30/09/2025
ESMA65-294529287-4737

Obecné pokyny

ohledně zajišťování cloudových služeb u externích poskytovatelů

Obsah

1 Oblast působnosti

Dotčené subjekty

1. Tyto obecné pokyny se vztahují na příslušné orgány a i) depozitáře alternativních investičních fondů uvedené v čl. 21 odst. 3 písm. c) a v čl. 21 odst. 3 třetím pododstavci směrnice o správcích alternativních investičních fondů, pokud nejsou finančními subjekty, na něž se vztahuje nařízení DORA, a ii) depozitáře SKIPCP uvedené v čl. 23 odst. 2 písm. c) směrnice o SKIPCP, pokud nejsou finančními subjekty, na něž se vztahuje nařízení DORA.[1]

Předmět

2. Tyto pokyny se vztahují na následující ustanovení:

   a) Pokud jde o depozitáře alternativních investičních fondů: čl. 21 směrnice o správcích alternativních investičních fondů; čl. 98 nařízení Komise v přenesené pravomoci (EU) č. 2013/231;

   b) Pokud jde o depozitáře SKIPCP: čl. 22, 22a a čl. 23 odst. 2 směrnice o SKIPCP; čl. 32 směrnice Komise 2010/43/EU; čl. 2 odst. 2 písm. j), čl. 3 odst. 1, čl. 13 odst. 2, čl. 15, 16 a 22 nařízení Komise v přenesené pravomoci (EU) č. 2016/438.

Časový rámec

3. Tyto obecné pokyny se použijí ode dne jejich zveřejnění na internetových stránkách orgánu ESMA ve všech úředních jazycích EU a na všechna ujednání o externím zajišťování cloudových služeb uzavřená, obnovená nebo pozměněná k tomuto datu nebo po něm.

4. S ohledem na uplatňování nařízení DORA se na finanční subjekty, na něž se nařízení DORA vztahuje a které jsou uvedeny v čl. 2 téhož nařízení, přestanou vztahovat předchozí obecné pokyny orgánu ESMA k outsourcingu poskytovatelů cloudových služeb. Na depozitáře alternativních investičních fondů a depozitáře SKIPCP uvedené v odstavci 1 výše se budou až do data zveřejnění těchto obecných pokynů na internetových stránkách orgánu ESMA ve všech úředních jazycích EU nadále vztahovat předchozí obecné pokyny orgánu ESMA k externímu zajišťování služeb poskytovateli cloudových služeb.

[1] Pokud jde o dohody o využívání cloudových služeb, finanční subjekty definované v čl. 2 odst. 1 a 2 nařízení Evropského parlamentu a Rady (EU) 2022/2554 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 DORA) podléhají zvláštním pravidlům stanoveným v nařízení DORA a souvisejících nařízeních Komise.

2 Odkazy na právní předpisy, zkratky a definice

2.1 Odkazy na právní předpisy

Nařízení o orgánu ESMA	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[2]
Směrnice o správcích alternativních investičních fondů	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[3]
Nařízení Komise v přenesené pravomoci (EU) č. 231/2013	Nařízení Komise v přenesené pravomoci (EU) č. 231/2013 ze dne 19. prosince 2012, kterým se doplňuje směrnice Evropského parlamentu a Rady 2011/61/EU, pokud jde o výjimky, obecné podmínky provozování činnosti, depozitáře, pákový efekt, transparentnost a dohled[4]
Směrnice o SKIPCP	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)[5]
Směrnice Komise 2010/43/EU	Směrnice Komise 2010/43/EU ze dne 1. července 2010, kterou se provádí směrnice Evropského parlamentu a Rady 2009/65/ES, pokud jde o organizační požadavky, střety zájmů, pravidla jednání, řízení rizik a obsah smlouvy mezi depozitářem a správcovskou společností[6]
DORA	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[7]

[2] Úř. věst. L 331, 15.12.2010, s. 84.
[3] Úř. věst. L 174, 1.7.2011, s. 1.
[4] Úř. věst. L 83, 22.3.2013, s. 1.
[5] Úř. věst. L 302, 17.11.2009, s. 32.
[6] Úř. věst. L 176, 10.7.2010, s. 42.
[7] *Úř. věst. L 333, 27.12.2022, s. 1–79*

Nařízení GDPR	Nařízení Evropského parlamentu a Rady 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)[8]

Zkratky

ESMA	Evropský orgán pro cenné papíry a trhy
EU	Evropská unie
PCS	poskytovatel cloudových služeb

Definice

funkce	znamená jakékoliv procesy, služby nebo činnosti;
zásadní nebo důležitá funkce	znamená jakékoliv funkce, jejichž nesprávné plnění nebo neplnění by vážně ohrozilo: a) plnění povinností podniku stanovených v příslušných právních předpisech; b) finanční výkonnost podniku nebo c) spolehlivost nebo kontinuitu hlavních služeb a činností podniku;
cloudové služby	znamená služby poskytované pomocí cloud computingu;
cloud computing neboli cloud[9]	znamená uspořádání umožňující síťový přístup k rozšiřitelnému a přizpůsobitelnému fondu fyzických nebo virtuálních zdrojů, které je možné sdílet (například serverů, operačních systémů, sítí, softwaru, aplikací a úložišť) poskytované k samoobslužnému provozu a správou na vyžádání.

