Úřední věstník
Evropské unie

CS
Řada L

2024/1773

25.6.2024

# NAŘÍZENÍ KOMISE V PŘENESENÉ PRAVOMOCI (EU) 2024/1773

**ze dne 13. března 2024,**

**kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) 2022/2554, pokud jde o regulační technické normy upřesňující podrobný obsah politiky týkající se smluvních ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran**

**(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. 28 odst. 10 třetí pododstavec uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Rámec digitální provozní odolnosti finančního sektoru vytvořený nařízením (EU) 2022/2554 vyžaduje, aby finanční subjekty stanovily určité klíčové zásady, které určují řízení rizika v oblasti IKT spojeného s třetími stranami a které jsou obzvláště důležité v případech, kdy finanční subjekty využívají poskytovatele služeb IKT z řad třetích stran na podporu svých zásadních nebo důležitých funkcí.

(2) Finanční subjekty musí jakožto součást svého rámce pro řízení rizika v oblasti IKT přijmout a pravidelně přezkoumávat strategii pro riziko v oblasti IKT spojené s třetími stranami. V souladu s čl. 28 odst. 2 nařízení (EU) 2022/2554 musí tato strategie obsahovat zásady využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran. Má se uplatňovat na individuálním a případně subkonsolidovaném či konsolidovaném základě.

(3) Finanční subjekty se značně liší velikostí, strukturou a vnitřní organizací a také povahou a složitostí svých činností a operací. Tuto rozmanitost je třeba vzít v úvahu při ukládání určitých základních regulatorních požadavků, které mají být vhodné pro všechny finanční subjekty, aby tyto subjekty mohly vypracovat politiku týkající se smluvních ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran (dále jen „politika“), a je třeba zajistit, aby tyto požadavky byly uplatňovány přiměřeným způsobem.

(4) Jsou-li finanční subjekty součástí skupiny, měl by tedy mateřský podnik, který je odpovědný za sestavování konsolidovaných nebo subkonsolidovaných účetních závěrek skupiny, zajistit, aby byla politika v rámci celé skupiny uplatňována konzistentně a jednotně.

(5) Při uplatňování politiky by poskytovatelé služeb IKT v rámci skupiny, včetně těch v plném nebo společném vlastnictví finančních subjektů v rámci téhož institucionálního systému ochrany, měli být považováni za poskytovatele služeb IKT z řad třetích stran. Rizika, která poskytovatelé služeb IKT v rámci skupiny představují, se mohou lišit, avšak podle nařízení (EU) 2022/2554 se na ně vztahují stejné požadavky. Stejně tak by se politika měla vztahovat na subdodavatele, kteří poskytují služby IKT podporující zásadní nebo důležité funkce nebo podstatné součásti těchto služeb poskytovatelům služeb IKT z řad třetích stran, v případě, že existuje řetězec poskytovatelů služeb IKT z řad třetích stran.

(6) Konečná odpovědnost vedoucího orgánu za řízení rizika finančního subjektu v oblasti IKT je zastřešujícím principem, jenž platí i v případě využívání poskytovatelů služeb IKT z řad třetích stran. Tato odpovědnost by dále měla být vyjádřena nepřetržitým angažováním vedoucího orgánu v kontrole a sledování řízení rizika v oblasti IKT, včetně přijetí politiky a jejího přezkumu prováděného alespoň jednou ročně.

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

(7) Aby bylo zajištěno náležité oznamování vedoucímu orgánu, měla by být v politice jasně vymezena a určena interní odpovědnost za schvalování, správu, kontrolu a dokumentaci smluvních ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran (dále jen „smluvní ujednání"), včetně služeb IKT poskytovaných na základě smluvních ujednání uvedených v čl. 28 odst. 1 písm. a) nařízení (EU) 2022/2554.

(8) Aby bylo možné zohlednit všechna možná rizika, jež mohou vzniknout v souvislosti s uzavíráním smluv o službách IKT podporujících zásadní nebo důležité funkce, měla by struktura politiky kopírovat všechny kroky z každé hlavní fáze životního cyklu smluvních ujednání s poskytovateli z řad třetích stran.

