NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2025/295

ze dne 24. října 2024,

kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy týkající se harmonizace podmínek umožňujících provádění činností dohledu

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského Parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 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 ([1]), a zejména na čl. 41 odst. 2 druhý pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Rámec digitální provozní odolnosti finančního sektoru stanovený nařízením (EU) 2022/2554 zavádí rámec dohledu Unie pro poskytovatele služeb informačních a komunikačních technologií (IKT) finančnímu sektoru z řad třetích stran, kteří jsou v souladu s článkem 31 uvedeného nařízení určeni jako kritičtí.

(2) Poskytovatel služeb IKT z řad třetích stran, který se rozhodne podat dobrovolnou žádost, aby byl určen jako kritický, by měl poskytnout přijímajícímu evropskému orgánu dohledu všechny nezbytné informace k prokázání své kritičnosti podle zásad a kritérií stanovených v nařízení (EU) 2022/2554. Z tohoto důvodu by informace, které mají být zahrnuty do žádosti o dobrovolnou účast, měly být dostatečně podrobné a úplné, aby umožnily jasné a úplné posouzení kritičnosti podle čl. 31 odst. 11 uvedeného nařízení. Příslušný evropský orgán dohledu by měl odmítnout každou neúplnou žádost a vyžádat si chybějící informace.

(3) Právní identifikace poskytovatelů služeb IKT z řad třetích stran v oblasti působnosti této regulační technické normy by měla být sladěna s identifikačním kódem stanoveným v prováděcím nařízení Komise přijatém v souladu s čl. 28 odst. 9 nařízení (EU) 2022/2554.

(4) V návaznosti na doporučení vydaná hlavním orgánem dohledu kritickým poskytovatelům služeb IKT z řad třetích stran by měl hlavní orgán dohledu sledovat, zda kritičtí poskytovatelé služeb IKT z řad třetích stran tato doporučení dodržují. S cílem zajistit účinné a efektivní monitorování opatření, která byla přijata, nebo nápravných opatření, která byla provedena kritickými poskytovateli služeb IKT z řad třetích stran v souvislosti s těmito doporučeními, by měl mít hlavní orgán dohledu možnost vyžádat si zprávy uvedené v čl. 35 odst. 1 písm. c) nařízení (EU) 2022/2554, které by měly být koncipovány jako průběžné zprávy o pokroku a závěrečné zprávy.

(5) Pro účely posouzení uvedeného v čl. 42 odst. 1 nařízení (EU) 2022/2554, podle kterého je hlavní orgán dohledu povinen posoudit, zda je vysvětlení poskytnuté kritickým poskytovatelem služeb IKT z řad třetích stran dostatečné, by mělo být oznámení kritického poskytovatele služeb IKT z řad třetích stran hlavnímu orgánu dohledu o jeho záměru řídit se obdrženými doporučeními doplněno popisem činností a opatření, která byla přijata ke zmírnění rizik uvedených v doporučeních, spolu s jejich příslušnými lhůtami. Toto vysvětlení by mělo mít podobu plánu nápravných opatření.

(6) Vzhledem k tomu, že se očekává, že hlavní orgán dohledu bude posuzovat subdodavatelská ujednání kritického poskytovatele služeb IKT z řad třetích stran, je třeba vypracovat šablonu pro poskytování informací o těchto ujednáních. Tato šablona by měla zohlednit skutečnost, že kritičtí poskytovatelé služeb IKT z řad třetích stran mají jinou strukturu než finanční subjekty.

([1]) Úř. věst. L 333, 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Jakmile hlavní orgán dohledu vydá doporučení pro kritického poskytovatele služeb IKT z řad třetích stran a příslušné orgány informují příslušné finanční subjekty o rizicích uvedených v těchto doporučeních, měl by hlavní orgán dohledu sledovat a posuzovat, jak kritický poskytovatel služeb IKT z řad třetích stran provádí opatření a nápravná opatření k dosažení souladu s doporučeními. Příslušné orgány by měly sledovat a posuzovat, do jaké míry jsou finanční subjekty vystaveny rizikům uvedeným v těchto doporučeních. V zájmu zachování rovných podmínek při plnění svých příslušných úkolů, zejména pokud jsou rizika identifikovaná v doporučeních závažná a týkají se velkého počtu finančních subjektů ve více členských státech, by si příslušné orgány i hlavní orgán dohledu měly mezi sebou vyměňovat veškerá relevantní zjištění, která jsou nezbytná pro plnění jejich příslušných úkolů. Cílem sdílení informací je zajistit, aby zpětná vazba hlavního orgánu dohledu určená kritickému poskytovateli služeb IKT z řad třetích stran v souvislosti s opatřeními a nápravnými opatřeními, která tento poskytovatel provádí, zohledňovala dopad na rizika finančních subjektů a aby činnosti dohledu prováděné příslušnými orgány byly založeny na posouzení provedeném hlavním orgánem dohledu.