[8] Úř. věst. L 119, 4.5.2016, s. 1.
[9] Pojem „cloud computing“ je často zkracován na „cloud“. Z důvodu snazší orientace se ve zbývající části tohoto dokumentu používá pojem „cloud“.

poskytovatel cloudových služeb	znamená třetí stranu poskytující cloudové služby v rámci ujednání o externím zajišťování cloudových služeb;
ujednání o externím zajišťování cloudových služeb	znamená ujednání v jakékoliv podobě, včetně dohody o pověření, mezi: (i) podnikem a PCS, podle kterého tento PCS vykonává funkci, kterou by jinak vykonával sám podnik, nebo (ii) podnikem a třetí stranou, která není PCS, ale která se významně spoléhá na to, že PCS bude vykonávat funkci, kterou by jinak podnik vykonával sám. V takovém případě je třeba odkaz na „PCS“ v těchto pokynech chápat jako odkaz na takovou třetí stranu.
další externí zajišťování	znamená situaci, kdy PCS dále přenáší externě zajišťovanou funkci (nebo její část) na jiného poskytovatele služeb v rámci ujednání o externím zajištění služeb;
model nasazení cloudu	znamená způsob, jakým může být cloud organizován na základě řízení a sdílení fyzických nebo virtuálních zdrojů. Mezi modely nasazení cloudu patří komunitní[10], hybridní[11], soukromé[12] a veřejné[13] cloudy;
podniky	a) depozitáři uvedení v čl. 21 odst. 3 písm. c) a v čl. 21 odst. 3 třetím pododstavci směrnice o správcích alternativních investičních fondů („depozitáři alternativních investičních fondů“); b) depozitáři uvedení v čl. 23 odst. 2 písm. c) směrnice o SKIPCP („depozitáři SKIPCP“).

[10] Model nasazení cloudu, kde cloudové služby poskytují podporu výhradně konkrétní skupině odběratelů těchto služeb a jsou touto skupinou sdíleny. Jedná se o odběratele, kteří mají sdílené požadavky a vzájemný vztah a z nichž alespoň jeden řídí zdroje.
[11] Model nasazení cloudu, který používá alespoň dva různé modely nasazení cloudu.
[12] Model nasazení cloudu, kde cloudové služby využívá výhradně jeden odběratel cloudových služeb a zdroje řídí tento odběratel cloudových služeb.
[13] Model nasazení cloudu, kde jsou cloudové služby potenciálně dostupné jakémukoliv odběrateli cloudových služeb a kde jsou zdroje řízeny poskytovatelem cloudových služeb.

3 Účel

5. Tyto obecné pokyny vycházejí z čl. 16 odst. 1 nařízení o orgánu ESMA. Cílem těchto obecných pokynů je zavést konzistentní, účinné a účelné postupy dohledu v rámci Evropského systému dohledu nad finančním trhem (ESFS) a zajistit společné, jednotné a důsledné uplatňování požadavků uvedených v oddíle 1.1 v části „Předmět“ tam, kde podniky využívají externích PCS. Cílem těchto obecných pokynů je zejména pomoci podnikům a příslušným orgánům identifikovat, řešit a sledovat rizika a problémy vyplývající z ujednání o externím zajišťování cloudových služeb, od rozhodování o externím zajišťování, výběru poskytovatele cloudových služeb, sledování externě zajišťovaných činností až po zajištění strategie odstoupení.

4 Dodržování předpisů a oznamovací povinnosti

4.1 Status obecných pokynů

6. V souladu s čl. 16 odst. 3 nařízení o orgánu ESMA vyvinou příslušné orgány a podniky veškeré úsilí, aby tyto obecné pokyny dodržovaly.

7. Příslušné orgány, na které se tyto obecné pokyny vztahují, by je měly splnit začleněním do svých vnitrostátních právních a/nebo dohledových rámců, včetně případů, kdy jsou konkrétní obecné pokyny zaměřeny především na podniky. V tomto případě by příslušné orgány měly zajistit v rámci svého dohledu, aby podniky tyto obecné pokyny dodržovaly.

4.2 Oznamovací povinnosti

8. Do dvou měsíců od zveřejnění obecných pokynů na internetových stránkách orgánu ESMA ve všech úředních jazycích EU příslušné orgány, na které se tyto obecné pokyny vztahují, musí oznámit orgánu ESMA, zda se obecnými pokyny i) řídí; ii) neřídí, ale hodlají se jimi řídit, nebo iii) neřídí a nehodlají se jimi řídit.

9. Pokud se jimi neřídí, příslušné orgány musí orgánu ESMA rovněž do dvou měsíců od zveřejnění obecných pokynů na internetových stránkách orgánu ESMA ve všech úředních jazycích EU oznámit důvody, proč se obecnými pokyny neřídí. Vzor oznámení je k dispozici na internetových stránkách orgánu ESMA. Po vyplnění je formulář zaslán orgánu ESMA.

10. Podniky nejsou povinny oznamovat, zda se těmito obecnými pokyny řídí.

5 Obecné pokyny ohledně zajišťování cloudových služeb u externích poskytovatelů

Obecný pokyn č. 1. Správa, dohled a dokumentace

11. Podnik by měl mít definovanou aktuální strategii externího zajišťování cloudových služeb, která je v souladu s příslušnými strategiemi a interními zásadami a procesy, včetně vztahu k informačním a komunikačním technologiím, bezpečnosti informací a řízení provozních rizik.