(9) Ke zmírnění identifikovaných rizik by v politice mělo být stanoveno, jak probíhá plánování smluvních ujednání, včetně posouzení rizik, náležité péče a procesu schvalování nových nebo podstatných změn těchto smluvních ujednání. Za účelem řízení rizik, jež mohou vzniknout před uzavřením smluvního ujednání s poskytovatelem služeb IKT z řad třetích stran, by v politice měl být stanoven vhodný a přiměřený postup výběru potenciálních poskytovatelů služeb IKT z řad třetích stran a posouzení jejich vhodnosti a mělo by v ní být vyžadováno, aby finanční subjekt zohlednil seznam určitých prvků, které by poskytovatelé služeb IKT z řad třetích stran měli mít zavedeny. Na seznam by měly být zařazeny prvky, které se týkají podnikatelské pověsti poskytovatelů služeb a jejich finančních, lidských a technických zdrojů, zabezpečení informací, organizační struktury, včetně řízení rizik, a interních kontrol.

(10) Aby se v případě, že jsou služby IKT podporující zásadní nebo důležité funkce poskytovány poskytovateli služeb IKT z řad třetích stran, zajistilo řádné řízení rizik, měla by politika zahrnovat informace o plnění, sledování a správě smluvních ujednání, a to v relevantních případech i na konsolidované a subkonsolidované úrovni. To zahrnuje požadavky na smluvní doložky o vzájemných povinnostech finančních subjektů a poskytovatelů služeb IKT z řad třetích stran, které by měly být stanoveny písemně. Aby se zajistil účinný dohled a podpořila odolnost v případě změn obchodního modelu nebo podnikatelského prostředí, měla by politika zajistit právo finančních subjektů nebo určených třetích stran a příslušných orgánů na kontroly a přístup k informacím a měla by také blíže upřesnit strategie ukončení smluvního vztahu a procesy ukončení smluvního ujednání.

(11) V rozsahu, v jakém poskytovatelé služeb IKT z řad třetích stran zpracovávají osobní údaje, nejsou politikou ani jakýmikoli smluvními ujednáními dotčeny povinnosti vyplývající z nařízení Evropského parlamentu a Rady (EU) 2016/679 ([2]), například mít uzavřenou písemnou smlouvu, v níž je popsáno zpracování osobních údajů, požadavek zajistit zabezpečení zpracování osobních údajů a stanoveny všechny ostatní prvky požadované uvedeným nařízením, a politika a smluvní ujednání by tyto povinnosti měly doplňovat.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Společný výbor evropských orgánů dohledu uvedený v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 ([3]), v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010 ([4]) a v článku 54 nařízení Evropského parlamentu a Rady (EU) č. 1095/2010 ([5]) uskutečnil o návrzích regulačních technických norem, z nichž toto nařízení vychází, otevřené veřejné konzultace, analyzoval potenciální náklady a přínosy navrhovaných norem a požádal o stanovisko skupinu subjektů působících v bankovnictví zřízenou podle článku 37 nařízení (EU) č. 1093/2010, skupinu subjektů působících v oblasti pojištění a zajištění a skupinu subjektů působících v oblasti zaměstnaneckého penzijního pojištění zřízené podle článku 37 nařízení (EU) č. 1094/2010 a skupinu subjektů působících v oblasti cenných papírů a trhů zřízenou podle článku 37 nařízení (EU) č. 1095/2010.

(13) V souladu s čl. 42 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ([6]) byl konzultován evropský inspektor ochrany údajů, který vydal stanovisko dne 24. ledna 2024,

PŘIJALA TOTO NAŘÍZENÍ:

