a čl. 43 odst. 2 vstoupí v platnost pouze tehdy, pokud proti němu Evropský parlament ani 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 58*

*Ustanovení o přezkumu*

1. Do... [pět let ode dne vstupu tohoto nařízení v platnost] Komise po konzultaci s EBA, ESMA, EIOPA a případně ESRB provede přezkum a předloží zprávu Evropskému parlamentu a Radě, k níž případně připojí legislativní návrh. Tento přezkum zahrnuje alespoň:

   a) kritéria pro určení kritických poskytovatelů služeb IKT z řad třetích stran v souladu s čl. 31 odst. 2;

   b) dobrovolnou povahu oznamování významných kybernetických hrozeb podle článku 19;

c) režim uvedený v čl. 31 odst. 12 a pravomoci hlavního orgánu dohledu stanovené v čl. 35 odst. 1 písm. d) bodě iv) první odrážce, a to s cílem posoudit účinnost těchto ustanovení s ohledem na zajištění účinného dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran usazenými ve třetí zemi a nezbytnost založit dceřiný podnik v Unii.

Pro účely prvního pododstavce tohoto písmene přezkum zahrnuje analýzu režimu uvedeného v čl. 31 odst. 12, včetně podmínek přístupu finančních subjektů Unie ke službám ze třetích zemí a dostupnosti těchto služeb na trhu Unie, a zohlední další vývoj na trzích služeb, na něž se vztahuje toto nařízení, praktické zkušenosti finančních subjektů a orgánů finančního dohledu, pokud jde o uplatňování tohoto režimu a dohled nad ním, a veškerý relevantní vývoj v oblasti regulace a dohledu na mezinárodní úrovni;

d) vhodnost toho, aby byly do oblasti působnosti tohoto nařízení zahrnuty finanční subjekty uvedené v čl. 2 odst. 3 písm. e), které využívají automatizované systémy prodeje, s ohledem na budoucí vývoj na trhu, pokud jde o využívání těchto systémů;

e) fungování a účinnost společné sítě dohledu při podpoře soudržnosti dohledu a efektivnosti výměny informací v mezích rámce dohledu.

2. V souvislosti s přezkumem směrnice (EU) 2015/2366 Komise posoudí potřebu větší kybernetické odolnosti platebních systémů a činností zpracování plateb a vhodnost rozšíření oblasti působnosti tohoto nařízení na provozovatele platebních systémů a subjekty zapojené do činností zpracování plateb. Na základě tohoto posouzení předloží Komise Evropskému parlamentu a Radě zprávu v rámci přezkumu směrnice (EU) 2015/2366 do ... [šest měsíců ode dne vstupu tohoto nařízení v platnost].

Na základě této zprávy o přezkumu a po konzultaci evropských orgánů dohledu, ECB a ESRB může Komise ve vhodných případech a v rámci legislativního návrhu, který může přijmout podle čl. 108 druhého pododstavce směrnice (EU) 2015/2366, předložit návrh na zajištění toho, aby všichni provozovatelé platebních systémů a subjekty zapojené do činností zpracování plateb podléhali náležitému dohledu, a to při zohlednění stávajícího dohledu ze strany centrální banky.

3. Do ... [tři roky ode dne vstupu tohoto nařízení v platnost] provede Komise po konzultaci s evropskými orgány dohledu a Výborem evropských orgánů dohledu nad auditem přezkum a předloží Evropskému parlamentu a Radě zprávu, k níž případně přiloží legislativní návrh týkající se vhodnosti přísnějších požadavků na statutární auditory a auditorské společnosti, pokud jde o digitální provozní odolnost, a to zahrnutím statutárních auditorů a auditorských společností do oblasti působnosti tohoto nařízení nebo změnou směrnice Evropského parlamentu a Rady 2006/43/ES[1].

[1] Směrnice Evropského parlamentu a Rady 2006/43/ES ze dne 17. května 2006 o povinném auditu ročních a konsolidovaných účetních závěrek, o změně směrnic Rady 78/660/EHS a 83/349/EHS a o zrušení směrnice Rady 84/253/EHS (Úř. věst. L 157. 9.6.2006. s. 87).

## ODDÍL II

## ZMĚNY

*Článek 59*

*Změny nařízení (ES) č. 1060/2009*

Nařízení (ES) č. 1060/2009 se mění takto:

1) V příloze I oddílu A bodu 4 se 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) …/…[*+].

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L …).“;

---

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

2) V příloze III se bod 12 nahrazuje tímto:

„12. Ratingová agentura porušuje čl. 6 odst. 2 ve spojení s oddílem A bodem 4 přílohy I tím, že nemá řádné administrativní nebo účetní postupy, mechanismy vnitřní kontroly, účinné postupy hodnocení rizik a účinná kontrolní a ochranná opatření pro řízení systémů IKT v souladu s nařízením (EU) …/…[+], nebo že nezavede a neudržuje rozhodovací postupy a organizační struktury, jak je vyžaduje zmíněný bod.“

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

*Článek 60*

*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) …/…[*+].