12. Podnik by měl:

    a) jasně určit odpovědnost za dokumentaci, řízení a kontrolu ujednání o externím zajišťování cloudových služeb v rámci své organizace;
    b) přidělit dostatečné zdroje k zajištění souladu s těmito obecnými pokyny a se všemi právními požadavky platnými pro jeho ujednání o externím zajišťování cloudových služeb;
    c) zřídit funkci dohledu nad externím zajišťováním cloudových služeb nebo jmenovat vedoucí zaměstnance, kteří se zodpovídají přímo řídícímu orgánu a jsou odpovědní za řízení rizik a dohled nad riziky vyplývající z ujednání o externím zajišťování cloudových služeb. Při dodržování tohoto pokynu by podniky měly brát v úvahu jak povahu, rozsah a složitost svého podnikání, a to i pokud jde o riziko pro finanční systém, tak rizika spojená s externě zajišťovanými funkcemi, a zajistit, aby měl jejich řídící orgán příslušné technické dovednosti k porozumění rizikům spojeným s ujednáními o externím zajišťování cloudových služeb. Malé a méně komplexní podniky by měly přinejmenším zajistit jasné rozdělení úloh a odpovědností týkající se správy ujednání o externím zajišťování cloudových služeb a dohledu nad nimi.

13. Podnik by měl sledovat výkon činností, bezpečnostní opatření a dodržování dohodnutých úrovní služeb ze strany svých PCS. Toto sledování by mělo být založeno na posouzení míry rizika a mělo by se primárně zaměřovat na zásadní nebo důležité funkce, které byly zadány externě.

14. Podnik by měl opětovně posuzovat, zda se jeho ujednání o externím zajišťování cloudových služeb týkají zásadní nebo důležité funkce, vždy poté, co se podstatně změnilo riziko, povaha nebo rozsah externě zajišťované funkce.

15. Podnik by měl udržovat aktualizovanou evidenci informací o všech svých ujednáních o externím zajišťování cloudových služeb, přičemž by měl rozlišovat mezi externím zajišťováním zásadních nebo důležitých funkcí a mezi ostatními ujednáními o externím zajišťování. Při rozlišování mezi externím zajišťováním zásadních nebo důležitých funkcí a mezi ostatními ujednáními o externím zajišťování by měl poskytnout stručné shrnutí důvodů, proč daná externě zajišťovaná funkce je nebo není považována za

zásadní nebo důležitou. S přihlédnutím k vnitrostátním právním předpisům by měl podnik také po přiměřenou dobu vést záznamy o ukončených ujednáních o externím zajišťování cloudových služeb.

16. V případě ujednání o externím zajišťování cloudových služeb týkajících se zásadních nebo důležitých funkcí by měla evidence obsahovat alespoň následující informace pro každé ujednání o externím zajišťování cloudových služeb:

    a) referenční číslo:
    b) datum zahájení a případně příští datum obnovení smlouvy, datum ukončení a/nebo výpovědní lhůty pro PCS a pro podnik;
    c) stručný popis externě zajišťované funkce, včetně dat, která jsou zajišťována externě, a zda tato data zahrnují osobní údaje (například uvedením ano nebo ne v samostatném datovém poli);
    d) podnikem přiřazenou kategorii odrážející povahu externě zajišťované funkce (například informačně-technologická funkce, kontrolní funkce), která by měla usnadnit identifikaci různých typů ujednání o externím zajišťování cloudových služeb;
    e) zda externě zajištěná funkce podporuje obchodní operace, u kterých je rozhodujícím faktorem čas;
    f) jméno a obchodní značku poskytovatele cloudových služeb, zemi, kde je registrován, registrační číslo společnosti, identifikační kód právnické osoby (je-li k dispozici), sídlo a jiné příslušné kontaktní údaje a jméno jeho případné mateřské společnosti;
    g) rozhodné právo ujednání o externím zajišťování cloudových služeb a případný výběr soudně příslušné země;
    h) typ cloudových služeb a modelů nasazení a specifická povaha dat, která mají být uchovávána, a místa (zejména regiony nebo země), kde mohou být tato data uložena;
    i) datum posledního posouzení zásadnosti nebo důležitosti externě zajišťované funkce a datum příštího plánovaného posouzení;
    j) datum posledního posouzení/auditu rizik poskytovatele cloudových služeb spolu se stručným shrnutím hlavních výsledků a datum příštího plánovaného posouzení/auditu rizik;
    k) osobu nebo rozhodovací orgán v podniku, která (který) schválila (schválil) ujednání o externím zajišťování cloudových služeb;
    l) případně jména veškerých subdodavatelů, jimž je významná část zásadní nebo důležité funkce (nebo její podstatné části) dále externě zadána, včetně země, kde jsou subdodavatelé registrováni, kde bude dále externě zajišťovaná služba poskytována, a případně místa (zejména regiony nebo země), kde budou uložena data;
    m) odhadované roční rozpočtové náklady ujednání o externím zajišťování cloudových služeb.

17. Pokud jde o ujednání o externím zajišťování cloudových služeb týkající se nikoli zásadních nebo nikoli důležitých funkcí, měl by podnik určit informace, které mají být zahrnuty do evidence, na základě povahy, rozsahu a složitosti rizik spojených s externě zajišťovanou funkcí.

