EIOPA-BoS-20-002

Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb

Obsah

Úvod

1. V souladu s článkem 16 nařízení (EU) č. 1094/2010[1] orgán EIOPA vydává obecné pokyny s cílem poskytnout pokyny pojišťovnám a zajišťovnám ohledně toho, jak je třeba uplatňovat ustanovení o externím zajištění služeb nebo činností (outsourcingu) uvedená ve směrnici 2009/138/ES[2] (dále jen „směrnice Solventnost II") a v nařízení Komise v přenesené pravomoci (EU) 2015/35[3] (dále jen „nařízení v přenesené pravomoci") v případě outsourcingu u poskytovatelů cloudových služeb.

2. Tyto obecné pokyny vycházejí z čl. 13 odst. 28 a článků 38 a 49 směrnice Solventnost II a článku 274 nařízení v přenesené pravomoci. Kromě toho tyto obecné pokyny vycházejí z pokynů uvedených v obecných pokynech k řídicímu a kontrolnímu systému orgánu EIOPA (EIOPA-BoS-14/253).

3. Tyto obecné pokyny jsou určeny příslušným orgánům s cílem poskytovat pokyny ohledně toho, jak by pojišťovny a zajišťovny (společně dále jen „podniky") měly uplatňovat požadavky na externí zajištění služeb nebo činností stanovené ve výše uvedených právních aktech v souvislosti s outsourcingem u poskytovatelů cloudových služeb.

4. Tyto obecné pokyny se vztahují jak na jednotlivé podniky, tak obdobně na skupiny[4].

   Subjekty, které podléhají jiným odvětvovým požadavkům a které jsou součástí skupiny, jsou vyloučeny z oblasti působnosti těchto obecných pokynů na úrovni jednotlivých podniků, protože musí dodržovat zvláštní odvětvové požadavky, jakož i příslušné pokyny vydané Evropským orgánem pro cenné papíry a trhy a Evropským orgánem pro bankovnictví.

5. V případě outsourcingu u poskytovatelů cloudových služeb – ať již přímo nebo prostřednictvím jejich dalšího externího zajištění – v rámci skupiny by se tyto pokyny měly uplatňovat ve spojení s ustanoveními obecných pokynů k řídicímu a kontrolnímu systému orgánu EIOPA ohledně outsourcingu v rámci skupiny.

6. Podniky a příslušné orgány by při dodržování těchto obecných pokynů nebo dohledu nad jejich dodržováním měly vzít v úvahu zásadu proporcionality[5] a rozhodující význam nebo důležitost služby externě zajištěné poskytovateli cloudových služeb. Zásada proporcionality by měla zajistit, aby postupy řízení a kontroly, včetně těch, které souvisejí s outsourcingem u poskytovatelů cloudových služeb, byly přiměřené povaze, rozsahu a komplexnosti podkladových rizik.

7. Tyto obecné pokyny je třeba vykládat v kontextu s obecnými pokyny k řídicímu a kontrolnímu systému orgánu EIOPA a s regulačními povinnostmi uvedenými v odstavci 1, aniž by tím byly uvedené obecné pokyny a regulační povinnosti dotčeny.

Definice

8. Nejsou-li v těchto obecných pokynech definovány jinak, použité pojmy mají význam definovaný v právních aktech uvedených v úvodu.

---

[1] 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 2009/79/EC (Úř. věst. L 331, 15.12.2010, s. 48).

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

[3] Nařízení Komise v přenesené pravomoci (EU) 2015/35 ze dne 10. října 2014, kterým se doplňuje směrnice Evropského parlamentu a Rady 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), (Úř. věst. L 12, 17.1.2015, s. 1).

[4] Čl. 212 odst. 1 směrnice Solventnost II.

[5] Čl. 29 odst. 3 směrnice Solventnost II.

9. Kromě toho se pro účely těchto obecných pokynů použijí tyto definice:

Poskytovatel služeb	znamená třetí stranu, která na základě ujednání o externím zajištění služeb nebo činností (outsourcingu) vykonává proces, službu nebo činnost nebo jejich část.
Poskytovatel cloudových služeb	znamená poskytovatele služeb podle výše uvedené definice, který je odpovědný za poskytování cloudových služeb na základě ujednání o externím zajištění služeb nebo činností.
Cloudové služby	znamenají služby poskytované za použití cloud computingu, což je model, který umožňuje neustálý a pohodlný síťový přístup podle potřeby ke sdílenému souboru konfigurovatelných výpočetních zdrojů (např. sítě, servery, ukládání dat, aplikace a služby), který může být s minimálním úsilím vynaloženým na správu či interakci s poskytovatelem služby rychle poskytnut a zpřístupněn.
Veřejný cloud	znamená cloudovou infrastrukturu, kterou může volně využívat široká veřejnost.
Soukromý cloud	znamená cloudovou infrastrukturu určenou pro výlučné užívání jediným podnikem.
Komunitní cloud	znamená cloudovou infrastrukturu určenou pro výlučné užívání konkrétní komunitou podniků, např. několika podniky v jediné skupině.
Hybridní cloud	znamená cloudovou infrastrukturu, která se skládá ze dvou či více různých cloudových infrastruktur.