*Článek 1*

**Celkový rizikový profil a složitost**

Politika využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran (dále jen „politika“) zohledňuje velikost a celkový rizikový profil finančního subjektu, povahu a rozsah jeho služeb, činností a operací a prvky zvýšené nebo snížené složitosti těchto služeb, činností a operací, včetně prvků, jež se týkají:

a) druhu služeb IKT, jež jsou zahrnuty do smluvního ujednání o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran (dále jen „smluvní ujednání“) mezi finančním subjektem a poskytovatelem služeb IKT z řad třetích stran;

b) místa poskytovatele služeb IKT z řad třetích stran nebo místa jeho mateřské společnosti;

c) toho, zda služby IKT podporující zásadní nebo důležité funkce poskytuje poskytovatel služeb IKT z řad třetích stran, který se nachází v členském státě, nebo ve třetí zemi, přičemž se přihlíží také k místu, odkud jsou služby IKT poskytovány, a místu, kde jsou zpracovávána a uchovávána data;

d) povahy údajů sdílených s poskytovatelem služeb IKT z řad třetích stran;

e) toho, zda je poskytovatel služeb IKT z řad třetích stran součástí téže skupiny jako finanční subjekt, kterému služby poskytuje;

([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).

([6]) 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).

f) využívání poskytovatelů služeb IKT z řad třetích stran, kteří mají povolení od příslušného orgánu v členském státě, jsou jím zaregistrováni nebo podléhají jeho dohledu či dozoru anebo se na ně vztahuje rámec dohledu podle kapitoly V oddílu II nařízení (EU) 2022/2554, a využívání poskytovatelů služeb IKT z řad třetích stran, kteří toto nesplňují;

g) využívání poskytovatelů služeb IKT z řad třetích stran, kteří mají povolení od orgánu dohledu ve třetí zemi, jsou jím zaregistrováni nebo podléhají jeho dohledu či kontrole, a využívání poskytovatelů služeb IKT z řad třetích stran, kteří toto nesplňují;

h) toho, zda je poskytování služeb IKT podporujících zásadní nebo důležité funkce koncentrováno u jediného poskytovatele služeb IKT z řad třetích stran, nebo u malého počtu takových poskytovatelů služeb;

i) možnosti přenést služby IKT podporující zásadní nebo důležité funkce k jinému poskytovateli služeb IKT z řad třetích stran, a to i v důsledku technologických specifik;

j) potenciálního dopadu narušení poskytování služeb IKT podporujících zásadní nebo důležité funkce na kontinuitu činností finančního subjektu a na dostupnost jeho služeb.

*Článek 2*

**Uplatňování v rámci skupiny**

V případech, kdy se toto nařízení použije na subkonsolidovaném či konsolidovaném základě, mateřský podnik, který je odpovědný za sestavování konsolidovaných nebo subkonsolidovaných účetních závěrek skupiny, zajistí, aby byla politika uplatňována konzistentně ve všech finančních subjektech, jež jsou součástí skupiny, a aby byla přiměřená pro účely účinného uplatňování tohoto nařízení na všech příslušných úrovních skupiny.

*Článek 3*

**Systém správy a řízení**

1. Vedoucí orgán politiku alespoň jednou ročně přezkoumá a v případě potřeby ji aktualizuje. Změny politiky se provádějí včas a co nejdříve je to v rámci příslušných smluvních ujednání možné. Plánovaný harmonogram jejich provedení finanční subjekt zdokumentuje.

2. V politice se stanoví metodika určování služeb IKT, které podporují zásadní nebo důležité funkce, nebo se na takovou metodiku uvede odkaz. V politice se rovněž stanoví, kdy má být toto posouzení provedeno a přezkoumáno.

3. V politice se jasně přiřadí vnitřní odpovědnost za schvalování, správu, kontrolu a dokumentaci příslušných smluvních ujednání a zajistí, aby byly v rámci finančního subjektu udržovány odpovídající dovednosti, zkušenosti a znalosti pro účinný dohled nad příslušnými smluvními ujednáními, včetně služeb IKT, které jsou na základě těchto ujednání poskytovány.

4. Aniž je dotčena konečná odpovědnost finančního subjektu za účinný dohled nad příslušnými smluvními ujednáními, požaduje se v rámci politiky, aby měl poskytovatel služeb IKT z řad třetích stran podle posouzení dostatečné zdroje k zajištění toho, aby finanční subjekt splňoval všechny právní a regulatorní požadavky týkající se poskytovaných služeb IKT podporujících zásadní nebo důležité funkce.