Obecný pokyn č. 2. Analýza předcházející externímu zajišťování služeb a hloubková kontrola

18. Před uzavřením jakéhokoliv ujednání o externím zajišťování cloudových služeb by podnik měl:

    a) posoudit, zda se ujednání o externím zajišťování cloudových služeb týká zásadní nebo důležité funkce;
    b) zjistit a vyhodnotit příslušná rizika ujednání o externím zajišťování cloudových služeb;
    c) provést náležitou hloubkovou kontrolu možného poskytovatele cloudových služeb;
    d) identifikovat a vyhodnotit jakýkoliv střet zájmů, který by mohl být externím zajišťováním způsoben.

19. Analýza předcházející externímu zajišťování služeb a hloubková kontrola možného PCS by měla být úměrná povaze, rozsahu a složitosti funkce, kterou má podnik v úmyslu externě zadat, a rizikům spojeným s touto funkcí. Měla by přinejmenším zahrnovat posouzení možného dopadu ujednání o externím zajišťování cloudových služeb na provozní a právní rizika podniku, na riziko nedodržení předpisů a riziko poškození dobré pověsti.

20. V případě, že se ujednání o externím zajišťování cloudových služeb týká zásadních nebo důležitých funkcí, měl by podnik také:

    a) posoudit všechna příslušná rizika, která mohou nastat v důsledku ujednání o externím zajišťování cloudových služeb, včetně rizik ve vztahu k informačním a komunikačním technologiím, bezpečnosti informací, kontinuitě činností, právním předpisům a jejich dodržování, riziku poškození dobré pověsti, operačním rizikům a možným omezením dohledu nad podnikem, vyplývající z:
        i. vybrané cloudové služby a navrhovaných modelů nasazení;
        ii. migrace a/nebo postupů provádění;
        iii. citlivosti funkce a souvisejících dat, u nichž se uvažuje o externím zajištění, a bezpečnostních opatření, která by bylo třeba přijmout;
        iv. interoperability systémů a aplikací podniku a poskytovatele cloudových služeb, zejména z jejich schopnosti vyměňovat si informace a vzájemně využívat vyměňované informace;
        v. přenositelnosti podnikových dat, zejména schopnosti snadno přenášet podniková data mezi různými PCS nebo zpět do podniku;

vi. politické stability, bezpečnostní situace a právního systému (včetně platných ustanovení o vymáhání práva, ustanovení insolvenčních zákonů, která by se použila v případě úpadku PCS, platných zákonů o ochraně údajů a toho, zda jsou podmínky pro převod osobních údajů do třetí země v souladu s nařízením GDPR) zemí (v rámci EU nebo mimo ni), kde by byly poskytovány externě zajišťované funkce a kde by byla uložena externě zadávaná data; v případě dalšího externího zajišťování vyplývající z dalších rizik, která mohou vzniknout, pokud se subdodavatel nachází ve třetí zemi nebo v jiné zemi než PCS, a v případě subdodavatelského řetězce z jakékoliv dalšího rizika, které může vzniknout, včetně toho souvisejícího s absencí přímé smlouvy mezi podnikem a subdodavatelem vykonávajícím externě zajišťovanou funkci;

vii. možného spojení v rámci podniku (včetně případného spojení na úrovni skupiny) způsobeného několika ujednáními o externím zajišťování cloudových služeb se stejným poskytovatelem cloudových služeb, jakož i možného spojení v rámci finančního sektoru EU způsobeného více podniky využívajícími stejného poskytovatele cloudových služeb nebo malou skupinu poskytovatelů cloudových služeb. Při hodnocení rizika koncentrace by měl podnik zohlednit všechna svá ujednání o externím zajišťování cloudových služeb (a případně ujednání o externím zajišťování cloudových služeb na úrovni skupiny) s tímto PCS;

b) zohlednit očekávané náklady a přínosy ujednání o externím zajišťování cloudových služeb, včetně zvážení všech závažných rizik, která mohou být zmírněna nebo lépe řízena, proti jakýmkoliv závažným rizikům, která mohou nastat v důsledku ujednání o externím zajišťování cloudových služeb.

21. V případě externího zajištění zásadních nebo důležitých funkcí by hloubková kontrola měla zahrnovat vyhodnocení vhodnosti PCS. Při posuzování vhodnosti PCS by měl podnik zajistit, aby PCS měl dobrou obchodní pověst, dovednosti, zdroje (včetně lidských, IT a finančních), organizační strukturu a případně příslušné (příslušná) oprávnění či registraci (registrace) k tomu, aby vykonával zásadní nebo důležité funkce spolehlivě a odborně a plnil své závazky během doby platnosti ujednání o externím zajišťování cloudových služeb. Dalšími faktory, které by při provádění hloubkové kontroly PCS měly být zváženy, jsou mimo jiné:

a) řízení bezpečnosti informací, zejména pak ochrana osobních, důvěrných nebo jinak citlivých údajů;
b) servisní podpora, včetně plánů podpory a kontaktů, a procesy krizového řízení;
c) zajištění kontinuity činností a plán obnovy provozu po havárii.

22. Za účelem podpory hloubkové kontroly může podnik také použít certifikace založené na mezinárodních standardech a zprávách externího nebo interního auditu tam, kde je to vhodné.

23. Pokud se podnik dozví o závažných nedostatcích a/nebo závažných změnách poskytovaných služeb nebo situace poskytovatele cloudových služeb, pak by analýza předcházející externímu zajišťování služeb a hloubková kontrola měly být neprodleně přezkoumány nebo v případě potřeby provedeny znovu.