(8) Aby bylo možné účinně a efektivně sdílet informace, měly by příslušné orgány v rámci své dohledové činnosti posoudit, do jaké míry jsou finanční subjekty podléhající jejich dohledu vystaveny rizikům uvedeným v doporučeních. Toto posouzení by mělo být provedeno přiměřeně a na základě rizik. Ve specifických případech, kdy jsou rizika spojená s doporučeními závažná a týkají se velkého počtu finančních subjektů ve více členských státech, by měl hlavní orgán dohledu požádat příslušné orgány o sdílení výsledků tohoto posouzení. Aby byly co nejlépe využity zdroje příslušných orgánů, měl by hlavní orgán dohledu při žádosti o poskytnutí výsledků tohoto posouzení vždy zohlednit, že cílem těchto žádostí je vyhodnotit provádění opatření a nápravných opatření kritických poskytovatelů služeb IKT z řad třetích stran.

(9) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([2]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 22. července 2024.

(10) Toto nařízení vychází z návrhu regulačních technických norem předloženého Komisi evropskými orgány dohledu.

(11) Společný výbor evropských orgánů dohledu uspořádal o návrzích regulačních technických norem, z nichž toto nařízení vychází, otevřené veřejné konzultace, provedl analýzu potenciálních souvisejících nákladů a přínosů a vyžádal si stanovisko skupiny subjektů působících v bankovnictví zřízené na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([3]), skupiny subjektů působících v oblasti pojištění a zajištění a skupiny subjektů působících v oblasti zaměstnaneckého penzijního pojištění zřízených na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ([4]) a skupiny subjektů působících v oblasti cenných papírů a trhů zřízené na základě článku 37 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ([5]),

([2]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Informace, jež mají být předloženy v žádosti poskytovatelem služeb IKT z řad třetích stran, jenž má být určen za kritického

1. Poskytovatel služeb informačních a komunikačních technologií (IKT) z řad třetích stran, jenž má být určen za kritického podle čl. 31 odst. 1 písm. a) nařízení (EU) 2022/2554, předloží v odůvodněné žádosti o dobrovolnou účast podle čl. 31 odst. 11 nařízení (EU) 2022/2554 následující informace:

a) název právnické osoby;

b) identifikační kód právnické osoby;

c) jméno kontaktní osoby a kontaktní údaje kritického poskytovatele služeb IKT z řad třetích stran;

d) zemi, kde má právnická osoba sídlo;

e) popis podnikové struktury zahrnující alespoň informace o mateřské společnosti a dalších spřízněných podnicích poskytujících služby IKT finančním subjektům Unie. Tyto informace v příslušných případech zahrnují:

   i) název právnických osob;

   ii) identifikační kód právnické osoby;

   iii) zemi, kde má právnická osoba sídlo;

f) odhad tržního podílu poskytovatele služeb IKT z řad třetích stran ve finančním sektoru Unie a odhad tržního podílu podle typu finančního subjektu podle čl. 2 odst. 1 nařízení (EU) 2022/2554 k roku podání žádosti o určení poskytovatele jakožto kritického a k roku předcházejícímu této žádosti;

g) popis každé služby IKT poskytované finančním subjektům Unie, včetně:

   i) popisu povahy činnosti a typu služeb IKT poskytovaných finančním subjektům;

   ii) seznamu funkcí finančních subjektů podporovaných poskytovanými službami IKT, je-li k dispozici;

   iii) informací o tom, zda služby IKT poskytované finančním subjektům podporují zásadní nebo důležité funkce, jsou-li k dispozici;