5. V politice se jasně určí funkce nebo vedoucí pracovník, kteří jsou odpovědní za sledování příslušných smluvních ujednání. V politice se stanoví, jak má tato funkce nebo tento vedoucí pracovník spolupracovat s kontrolními funkcemi, ledaže je jejich součástí, a vymezí kanály pro oznamování vedoucímu orgánu, včetně povahy informací, které se mají oznamovat, a dokumentů, které se mají předkládat. Stanoví se v ní rovněž četnost tohoto oznamování.

6. Politika zajistí, aby smluvní ujednání byla v souladu s:

a) rámcem pro řízení rizika v oblasti IKT uvedeným v článku 6 nařízení (EU) 2022/2554;

b) politikou zabezpečení informací uvedenou v čl. 9 odst. 4 nařízení (EU) 2022/2554;

c) politikou zachování provozu IKT uvedenou v článku 11 nařízení (EU) 2022/2554;

d) požadavky na hlášení incidentů stanovenými v článku 19 nařízení (EU) 2022/2554.

7. Politika vyžaduje, aby služby IKT podporující zásadní nebo důležité funkce poskytované poskytovateli služeb IKT z řad třetích stran podléhaly nezávislému přezkumu a byly zahrnuty do plánu auditu.

8. V politice se výslovně stanoví, že smluvní ujednání:

a) nezbavují finanční subjekt a jeho vedoucí orgán regulačních povinností a odpovědnosti vůči klientům;

b) nesmí bránit účinnému dohledu nad finančním subjektem a nesmí být v rozporu se žádnými omezeními služeb a činností z hlediska dohledu;

c) musí vyžadovat, aby poskytovatelé služeb IKT z řad třetích stran spolupracovali s příslušnými orgány;

d) musí vyžadovat, aby finanční subjekt, jeho auditoři a příslušné orgány měli účinný přístup k údajům a do prostor, které jsou spojeny s využíváním služeb IKT podporujících zásadní nebo důležité funkce.

*Článek 4*

**Hlavní fáze životního cyklu přijímání a využívání smluvních ujednání**

V politice se stanoví požadavky, včetně pravidel, povinností a procesů, pro každou hlavní fázi životního cyklu smluvního ujednání, které zahrnují alespoň:

a) povinnosti vedoucího orgánu, včetně jeho případného zapojení do procesu rozhodování o využívání služeb IKT podporujících zásadní nebo důležité funkce poskytovaných poskytovateli služeb IKT z řad třetích stran;

b) plánování smluvních ujednání, včetně posouzení rizik, náležité péče podle článků 5 a 6 a procesu schvalování nových nebo podstatných změn smluvních ujednání podle čl. 8 odst. 4;

c) zapojení obchodních útvarů, interních kontrol a dalších příslušných útvarů s ohledem na smluvní ujednání;

d) plnění, sledování a správu smluvních ujednání podle článků 7, 8 a 9, a to v relevantních případech i na konsolidované a subkonsolidované úrovni;

e) dokumentaci a vedení záznamů s ohledem na požadavky týkající se registru informací stanovené v čl. 28 odst. 3 nařízení (EU) 2022/2554;

f) strategie ukončení smluvního vztahu a procesy ukončení smluvního ujednání stanovené v článku 10.

*Článek 5*

**Posouzení rizik ex ante**

1. Politika vyžaduje, aby před uzavřením smluvního ujednání byly stanoveny požadavky obchodní činnosti finančního subjektu.

2. Politika vyžaduje, aby před uzavřením smluvního ujednání bylo provedeno posouzení rizik na úrovni finančního subjektu a v relevantních případech na konsolidované a subkonsolidované úrovni.

Při posuzování rizik se zohlední všechny příslušné požadavky stanovené v nařízení (EU) 2022/2554 a v platných odvětvových právních předpisech Unie. Zváží se zejména dopad poskytování služeb IKT podporujících zásadní nebo důležité funkce poskytovateli služeb IKT z řad třetích stran na finanční subjekt a všechna rizika, která poskytování těchto služeb IKT podporujících zásadní nebo důležité funkce poskytovateli služeb IKT z řad třetích stran představuje, včetně těchto rizik:

a) operační rizika;

b) právní rizika;

c) rizika v oblasti IKT;

d) reputační rizika;

e) rizika spojená s ochranou důvěrných nebo osobních údajů;

f) rizika spojená s dostupností údajů;

g) rizika spojená s místem, kde jsou údaje zpracovávány a uchovávány;

h) rizika spojená s místem poskytovatele služeb IKT z řad třetích stran;

i) rizika koncentrace IKT na úrovni subjektu.