24. V případě, že podnik vstoupí do nového ujednání nebo obnoví stávající ujednání s PCS, který již byl posouzen, měl by na základě přístupu založeného na posouzení míry rizika určit, zda je nutná nová hloubková kontrola.

Obecný pokyn č. 3. Klíčové smluvní prvky

25. Příslušná práva a povinnosti podniku a poskytovatele cloudových služeb by měly být jednoznačně formulovány v podobě písemné dohody.

26. Písemná dohoda by měla podniku výslovně umožnit ji v případě potřeby ukončit.

27. V případě externího zajištění zásadních nebo důležitých funkcí by písemná dohoda měla obsahovat alespoň:

    a) jasný popis externě zajišťované funkce;

    b) datum počátku a případné datum ukončení dohody a výpovědní lhůty pro poskytovatele cloudových služeb a pro podnik;

    c) rozhodné právo dohody a případný výběr soudně příslušné země;

    d) finanční závazky podniku i poskytovatele cloudových služeb;

    e) zda je povoleno další externí zajišťování a pokud ano, za jakých podmínek, s ohledem na obecný pokyn č. 7;

    f) místo/místa (tj. regiony nebo země), kde bude externě zajišťovaná funkce prováděna a kde budou uložena a zpracována data, a podmínky, které musí být splněny, včetně požadavku informovat podnik v případě, že PCS navrhne změnit uvedená místa;

    g) ustanovení týkající se bezpečnosti informací a ochrany osobních údajů s ohledem na obecný pokyn č. 4;

    h) právo podniku pravidelně sledovat výkonnost poskytovatele cloudových služeb v rámci ujednání o externím zajišťování cloudových služeb s ohledem na obecný pokyn č. 6;

    i) dohodnuté úrovně služeb, které by měly zahrnovat kvantitativní a kvalitativní výkonnostní cíle za účelem umožnění včasného monitorování, aby v případě, že nejsou dohodnuté úrovně služeb splněny, mohla být vhodná nápravná opatření přijata bez zbytečného prodlení;

j) oznamovací povinnosti poskytovatele cloudových služeb vůči podniku, včetně případných povinností předkládat zprávy týkající se funkce bezpečnosti podniku a klíčových funkcí, jako jsou zprávy připravené funkcí vnitřního auditu poskytovatele cloudových služeb;

k) ustanovení týkající se krizového řízení ze strany PCS, včetně povinnosti PCS hlásit podniku bez zbytečného prodlení incidenty, které ovlivnily fungování služby smluvně stanovené pro podnik;

l) zda by měl PCS uzavřít povinné pojištění určitých rizik, a případně požadovanou úroveň pojistného krytí;

m) požadavky na PCS ve věci provádění a testování plánů kontinuity činností a obnovy provozu po havárii;

n) požadavek, aby PCS udělil podniku, jeho příslušným orgánům a jakékoliv jiné osobě určené podnikem nebo příslušnými orgány právo na přístup („přístupová práva“) a na kontrolu („práva na audit“) příslušných informací, prostor, systémů a zařízení PCS v rozsahu nezbytném ke sledování výkonnosti PCS v rámci ujednání o externím zajišťování cloudových služeb a jeho souladu s platnými regulačními a smluvními požadavky, a to s ohledem na obecný pokyn č. 6;

o) ustanovení zajišťující, že k datům, které PCS zpracovává nebo ukládá jménem podniku, lze podle potřeby přistupovat, obnovovat je a případně je podniku vrátit, a to s ohledem na obecný pokyn č. 5.

Obecný pokyn č. 4. Bezpečnost informací

28. Podnik by měl stanovit požadavky na zabezpečení informací ve svých interních zásadách a postupech a v rámci písemného ujednání o externím zajišťování cloudových služeb a průběžně sledovat dodržování těchto požadavků, mimo jiné za účelem ochrany důvěrných, osobních nebo jinak citlivých údajů. Tyto požadavky by měly být přiměřené povaze, rozsahu a složitosti funkce, kterou podnik zadává poskytovateli cloudových služeb, a rizikům spojeným s touto funkcí.

29. Za tímto účelem by v případě externího zajišťování zásadních nebo důležitých funkcí, aniž by byly dotčeny příslušné požadavky nařízení GDPR, měl podnik, který uplatňuje přístup založený na posouzení míry rizika, alespoň:

a) *organizace bezpečnosti informací:* zajistit jasné rozdělení úloh a odpovědností v oblasti bezpečnosti informací mezi podnikem a PCS, a to i ve vztahu k detekci hrozeb, krizovému řízení a správě oprav, a zajistit, aby byl PCS účinně schopen plnit svou úlohu a odpovědnost;
b) *správa identit a řízení přístupů*: zajistit, aby byly zavedeny silné ověřovací mechanismy (například vícefaktorové ověřování) a kontroly přístupu s cílem zabránit neoprávněnému přístupu k datům a back-endovým cloudovým zdrojům podniku;