h) seznam finančních subjektů, které využívají služby IKT poskytované poskytovatelem služeb IKT z řad třetích stran, včetně následujících informací o každém z obsluhovaných finančních subjektů, jsou-li k dispozici:

   i) názvu právnické osoby;

   ii) identifikačního kódu právnické osoby, je-li poskytovateli služeb IKT z řad třetích stran znám;

   iii) typu finančního subjektu podle čl. 2 odst. 1 nařízení (EU) 2022/2554;

   iv) místa, odkud jsou služby IKT této konkrétní právnické osobě poskytovány;

i) seznam kritických poskytovatelů služeb IKT z řad třetích stran uvedených v posledním dostupném seznamu těchto poskytovatelů zveřejněném evropskými orgány dohledu podle čl. 31 odst. 9 nařízení (EU) 2022/2554, kteří využívají služeb poskytovaných žadatelem, je-li k dispozici;

j) vlastní posouzení, pokud jde o:

   i) míru nahraditelnosti každé služby IKT poskytované žadatelem s ohledem na následující prvky:

      — podíl poskytovatele služeb IKT z řad třetích stran na trhu ve finančním sektoru Unie,

— počet známých relevantních konkurentů podle druhu služeb IKT nebo skupiny služeb IKT,

— popis specifik týkajících se nabízených služeb IKT, též v souvislosti s jakoukoli chráněnou technologií, nebo specifických rysů organizace nebo činnosti poskytovatele služeb IKT z řad třetích stran;

ii) informace o dostupnosti alternativních poskytovatelů služeb IKT z řad třetích stran, kteří poskytují stejné služby IKT jako poskytovatel služeb IKT z řad třetích stran, který žádost předkládá;

k) informace o budoucí obchodní strategii v souvislosti s poskytováním služeb IKT a infrastruktury finančním subjektům v Unii, včetně jakýchkoli plánovaných změn ve struktuře skupiny nebo struktuře řízení, vstupu na nové trhy nebo provozování nových činností;

l) určení subdodavatelů poskytovatele služeb IKT z řad třetích stran, kteří byli určeni za kritické poskytovatele služeb IKT z řad třetích stran;

m) jakékoli další důvody, které jsou relevantní pro to, aby byl poskytovatel služeb IKT z řad třetích stran na základě své žádosti určen za kritického.

2. Je-li poskytovatel služeb IKT z řad třetích stran součástí skupiny, informace uvedené v odstavci 1 se poskytují ve vztahu ke službám IKT poskytovaným danou skupinou jako celkem.

Článek 2

Obsah, struktura a formát informací, které mají být předloženy, zpřístupněny nebo oznámeny kritickými poskytovateli služeb IKT z řad třetích stran

1. Kritičtí poskytovatelé služeb IKT z řad třetích stran poskytnou hlavnímu orgánu dohledu na jeho žádost veškeré informace, které jsou nezbytné k tomu, aby mohl hlavní orgán dohledu plnit své povinnosti v oblasti dohledu v souladu s požadavky nařízení (EU) 2022/2554.

2. Informace uvedené v odstavci 1 zahrnují mimo jiné:

a) informace o ujednáních a kopie smluvních dokumentů mezi:

i) kritickým poskytovatelem služeb IKT z řad třetích stran a finančními subjekty uvedenými v čl. 2 odst. 1 nařízení (EU) 2022/2554;

ii) kritickým poskytovatelem služeb IKT z řad třetích stran a jeho subdodavateli s cílem zachytit technologický hodnotový řetězec služeb IKT poskytovaných finančním subjektům v Unii;

b) informace o organizační struktuře a struktuře skupiny kritického poskytovatele služeb IKT z řad třetích stran, včetně identifikace všech subjektů patřících do stejné skupiny, které přímo či nepřímo poskytují služby IKT finančním subjektům v Unii;

c) informace o hlavních akcionářích, včetně jejich struktury a zeměpisného rozložení, kteréhokoli z následujících subjektů:

i) subjekty, které drží, výhradně nebo společně se svými propojenými subjekty, 25 % nebo více kapitálu nebo hlasovacích práv kritického poskytovatele služeb IKT z řad třetích stran;