*Článek 6*

**Náležitá péče**

1. V politice se stanoví vhodný a přiměřený postup výběru a posouzení potenciálních poskytovatelů služeb IKT z řad třetích stran s přihlédnutím k tomu, zda je daný poskytovatel služeb IKT z řad třetích stran poskytovatelem služeb IKT v rámci skupiny, a vyžaduje se v ní, aby finanční subjekt před uzavřením smluvního ujednání posoudil, zda poskytovatel služeb IKT z řad třetích stran:

a) má podnikatelskou pověst, dostatečné schopnosti, odborné znalosti a odpovídající finanční, lidské a technické zdroje, normy bezpečnosti informací, vhodnou organizační strukturu, řízení rizik a interní kontroly a v příslušných případech požadovaná povolení nebo registrace potřebné k tomu, aby byl schopen poskytovat služby IKT podporující zásadní nebo důležité funkce spolehlivě a odborně;

b) je schopen sledovat relevantní technologický vývoj a identifikovat nejlepší postupy v oblasti bezpečnosti IKT a ve vhodných případech je zavádět, aby měl účinný a spolehlivý rámec digitální provozní odolnosti;

c) k provádění služeb IKT podporujících zásadní nebo důležité funkce nebo podstatných součástí těchto služeb využívá nebo hodlá využívat subdodavatele IKT;

d) se nachází nebo zpracovává či uchovává data ve třetí zemi, a pokud tomu tak je, zda tento postup ovlivňuje úroveň operačních nebo reputačních rizik nebo rizika, že se ho dotknou omezující opatření, včetně embarg a sankcí, která mohou mít dopad na schopnost poskytovatele služeb IKT z řad třetích stran poskytovat služby IKT nebo na schopnost finančního subjektu tyto služby IKT přijímat;

e) souhlasí se smluvními ujednáními, která zajišťují, aby samotný finanční subjekt, určené třetí strany a příslušné orgány mohly účinně u poskytovatele služeb IKT z řad třetích stran provádět audity včetně auditů na místě;

f) jedná etickým a sociálně odpovědným způsobem, dodržuje lidská práva a práva dětí, včetně zákazu dětské práce, dodržuje platné zásady ochrany životního prostředí a zajišťuje odpovídající pracovní podmínky.

2. V politice se stanoví požadovaná úroveň ujištění o účinnosti rámce poskytovatelů služeb IKT z řad třetích stran pro řízení rizika v souvislosti se službami IKT podporujícími zásadní nebo důležité funkce, které má poskytovatel služeb IKT z řad třetích stran poskytovat. Politika vyžaduje, aby postup náležité péče zahrnoval posouzení toho, zda existují opatření ke zmírnění rizik a k zachování provozu, a způsobu, jakým je u poskytovatele služeb IKT z řad třetích stran zajištěno jejich fungování.

3. V politice se stanoví postup náležité péče při výběru a posuzování potenciálních poskytovatelů služeb IKT z řad třetích stran a určí, které z následujících prvků se mají použít k získání požadované úrovně ujištění o výkonnosti poskytovatele služeb IKT z řad třetích stran:

a) audity nebo nezávislá posouzení provedené samotným finančním subjektem nebo jeho jménem;

b) využití nezávislých auditních zpráv vypracovaných na žádost poskytovatele služeb IKT z řad třetích stran;

c) využití auditních zpráv vypracovaných interní auditní funkcí poskytovatele služeb IKT z řad třetích stran;

d) využití vhodných osvědčení vydaných třetími stranami;

e) využití dalších relevantních informací, jež má finanční subjekt k dispozici, nebo dalších informací poskytnutých poskytovatelem služeb IKT z řad třetích stran.