c) *šifrování a správa klíčů*: zajistit, aby se v případě potřeby používaly příslušné šifrovací technologie pro přenášená data, data v paměti, data v klidovém umístění a pro zálohování dat, a to v kombinaci s vhodnými řešeními pro správu klíčů, aby se omezilo riziko neautorizovaného přístupu k šifrovacím klíčům; podnik by měl při výběru řešení pro správu šifrovacích klíčů vzít v úvahu zejména nejmodernější technologii a procesy;
d) *zabezpečení provozu a sítě*: zvážit příslušnou úroveň dostupnosti sítě, segregaci sítě (například izolaci nájemce ve sdíleném prostředí cloudu, provozní rozdělení, jde-li o web, aplikační logiku, operační systém, síť, systém řízení báze dat (SŘBD či DBMS) a vrstvy úložiště) a typ provozního prostředí (například testovací, pro uživatelské akceptační testy, vývojové, produkční);
e) *rozhraní pro programování aplikací (API)*: zvážit mechanismy pro začlenění cloudových služeb do systémů podniku, aby byla zajištěna bezpečnosti API (například vytvoření a udržování zásad a postupů zabezpečení informací pro API přes více systémových rozhraní, soudních příslušností a obchodních funkcí s cílem zabránit neoprávněnému vyzrazení, úpravě nebo zničení dat);
f) *kontinuita činností a obnova provozu po havárii*: zajistit, aby byly zavedeny účinné kontroly kontinuity činností a obnovy provozu po havárii (například stanovením minimálních požadavků na kapacitu, výběrem z nabídky hostingu podle geografického rozložení, s možností přecházet z jednoho na druhý nebo vyžádáním a kontrolou dokumentace zobrazující cestu přenosu dat podniku mezi systémy poskytovatele cloudových služeb, jakož i zvážením možnosti replikace image (obrazu) disku do nezávislého úložiště, které je dostatečně izolované od sítě nebo je off-line);
g) *umístění dat*: přijmout přístup založený na posouzení míry rizika vůči místu/místům (zejména regionům nebo zemím) pro ukládání a zpracování dat;
h) *dodržování předpisů a monitorování*: ověřit, zda poskytovatel cloudových služeb dodržuje mezinárodně uznávané standardy bezpečnosti informací a zavedl vhodné kontroly bezpečnosti informací (například tím, že poskytovatele cloudových služeb požádá o poskytnutí důkazu o tom, že provádí příslušné kontroly bezpečnosti informací, a prováděním pravidelných hodnocení a testů opatření, která poskytovatel cloudových služeb ohledně bezpečnosti informací přijal).

Obecný pokyn č. 5. Strategie odstoupení

30. V případě externího zajištění zásadních nebo důležitých funkcí by podnik měl mít zaručenou možnost odstoupit od ujednání o externím zajišťování cloudových služeb bez zbytečného narušení svých obchodních aktivit a služeb pro své klienty a bez jakékoliv újmy na plnění svých povinností vyplývajících z příslušných právních předpisů, jakož i na důvěrnosti, integritě a dostupnosti svých dat. Za tímto účelem by podnik měl:

a) vyvinout plány odstoupení, které jsou srozumitelné, zdokumentované a dostatečně otestované. Tyto plány by měly být podle potřeby aktualizovány, a to i v případě změn v externě zajišťované funkci;
b) určit alternativní řešení a vypracovat plány přechodu určené k odebrání externě zajišťované funkce a dat od poskytovatele cloudových služeb a případně od jakéhokoliv subdodavatele a přenést je k náhradnímu PCS určeného podnikem nebo přímo zpět do podniku. Tato řešení by měla být stanovena s ohledem na problémy, které mohou nastat v důsledku umístění dat, přičemž by se měla přijímat nezbytná opatření s cílem zajistit kontinuitu činností během přechodné fáze;
c) zajistit, aby písemné ujednání o externím zajišťování cloudových služeb obsahovalo povinnost poskytovatele cloudových služeb podporovat řádný převod externě zajišťované funkce a související zpracování z tohoto PCS a jakéhokoliv subdodavatele na jiného PCS určeného podnikem nebo přímo na podnik v případě, že podnik uvede do chodu strategii odstoupení. Povinnost podporovat řádný převod externě zajišťované funkce a související zacházení s daty by měla případně zahrnovat bezpečné vymazání dat ze systémů PCS a jakéhokoliv subdodavatele.

31. Při vypracovávání plánů odstoupení a řešení uvedených v písmenech a) a b) výše („strategie odstoupení“) by podnik měl zvážit následující:

a) stanovení cíle strategie odstoupení;
b) definování rozhodných událostí, které by mohly aktivovat strategii odstoupení. Mezi ně by mělo patřit přinejmenším ukončení ujednání o externím zajišťování cloudových služeb z iniciativy podniku nebo PCS a výpadek fungování nebo jiné závažné přerušení obchodní činnosti PCS;
c) provedení analýzy dopadu na podnikání, která je přiměřená externě zadané funkci, aby bylo možné určit, jaké lidské a jiné zdroje by byly potřebné k provedení strategie odstoupení;
d) přiřazení úloh a odpovědností v rámci řízení strategie odstoupení;
e) otestování vhodnosti strategie odstoupení pomocí přístupu založeného na posouzení míry rizika (například provedením analýzy potenciálních nákladů, dopadů, zdrojů a časových důsledků převodu externě zajišťované služby na náhradního poskytovatele);
f) definování kritéria úspěšnosti přechodu.

32. Podnik by měl zahrnout ukazatele rozhodných událostí ze strategie odstoupení do svého průběžného monitorování služeb od poskytovatele cloudových služeb v rámci ujednání o externím zajišťování cloudových služeb a dále do dohledu nad nimi.

Obecný pokyn č. 6. Přístupová práva a práva provádět audit

33. Podnik by měl zajistit, aby písemné ujednání o externím zajišťování cloudových služeb neomezovalo účinný výkon přístupových práv a práv provádět audit ani dohled nad PCS ze strany podniku a příslušného orgánu.