ii) subjekty, které mají právo jmenovat nebo odvolat většinu členů správního, řídícího nebo kontrolního orgánu kritického poskytovatele služeb IKT z řad třetích stran;

iii) subjekty, které na základě dohody kontrolují většinu hlasovacích práv akcionářů nebo členů kritického poskytovatele služeb IKT z řad třetích stran;

d) informace o tržním podílu kritického poskytovatele služeb IKT z řad třetích stran podle druhu služeb na relevantních trzích, kde působí;

e) informace o interních systémech správy a řízení kritického poskytovatele služeb IKT z řad třetích stran, včetně struktury s rozdělením odpovědnosti za řízení a pravidel odpovědnosti;

f) zápisy z jednání řídícího orgánu a všech dalších příslušných interních výborů kritického poskytovatele služeb IKT z řad třetích stran, které se jakýmkoli způsobem týkají činností a rizik souvisejících se službami IKT třetích stran podporujícími funkce finančních subjektů v Unii;

g) informace o bezpečnosti IKT kritického poskytovatele služeb IKT z řad třetích stran, včetně příslušných strategií, cílů, politik, postupů, protokolů, procesů, kontrolních opatření na ochranu citlivých údajů, kontrol přístupu, postupů šifrování, plánů reakce na incidenty a informací o dodržování všech příslušných předpisů a případně vnitrostátních a mezinárodních norem;

h) informace o technických a organizačních opatřeních k zajištění ochrany a důvěrnosti údajů včetně osobních a jiných než osobních údajů, zavedených kontrolních opatřeních na ochranu citlivých údajů, kontrolách přístupu, postupech šifrování a plánu reakce na narušení bezpečnosti údajů; pokud se na poskytovatele služeb IKT z řad třetích stran v souvislosti se zpracováním osobních údajů vztahují právní předpisy třetích zemí, včetně žádosti o přístup vlády třetí země, pak také seznam těchto zemí a příslušných právních předpisů;

i) informace o mechanismech, které kritický poskytovatel služeb IKT z řad třetích stran nabízí finančním subjektům Unie pro přenositelnost dat a přenositelnost a interoperabilitu aplikací;

j) informace o umístění datových center a výrobních středisek IKT používaných pro účely poskytování služeb finančním subjektům, včetně seznamu všech příslušných prostor a zařízení kritického poskytovatele služeb IKT z řad třetích stran, a to i mimo Unii;

k) informace o poskytování služeb kritickým poskytovatelem služeb IKT z řad třetích stran ze třetí země, včetně informací o příslušných právních předpisech, které se vztahují na osobní a jiné než osobní údaje zpracovávané poskytovatelem služeb IKT z řad třetích stran;

l) informace o opatřeních přijatých k řešení rizik vyplývajících z poskytování služeb IKT kritickým poskytovatelem služeb IKT z řad třetích stran a jeho subdodavateli ze třetích zemí;

m) informace o rámci pro řízení rizik a o rámci pro řízení incidentů, včetně politik, postupů, nástrojů, mechanismů a systémů správy a řízení kritického poskytovatele služeb IKT z řad třetích stran a jeho subdodavatelů, včetně seznamu a popisu významných incidentů s přímým nebo nepřímým dopadem na finanční subjekty v Unii, včetně příslušných podrobností pro určení významu incidentu pro finanční subjekty a posouzení možných přeshraničních dopadů;

n) informace o rámci pro řízení změn, včetně politik, postupů a kontrolních mechanismů kritického poskytovatele služeb IKT z řad třetích stran a jeho subdodavatelů;

o) informace o celkovém rámci pro reakci a obnovu kritického poskytovatele služeb IKT z řad třetích stran, včetně plánů zachování provozu a souvisejících opatření a postupů, politiky životního cyklu vývoje softwaru, plánů reakce a obnovy a souvisejících opatření a postupů a opatření a postupů pro zálohování;

p) informace o sledování výkonnosti, monitorování bezpečnosti a sledování incidentů, jakož i informace o mechanismech podávání zpráv týkajících se kvality služeb, incidentů a dodržování sjednaných dohod o úrovni služeb (SLA) a cílů týkajících se úrovně služeb (SLO) nebo podobných ujednání mezi kritickými poskytovateli služeb IKT z řad třetích stran a finančními subjekty v Unii;