4. Finanční subjekty zajistí odpovídající úroveň ujištění o výkonnosti poskytovatele služeb IKT z řad třetích stran a zohlední přitom prvky uvedené v odst. 3 písm. a) až e). Je-li to vhodné, použije se více než jeden z prvků uvedených v uvedených písmenech.

*Článek 7*

**Střety zájmů**

1. V politice se stanoví vhodná opatření k identifikaci, prevenci a řešení skutečných nebo potenciálních střetů zájmů vznikajících v případě využívání poskytovatelů služeb IKT z řad třetích stran, která mají být přijata před uzavřením příslušných smluvních ujednání, a zavede průběžné sledování těchto střetů zájmů.

2. Pokud služby IKT podporující zásadní nebo důležité funkce poskytují poskytovatelé služeb IKT v rámci skupiny, stanoví se v politice, že rozhodnutí týkající se podmínek poskytování služeb IKT včetně finančních podmínek musí být objektivní.

*Článek 8*

**Smluvní doložky**

1. V politice se stanoví, že příslušná smluvní ujednání musí být vyhotovena písemně a musí obsahovat všechny prvky uvedené v čl. 30 odst. 2 a 3 nařízení (EU) 2022/2554. Politika rovněž zahrnuje prvky vztahující se k požadavkům uvedeným v čl. 1 odst. 1 písm. a) nařízení (EU) 2022/2554 a případně v dalších příslušných právních předpisech Unie a vnitrostátních právních předpisech.

2. V politice se stanoví, že v příslušných smluvních ujednáních musí být zakotveno právo finančního subjektu na přístup k informacím, na provádění kontrol a auditů a na provádění testů IKT. Za tímto účelem politika vyžaduje, aby finanční subjekt používal tyto metody, aniž je dotčena konečná odpovědnost finančního subjektu:

a) vlastní interní audit nebo audit prováděný určenou třetí stranou;

b) ve vhodných případech společné audity a společné testování IKT, včetně penetračního testování na základě hrozeb, které jsou organizovány společně s jinými finančními subjekty nebo podniky využívajícími na základě smlouvy služby IKT téhož poskytovatele služeb IKT z řad třetích stran a které jsou prováděny těmito finančními subjekty nebo podniky nebo jimi určenou třetí stranou;

c) ve vhodných případech osvědčení vydávaná třetími stranami;

d) ve vhodných případech auditní zprávy vypracovávané interně nebo třetími stranami a zpřístupňované poskytovatelem služeb IKT z řad třetích stran.

3. Finanční subjekt nesmí dlouhodobě spoléhat pouze na osvědčení uvedená v odst. 2 písm. c) nebo na auditní zprávy uvedené v písmenu d) téhož odstavce. Politika povoluje použití metod uvedených v odst. 2 písm. c) a d) pouze v případě, že finanční subjekt:

a) je spokojen s plánem auditu poskytovatele služeb IKT z řad třetích stran určeným pro příslušná smluvní ujednání;

b) zajistí, aby rozsah osvědčení nebo auditních zpráv pokrýval jím určené systémy a klíčové kontroly, a zajistí dodržování příslušných regulatorních požadavků;

c) průběžně důkladně posuzuje obsah osvědčení nebo auditních zpráv a ověřuje, že zprávy nebo osvědčení nejsou zastaralé;

d) zajistí, aby klíčové systémy a kontroly byly zahrnuty i do budoucích verzí osvědčení nebo auditní zprávy;

e) je spokojen se způsobilostí strany, jež vydává osvědčení nebo provádí audit;

f) je přesvědčen, že osvědčení jsou vydávána a audity jsou prováděny podle příslušných obecně uznávaných profesních standardů a zahrnují test provozní účinnosti zavedených klíčových kontrol;

g) má smluvní právo požadovat s četností, která je z hlediska řízení rizik přiměřená a oprávněná, změny rozsahu osvědčení nebo auditních zpráv za účelem zahrnutí dalších relevantních systémů a kontrol;

h) má smluvní právo provádět podle vlastního uvážení ve vztahu ke smluvním ujednáním individuální a společné audity a vykonávat tato práva v souladu s dohodnutou četností.