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L …).“;

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

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 zachování provozu a plán obnovy činnosti po havárii, který zahrnuje politiku zachování provozu IKT a plány reakce a obnovy v oblasti IKT zavedené a prováděné v souladu s nařízením (EU) …/…[+], s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění povinností ústřední protistrany.“;

b) v odstavci 3 se první pododstavec nahrazuje tímto:

„3. 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 politiky zachování provozu IKT a plánu obnovy činnosti po havárii IKT.“

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

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

„3. K 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 rizika 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 vypracováním vhodných systémů, kontrol a postupů, včetně systémů IKT řízených v souladu s nařízením (EU) …/…[+].

2. Registr obchodních údajů stanoví, provádí a dodržuje adekvátní politiku zachování provozu a plán obnovy činnosti po havárii, včetně politiky zachování provozu IKT a plánů reakce a obnovy v oblasti IKT vypracovaných v souladu s nařízením (EU) …/…[+], s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění svých povinností.“

5) v článku 80 se zrušuje odstavec 1.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

6) v příloze I se oddíl II mění takto:

a) písmena a) a b) se nahrazují tímto:

„a) registr obchodních údajů porušuje čl. 79 odst. 1 tím, že neurčí zdroje operačního rizika nebo nezajistí jejich minimalizaci vypracováním vhodných systémů, kontrol a postupů, včetně systémů IKT řízených v souladu s nařízením (EU) …/…[+];

b) registr obchodních údajů porušuje čl. 79 odst. 2 tím, že nestanoví, neprovádí nebo nedodržuje adekvátní politiku zachování provozu a plán obnovy po havárii vypracované v souladu s nařízením (EU) …/…[+] s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění svých povinností.“;

b) písmeno c) se zrušuje.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

7) příloha III se mění takto:

a) oddíl II se mění takto:

i) písmeno c) se nahrazuje tímto:

„c) ústřední protistrana tier 2 porušuje čl. 26 odst. 3 tím, že nemá nebo neprovozuje organizační strukturu, která zajišťuje nepřetržitý a řádný výkon jejích služeb a činností, nebo nevyužívá vhodné a přiměřené systémy, zdroje a postupy, včetně systémů IKT řízených v souladu s nařízením (EU) …/…[+];

ii) písmeno f) se zrušuje;

b) v oddíle III se písmeno a) nahrazuje tímto:

„a) ústřední protistrana tier 2 porušuje čl. 34 odst. 1 tím, že nezavede, neprovádí nebo neudržuje adekvátní politiku zachování provozu a plán reakce a obnovy vypracovaný v souladu s nařízením (EU) …/…[+]s cílem zajistit zachování svých funkcí, včasné obnovení operací a plnění povinností ústřední protistrany, který umožňuje alespoň obnovit všechny obchody k okamžiku přerušení, aby ústřední protistrana mohla nadále s jistotou fungovat a dokončit vypořádání ve stanovený den;“.

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

*Článek 61*

*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 zaváděním vhodných nástrojů, procesů a politik IKT zavedených a řízených v souladu s nařízením Evropského parlamentu a Rady (EU) …/…[*+] a rovněž pomocí jakýchkoli jiných vhodných nástrojů, kontrol a postupů pro jiné druhy operačního rizika, mimo jiné pro všechny vypořádací systémy, které provozuje.

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L …).“

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

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 adekvátní politiku zachování provozu a plán obnovy provozu po havárii, včetně politiky zachování provozu IKT a plánů reakce a obnovy v oblasti IKT vypracovaných v souladu s nařízením (EU) …/…[+], 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. 12 odst. 5 a 7 nařízení (EU) …/…[+].“

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

4) odstavec 6 se nahrazuje tímto:

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

5) v odstavci 7 se první pododstavec nahrazuje tímto:

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

*Článek 62*

*Změny nařízení (EU) č. 600/2014*

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

1) článek 27g se mění takto:

a) odstavec 4 se nahrazuje tímto:

„4. „Schválený systém pro uveřejňování splňuje požadavky týkající se bezpečnosti sítí a informačních systémů stanovené v nařízení Evropského parlamentu a Rady (EU) …/… [*+].

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L …).“;

---

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

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

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

2) článek 27h se mění takto:

a) odstavec 5 se nahrazuje tímto:

„5. Schválený systém pro uveřejňování splňuje požadavky týkající se bezpečnosti sítí a informačních systémů stanovené v nařízení (EU) …/…[+].“;

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 nahrazuje tímto:

„3. Schválený mechanismus pro hlášení obchodů splňuje požadavky týkající se bezpečnosti sítí a informačních systémů stanovené v nařízení (EU) …/…[+].“;

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)).

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

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

*Článek 63*

*Změny nařízení (EU) 2016/1011*

V článku 6 nařízení (EU) 2016/1011 se doplňuje nový odstavec, který zní:

„6. U referenčních hodnot s kritickým významem administrátor 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) …/…[*+].

---

[*] Nařízení Evropského parlamentu a Rady (EU) …/… ze dne … o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011 (Úř. věst. L …).“

[+] Úř. věst.: vložte prosím číslo nařízení obsaženého v dokumentu PE-CONS 41/22 (2020/0266(COD)) a doplňte odpovídajícím způsobem poznámku pod čarou.

*Článek 64*

*Vstup v platnost a použitelnost*

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

Použije se ode dne … [24 měsíců ode dne vstupu tohoto nařízení v platnost].

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

V ... dne ...

| | |
|---|---|
| *Za Evropský parlament* | *Za Radu* |
| *předsedkyně* | *předseda* nebo *předsedkyně* |