q) informace o rámci pro řízení IKT z řad třetích stran, který uplatňuje kritický poskytovatel služeb IKT z řad třetích stran, včetně strategií, politik, postupů, procesů a kontrolních mechanismů, včetně podrobností o uplatňování náležité péče a posouzení rizik, které kritický poskytovatel služeb IKT z řad třetích stran provedl u svých subdodavatelů před uzavřením smlouvy s nimi, a o sledování jejich spolupráce se zohledněním všech relevantních rizik týkajících se IKT a protistrany;

r) výpisy z monitorovacích a skenovacích systémů kritického poskytovatele služeb IKT z řad třetích stran a jeho subdodavatelů, zahrnující mimo jiné monitorování sítě, monitorování serverů, monitorování aplikací, monitorování zabezpečení, skenování zranitelností, správu protokolů, monitorování výkonu, řízení incidentů a měření s ohledem na cíle spolehlivosti, jako jsou SLO;

s) výpisy z jakéhokoli produkčního, předprodukčního a testovacího systému nebo aplikace, které používá kritický poskytovatel služeb IKT z řad třetích stran a jeho subdodavatelé k přímému nebo nepřímému poskytování služeb finančním subjektům v Unii;

t) zprávy o dodržování předpisů a dostupné zprávy o auditu, jakož i veškerá příslušná zjištění auditu, včetně auditů provedených vnitrostátními orgány v Unii a mimo Unii, pokud dohody o spolupráci s příslušnými orgány takovou výměnu informací umožňují, nebo osvědčení, kterých dosáhl kritický poskytovatel služeb IKT z řad třetích stran nebo jeho subdodavatelé, včetně zpráv interních a externích auditorů, osvědčení nebo posouzení souladu s odvětvovými normami. Patří sem informace o jakémkoli typu dostupného nezávislého testování odolnosti systémů IKT kritického poskytovatele služeb IKT z řad třetích stran, včetně jakéhokoli typu penetračního testování na základě hrozeb, které poskytovatel služeb IKT z řad třetích stran provedl;

u) informace o všech hodnoceních provedených kritickým poskytovatelem služeb IKT z řad třetích stran, na jeho žádost nebo jeho jménem, která hodnotí vhodnost a bezúhonnost osob zastávajících klíčové pozice u kritického poskytovatele služeb IKT z řad třetích stran;

v) informace o jakémkoli plánu nápravných opatření k řešení doporučení podle článku 3 a příslušné související informace, které potvrzují, že náprava byla provedena;

w) informace o dostupných programech školení zaměstnanců a programech zvyšování povědomí o bezpečnosti, včetně případných informací o investicích, zdrojích a metodách kritického poskytovatele služeb IKT z řad třetích stran, pokud jde o školení jeho zaměstnanců v oblasti nakládání s citlivými finančními údaji a udržování vysoké úrovně bezpečnosti;

x) informace o činnostech kritického poskytovatele služeb IKT z řad třetích stran a finanční výkazy, včetně informací o rozpočtu a zdrojích souvisejících s IKT a bezpečností.

Článek 3

Informace od kritických poskytovatelů služeb IKT z řad třetích stran po vydání doporučení

1. Kritický poskytovatel služeb IKT z řad třetích stran předloží hlavnímu orgánu dohledu zprávu obsahující plán nápravných opatření v souvislosti s doporučeními a nápravnými opatřeními, která kritický poskytovatel služeb IKT z řad třetích stran plánuje provést s cílem zmírnit rizika uvedená v doporučeních podle čl. 35 odst. 1 písm. d) nařízení (EU) 2022/2554. Zpráva musí být v souladu s časovým rámcem, který hlavní orgán dohledu stanovil pro každé doporučení.