34. Podnik by měl zajistit, aby výkon přístupových práv a práv provádět audit (například četnost auditů a auditované oblasti a služby) zohledňoval, zda externí zajišťování souvisí se zásadní nebo důležitou funkcí, jakož i s povahou a rozsahem rizik a dopadů, které na podnik má ujednání o externím zajišťování cloudových služeb.

35. V případě, že výkon přístupových práv nebo práv provádět audit nebo použití určitých auditorských technik vytváří riziko v prostředí PCS a/nebo jiného klienta PCS (například ovlivněním úrovní služeb, důvěrnosti, integrity a dostupnosti dat), PCS by měl podniku poskytnout jasné zdůvodnění, proč by to vedlo k riziku, a PCS by se měl s podnikem dohodnout na alternativních způsobech, jak dosáhnout podobného výsledku (například zahrnutím konkrétních testů kontrol do konkrétní zprávy či pomocí osvědčení vydaného poskytovatelem cloudových služeb).

36. Aniž je dotčena jejich konečná odpovědnost za ujednání o externím zajišťování cloudových služeb, mohou podniky za účelem účinnějšího využití auditních zdrojů a snížení organizační zátěže pro poskytovatele cloudových služeb a jeho zákazníky využít:

    a) osvědčení vydaná třetí stranou a zprávy externího nebo interního auditu zpřístupněné poskytovatelem cloudových služeb;
    b) společné audity prováděné zároveň s ostatními klienty stejného PCS nebo společné audity prováděné auditorem třetí strany jmenovaným více klienty stejného PCS.

37. V případě externího zajišťování zásadních nebo důležitých funkcí by měl podnik posoudit, zda jsou osvědčení třetích stran a zprávy externího nebo interního auditu uvedené v odst. 37 písm. a) přiměřené a dostatečné pro splnění jeho povinností vyplývajících z příslušných právních předpisů, a měl by se zaměřit na to, aby se v průběhu času nespoléhal výhradně na tato osvědčení a zprávy.

38. V případě externího zajišťování zásadních nebo důležitých funkcí by měl podnik využívat osvědčení třetích stran a zprávy externího nebo interního auditu uvedené v odst. 37 písm. a), pouze pokud:

    a) je přesvědčen, že rozsah osvědčení nebo zpráv o auditu zahrnuje klíčové systémy poskytovatele cloudových služeb (například procesy, aplikace, infrastrukturu, datová centra), klíčové kontroly určené podnikem a je v souladu s příslušnými platnými právními předpisy;

b) bude pravidelně důkladně posuzovat obsah osvědčení nebo zpráv o auditu a ověřovat, zda osvědčení nebo zprávy nejsou zastaralé;
c) zajistí, aby klíčové systémy a kontroly poskytovatele cloudových služeb byly zahrnuty v budoucích verzích osvědčení nebo zpráv o auditu;
d) je spokojen se stranou vydávající osvědčení či provádějící audit (například s ohledem na její kvalifikaci, odbornost, opakované provádění či ověřování důkazů v podkladové složce auditu, jakož i střídání certifikační nebo auditorské společnosti);
e) je přesvědčen, že osvědčení jsou vydávána a audity prováděny podle příslušných standardů a zahrnují test účinnosti zavedených klíčových kontrol;
f) má smluvní právo požadovat rozšíření rozsahu osvědčení nebo zpráv o auditu na další příslušné systémy a kontroly poskytovatele cloudových služeb, přičemž počet a četnost takových žádostí o úpravu rozsahu by měly být přiměřené a oprávněné z pohledu řízení rizik;
g) si ponechá smluvní právo provádět individuální audity, pokud jde o externě zajišťovanou funkci, na místě a podle svého uvážení.

39. Podnik by měl zajistit, aby před návštěvou na místě, včetně situace, kdy je navštěvující třetí strana jmenovaná podnikem (například auditor), bylo poskytovateli cloudových služeb předem a v přiměřené lhůtě doručeno oznámení, s výjimkou případů, kdy není možné předem a včas oznámení doručit z důvodu mimořádné nebo krizové situace nebo pokud by vedlo k situaci, kdy by audit již nebyl účinný. Toto oznámení by mělo uvádět místo a účel návštěvy a pracovníky, kteří se návštěvy zúčastní.

40. Vzhledem k tomu, že cloudové služby představují vysokou úroveň technické složitosti a vyvolávají specifické problémy v oblasti soudní příslušnosti, měli by pracovníci provádějící audit, ať už jsou interními auditory podniku, nebo auditory jednajícími jeho jménem, mít správné dovednosti a znalosti pro řádné posouzení příslušné cloudové služby a pro provedení účinného a relevantního auditu. To by se mělo vztahovat také na podnikové zaměstnance, kteří kontrolují osvědčení nebo zprávy o auditu dodané poskytovatelem cloudových služeb.