4. Politika zajistí, aby podstatné změny smluvního ujednání byly formalizovány v písemném dokumentu opatřeném datem a podpisy všech stran, a stanoví postup prodlužování smluvních ujednání.

*Článek 9*

**Sledování smluvních ujednání**

1. Politika vyžaduje, aby ve smluvních ujednáních byla stanovena opatření a klíčové ukazatele pro průběžné sledování výsledků poskytovatelů služeb IKT z řad třetích stran, včetně opatření ke sledování dodržování požadavků, jež se týkají důvěrnosti, dostupnosti, integrity a hodnověrnosti údajů a informací, a dodržování příslušných politik a postupů finančního subjektu ze strany poskytovatelů služeb IKT z řad třetích stran. V politice se rovněž stanoví opatření, která se uplatní v případě nedodržení dohod o úrovni služeb, a to případně včetně smluvních pokut.

2. V politice se stanoví způsob, jakým má finanční subjekt posuzovat, zda poskytovatelé služeb IKT z řad třetích stran, kteří jsou využíváni v souvislosti se službami IKT podporujícími zásadní nebo důležité funkce, splňují příslušné standardy výkonnosti a kvality v souladu se smluvním ujednáním a vlastními politikami finančního subjektu. Politika zejména zajistí, aby:

a) poskytovatelé služeb IKT z řad třetích stran podávali finančnímu subjektu náležité zprávy o svých činnostech a službách, včetně pravidelných zpráv, zpráv o incidentech, zpráv o poskytování služeb, zpráv o bezpečnosti IKT a zpráv o opatřeních k zachování provozu a o testování zachování provozu;

b) výsledky poskytovatelů služeb IKT z řad třetích stran byly posuzovány na základě klíčových ukazatelů výkonnosti, klíčových kontrolních ukazatelů, auditů, vlastních osvědčení a nezávislých přezkumů v souladu s rámcem finančního subjektu pro řízení rizika v oblasti IKT;

c) finanční subjekt získával od poskytovatelů služeb IKT z řad třetích stran další relevantní informace;

d) byl finanční subjekt v příslušných případech informován o incidentech souvisejících s IKT a o provozních nebo bezpečnostních incidentech souvisejících s platbami;

e) se prováděly nezávislý přezkum a audity za účelem ověření, že jsou dodržovány právní a regulatorní požadavky a zásady.

3. V politice se stanoví, že posouzení podle odstavce 2 se má zdokumentovat a výsledky se mají použít k aktualizaci posouzení rizik prováděného finančním subjektem podle článku 6.

4. V politice se stanoví vhodná opatření, která má finanční subjekt přijmout, pokud na straně poskytovatelů služeb IKT z řad třetích stran zjistí nedostatky, včetně incidentů souvisejících s IKT a provozních nebo bezpečnostních incidentů souvisejících s platbami, v poskytování služeb IKT podporujících zásadní nebo důležité funkce nebo v dodržování smluvních ujednání nebo právních požadavků. Rovněž se v ní stanoví, jakým způsobem se má provádění těchto opatření sledovat, aby se zajistilo jejich účinné splnění ve stanoveném časovém rámci, přičemž se zohlední závažnost daných nedostatků.

*Článek 10*

**Ukončení smluvních ujednání**

Politika obsahuje požadavky na zdokumentovaný plán ukončení smluvního vztahu vypracovávaný pro každé smluvní ujednání a na pravidelný přezkum a testování tohoto plánu. Při sestavování plánu ukončení smluvního vztahu se vezmou v úvahu:

a) nepředvídaná a přetrvávající přerušení služeb;

b) nevhodné či chybné poskytování služeb;

c) neočekávané ukončení smluvního ujednání.

Plán ukončení smluvního vztahu musí být realistický, proveditelný, založený na věrohodných scénářích a přiměřených předpokladech a musí mít předpokládaný harmonogram provádění slučitelný s podmínkami ukončení smluvního vztahu stanovenými ve smluvních ujednáních.

*Článek 11*

**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 13. března 2024.

*Za Komisi*
*předsedkyně*
Ursula VON DER LEYEN