2. Aby bylo možné sledovat provádění opatření, která byla přijata, nebo nápravných opatření, která byla provedena kritickým poskytovatelem služeb IKT z řad třetích stran v souvislosti s obdrženými doporučeními, předloží kritický poskytovatel služeb IKT z řad třetích stran na požádání hlavnímu orgánu dohledu:

a) průběžné zprávy o pokroku a související podpůrné dokumenty, v nichž je uveden pokrok při provádění opatření a kroků uvedených ve zprávě, kterou kritický poskytovatel služeb IKT z řad třetích stran poskytl hlavnímu orgánu dohledu v časovém rámci stanoveném hlavním orgánem dohledu;

b) závěrečné zprávy a související podpůrné dokumenty, v nichž jsou uvedena opatření, která byla přijata, nebo nápravná opatření, která kritický poskytovatel služeb IKT z řad třetích stran provedl za účelem zmírnění rizik uvedených v obdržených doporučeních.

Článek 4

Struktura a formát informací poskytovaných kritickými poskytovateli služeb IKT z řad třetích stran

1. Kritický poskytovatel služeb IKT z řad třetích stran poskytne hlavnímu orgánu dohledu požadované informace prostřednictvím vyhrazených bezpečných elektronických kanálů, které hlavní orgán dohledu uvedl ve své žádosti, a ve formě stanovené hlavním orgánem dohledu.

2. Při poskytování informací hlavnímu orgánu dohledu kritičtí poskytovatelé služeb IKT z řad třetích stran:

a) dodržují strukturu uvedenou hlavním orgánem dohledu v jeho žádosti o informace;

b) jasně určí, kde se příslušná informace v předložené dokumentaci nachází.

3. Informace, které kritický poskytovatel služeb IKT z řad třetích stran předkládá, zpřístupňuje nebo oznamuje hlavnímu orgánu dohledu, jsou v jazyce obvyklém v oblasti mezinárodních financí.

Článek 5

Šablona pro poskytování informací o subdodavatelských ujednáních

Kritický poskytovatel služeb IKT z řad třetích stran, který je povinen sdílet informace o subdodavatelských ujednáních, poskytne informace hlavnímu orgánu dohledu podle šablony uvedené v příloze.

Článek 6

Posouzení rizik uvedených v doporučeních hlavního orgánu dohledu ze strany příslušných orgánů

1. Příslušný orgán v rámci dohledu nad finančními subjekty posoudí dopad na finanční subjekty opatření přijatých kritickým poskytovatelem služeb IKT z řad třetích stran na základě doporučení hlavního orgánu dohledu v souladu se zásadou proporcionality.

2. Při provádění posouzení uvedeného v odstavci 1 vezme příslušný orgán v úvahu všechny následující prvky:

a) přiměřenost a soudržnost opravných a nápravných opatření zavedených finančními subjekty ke zmírnění rizik uvedených v doporučeních;

b) posouzení provedené hlavním orgánem dohledu ohledně dodržování opatření a kroků obsažených ve zprávě ze strany kritického poskytovatele služeb IKT z řad třetích stran, pokud má dopad na expozici finančních subjektů v jeho působnosti rizikům uvedeným v doporučeních;

c) stanovisko všech ostatních příslušných orgánů, které byly konzultovány v souladu s čl. 42 odst. 5 nařízení (EU) 2022/2554;

d) to, zda hlavní orgán dohledu považoval opatření a nápravná opatření zavedená kritickým poskytovatelem služeb IKT z řad třetích stran za přiměřená ke zmírnění expozice finančních subjektů v jeho působnosti rizikům uvedeným v doporučeních.

3. Na žádost hlavního orgánu dohledu poskytne příslušný orgán v přiměřené lhůtě výsledky posouzení uvedeného v odstavci 1. Při vyžádání výsledků tohoto posouzení hlavní orgán dohledu zohlední zásadu proporcionality a rozsah rizik spojených s doporučeními, včetně přeshraničních dopadů těchto rizik, pokud mají dopad na finanční subjekty působící ve více než jednom členském státě.

4. Příslušný orgán v relevantních případech požádá finanční subjekty o poskytnutí veškerých informací nezbytných k provedení posouzení uvedeného v odstavci 1.