Obecný pokyn č. 7. Další externí zajišťování

41. Pokud je povoleno další externí zajišťování zásadních nebo důležitých funkcí (nebo jejich podstatných částí), písemné ujednání o externím zajišťování cloudových služeb mezi podnikem a poskytovatelem cloudových služeb by mělo:

a) specifikovat jakoukoliv část nebo aspekt externě zajišťované funkce, které jsou vyloučeny z potenciálního dalšího externího zajišťování;
b) určit podmínky, které musí být dodržovány v případě dalšího externího zajišťování;
c) stanovit, že PCS zůstává odpovědný a je povinen dohlížet na služby, které jsou předmětem dalšího externího zajišťování, aby zajistil nepřetržité plnění všech smluvních závazků mezi PCS a podnikem;

d) obsahovat povinnost poskytovatele cloudových služeb informovat podnik o jakémkoliv zamýšleném dalším externím zajišťování nebo o jeho podstatných změnách, zejména pokud by to mohlo ovlivnit schopnost PCS plnit své závazky vyplývající z ujednání o externím zajišťování cloudových služeb mezi PCS a podnikem. Lhůta pro oznámení stanovená v písemné dohodě by měla podniku poskytnout dostatek času alespoň na provedení posouzení rizik navrhovaného dalšího externího zajišťování nebo jeho podstatných změn a na vznesení námitky proti nim nebo na jejich výslovné schválení, jak je uvedeno v písmenu e) níže;
e) zajistit, aby podnik měl právo vznést námitky proti zamýšlenému dalšímu externímu zajišťování nebo jeho podstatným změnám nebo aby byl vyžadován výslovný souhlas před tím, než navrhované další externí zajišťování nebo podstatné změny vstoupí v platnost;
f) zajistit, aby podnik měl smluvní právo ukončit ujednání o externím zajišťování cloudových služeb s PCS v případě, že vznese námitky proti navrhovanému dalšímu externímu zajišťování nebo jeho podstatným změnám a v případě neoprávněného dalšího externího zajišťování (například pokud PCS provádí další externí zajišťování, aniž by o tom podnik informoval, nebo vážně porušuje podmínky dalšího externího zajišťování uvedené v ujednání o externím zajišťování cloudových služeb).

42. Podnik by měl zajistit, aby PCS náležitě dohlížel na subdodavatele.

Obecný pokyn č. 8. Písemné oznámení příslušným orgánům

43. Podnik by měl písemně včas informovat svůj příslušný orgán o plánovaných ujednáních o externím zajišťování cloudových služeb, která se týkají zásadní nebo důležité funkce. Podnik by měl také včas a písemně informovat svůj příslušný orgán o těch ujednáních o externím zajišťování cloudových služeb, která se týkají funkce, která byla dříve klasifikována jako nikoli zásadní nebo nikoli důležitá a poté se stala zásadní nebo důležitou.

44. Písemné oznámení podniku by mělo při zohlednění zásady proporcionality obsahovat alespoň tyto informace:

a) datum počátku a případně datum příštího obnovení ujednání o externím zajišťování cloudových služeb, datum ukončení a/nebo výpovědní lhůty pro PCS a pro podnik;
b) stručný popis externě zajišťované funkce;
c) stručné shrnutí důvodů, proč je externě zajišťovaná funkce nebo činnost považována za zásadní nebo důležitou;
d) jméno a případnou obchodní značku poskytovatele cloudových služeb, zemi, kde je registrován, registrační číslo společnosti, identifikační kód právnické osoby (je-li k dispozici), sídlo a jiné příslušné kontaktní údaje a jméno jeho případné mateřské společnosti;

e) rozhodné právo ujednání o externím zajišťování cloudových služeb a případný výběr soudně příslušné země;
f) typ cloudového modelu nasazení a specifickou povahu dat, která mají být uchovávána poskytovatelem cloudových služeb, a místa (zejména regiony nebo země), kde mohou být tato data uložena;
g) datum posledního posouzení zásadnosti nebo důležitosti externě zajišťované funkce;
h) datum posledního posouzení nebo auditu rizik poskytovatele cloudových služeb spolu se stručným shrnutím hlavních výsledků a datum příštího plánovaného posouzení nebo auditu rizika;
i) osobu nebo rozhodovací orgán v podniku, která (který) schválila (schválil) ujednání o externím zajišťování cloudových služeb;
j) případně jména veškerých subdodavatelů, jimž je významná část zásadní nebo důležité funkce dále externě zadána, včetně země nebo regionu, kde jsou subdodavatelé registrováni, kde bude dále externě zajišťovaná služba poskytována a kde budou uložena data.

Obecný pokyn č. 9. Dohled nad ujednáními o externím zajišťování cloudových služeb

45. Příslušné orgány by měly v rámci provádění dohledu posoudit rizika vyplývající z ujednání o externím zajišťování cloudových služeb. Toto posouzení by se mělo zejména zaměřit na opatření, která se vztahují k externímu zajišťování zásadních nebo důležitých funkcí.

46. Příslušné orgány by měly mít jistotu, že jsou schopny vykonávat účinný dohled, a to zejména tehdy, když podniky externě zajišťují zásadní nebo důležité funkce, které jsou prováděny mimo EU.

47. Příslušné orgány by měly na základě přístupu založeného na posouzení míry rizika vyhodnotit, zda podniky:

a) mají zavedeno příslušné řízení, zdroje a provozní procesy, aby bylo možné náležitě a účinně uzavírat a realizovat ujednání o externím zajišťování cloudových služeb a nad těmito ujednáními dohlížet;
b) rozeznávají a řídí všechna příslušná rizika ve vztahu k externímu zajišťování cloudových služeb.

48. Pokud jsou zjištěna rizika koncentrace, měly by příslušné orgány sledovat vývoj těchto rizik a hodnotit jejich potenciální dopad jak na jiné podniky, nad nimiž vykonávají dohled, tak na stabilitu finančního trhu.