Článek 7

Vstup v platnost

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

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

V Bruselu dne 24. října 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA

ŠABLONA PRO SDÍLENÍ INFORMACÍ O SUBDODAVATELSKÝCH UJEDNÁNÍCH

Kategorie údajů	Klíčové údaje
Obecné informace	— Název kritického poskytovatele služeb IKT z řad třetích stran — Identifikační kód kritického poskytovatele služeb IKT z řad třetích stran — Jméno kontaktní osoby a kontaktní údaje kritického poskytovatele služeb IKT z řad třetích stran — Datum předložení šablony
Přehled subdodavatelských ujednání	— Zmapování subdodavatelských ujednání, včetně stručného popisu účelu a rozsahu subdodavatelských vztahů (včetně uvedení úrovně kritičnosti nebo důležitosti subdodavatelských ujednání pro kritického poskytovatele služeb IKT z řad třetích stran) — Specifikace a popis druhů subdodavatelských služeb IKT a jejich význam pro služby IKT poskytované finančním subjektům v souladu s prováděcími technickými normami přijatými podle čl. 28 odst. 9 nařízení (EU) 2022/2554 — Při specifikaci druhů služeb IKT se řiďte seznamem v příloze IV prováděcích technických norem přijatých podle čl. 28 odst. 9 nařízení (EU) 2022/2554
Informace o subdodavatelích	— Název a údaje o právnické osobě (včetně identifikačního kódu) u každého subdodavatele — Kontaktní údaje pracovníků odpovědných za jednotlivé subdodavatelské vztahy ve struktuře řízení kritického poskytovatele služeb IKT z řad třetích stran — Přehled odborných znalostí, zkušeností a kvalifikace každého subdodavatele v souvislosti s nasmlouvanými službami IKT
Popis služeb poskytovaných subdodavateli	— Podrobný popis konkrétních služeb IKT poskytovaných jednotlivými subdodavateli — Rozdělení odpovědností a úkolů přidělených subdodavatelům s podrobným popisem jednotlivých rolí v různých fázích procesů IKT — Informace o úrovni přístupu subdodavatelů k osobním či jinak citlivým údajům nebo systémům týkajícím se služeb IKT poskytovaných finančním subjektům — Informace o lokalitách, z nichž jsou služby subdodavatelů poskytovány, a o opatřeních přijatých k řešení rizik vyplývajících ze služeb poskytovaných mimo Unii
Správa a řízení subdodávek a dohled nad nimi	— Popis zavedeného smluvního a řídicího rámce pro řízení subdodavatelských vztahů, včetně ustanovení omezujících používání citlivých údajů — Vysvětlení postupů pro výběr, zapojení a monitorování subdodavatelů — Přehled měřítek výkonnosti, cílů a dohod o úrovni služeb a klíčových výkonnostních ukazatelů používaných k hodnocení výkonnosti a monitorování spolehlivosti subdodavatelů
Řízení rizik a zajišťování souladu s předpisy	— Posouzení rizikových profilů subdodavatele a potenciálního dopadu na služby IKT poskytované finančním subjektům — Vysvětlení opatření ke zmírnění rizik zavedených k řešení rizik souvisejících se subdodávkami — Podrobnosti o tom, jak subdodavatel dodržuje příslušné předpisy, včetně předpisů o ochraně údajů a odvětvových norem

Kategorie údajů	Klíčové údaje
Plánování zachování provozu a pohotovostní plánování	— Přehled plánů subdodavatele pro zachování provozu a plánů reakce a obnovy — Popis zavedených opatření k zajištění kontinuity služeb v případě přerušení nebo ukončení smlouvy ze strany subdodavatele — Četnost testů plánů zachování provozu a plánů reakce a obnovy ze strany subdodavatelů, data provedených testů za poslední tři roky a upřesnění, zda se těchto testů účastnil kritický poskytovatel služeb IKT z řad třetích stran
Podávání zpráv	— Popis mechanismů podávání zpráv a četnost podávání zpráv mezi kritickým poskytovatelem služeb IKT z řad třetích stran a jeho subdodavateli
Náprava a řízení incidentů	— Přehled postupů pro řešení incidentů, narušení nebo nedodržení předpisů v souvislosti se subdodavateli
Osvědčení a audity	— Informace o všech osvědčeních, nezávislých auditech nebo hodnoceních provedených u subdodavatelů za účelem ověření jejich bezpečnostních kontrol, standardů kvality nebo dodržování právních předpisů — Datum a četnost auditů subdodavatelů prováděných kritickým poskytovatelem služeb IKT z řad třetích stran