Datum použitelnosti

10. Tyto obecné pokyny se použijí od 1. ledna 2021 na všechna ujednání o externím zajištění cloudových služeb, která byla uzavřena nebo pozměněna k tomuto datu nebo později.

11. Podniky by měly přezkoumat a odpovídajícím způsobem změnit stávající ujednání o externím zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, s cílem zajistit dodržování těchto obecných pokynů do 31. prosince 2022.

12. Nebude-li přezkum ujednání o externím zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, dokončen do 31. prosince 2022, měl by podnik o této skutečnosti informovat svůj orgán dohledu[6], včetně opatření plánovaných za účelem provedení přezkumu nebo případné strategie odstoupení. Orgán dohledu se může v případě potřeby dohodnout s podnikem na prodloužené lhůtě pro dokončení tohoto přezkumu.

13. Aktualizace (v případě potřeby) zásad a vnitřních procesů podniku by měla být provedena do 1. ledna 2021, zatímco požadavky na dokumentaci, pokud jde o ujednání o externím zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, by měly být provedeny do 31. prosince 2022.

[6] Čl. 13 odst. 10 směrnice Solventnost II.

Obecný pokyn 1 – Cloudové služby a outsourcing

14. Podnik by měl stanovit, zda ujednání s externím poskytovatelem cloudových služeb spadá do definice pojmu externí zajištění služeb nebo činností (outsourcing) podle směrnice Solventnost II. Při posuzování je nutné brát v úvahu:

a. zda se externě zajišťované provozní funkce nebo činnost (nebo její část) provádí opakovaně nebo průběžně a

b. zda by tato provozní funkce nebo činnost (nebo její část) normálně spadala do rozsahu provozních funkcí nebo činností, které by byly nebo mohly být podnikem prováděny v rámci jeho běžných obchodních činností, ačkoli podnik tuto provozní funkci nebo činnost v minulosti nevykonával.

15. Pokud se ujednání s poskytovatelem služeb týká většího počtu provozních funkcí nebo činností, měl by podnik při svém posouzení zvážit všechny aspekty ujednání.

16. Pokud podnik zajišťuje provozní funkce nebo činnosti u externích poskytovatelů služeb, kteří nejsou poskytovateli cloudových služeb, ale při poskytování svých služeb se do značné míry spoléhají na cloudové infrastruktury (například pokud je poskytovatel cloudových služeb součástí řetězce dalšího externího zajištění), ujednání pro takové externí zajištění služeb nebo činností spadá do oblasti působnosti těchto obecných pokynů.

Obecný pokyn 2 – Obecné zásady řízení a kontroly v případě outsourcingu cloudových služeb

17. Aniž by byl dotčen čl. 274 odst. 3 nařízení v přenesené pravomoci, správní, řídící nebo kontrolní orgán podniku by měl zajistit, aby se každé rozhodnutí o outsourcingu rozhodujících nebo důležitých provozních funkcí nebo činností u poskytovatelů cloudových služeb zakládalo na důkladném posouzení rizik, včetně všech příslušných rizik vyplývajících z ujednání, jako jsou rizika v oblasti informačních a komunikačních technologií (dále jen „IKT"), kontinuity činností, právní rizika a rizika dodržení souladu, rizika koncentrace, další operační rizika a rizika spojená s migrací dat a/nebo případně fází zavádění.

18. V případě outsourcingu rozhodujících nebo důležitých provozních funkcí nebo činností u poskytovatelů cloudových služeb by měl podnik případně zohlednit změny ve svém rizikovém profilu v důsledku ujednání o externím zajištění cloudových služeb ve svém vlastním posouzení rizik a solventnosti (ORSA).

19. Využívání cloudových služeb by mělo být v souladu se strategiemi podniku (například strategií IKT, strategií informační bezpečnosti, strategií řízení operačních rizik) a vnitřními zásadami a procesy, které by měly být v případě potřeby aktualizovány.

Obecný pokyn 3 – Aktualizace písemné koncepce outsourcingu

20. V případě outsourcingu u poskytovatelů cloudových služeb by podnik měl aktualizovat písemnou koncepci outsourcingu (například tím, že ji přezkoumá, doplní samostatný dodatek nebo vypracuje nové zvláštní politiky) a další příslušné vnitřní politiky (například pokud jde o informační bezpečnost), přičemž by měl zohlednit specifické charakteristiky externího zajištění cloudových služeb alespoň v těchto oblastech:

a. úlohy a odpovědnosti příslušných funkcí podniku, zejména správního, řídícího nebo kontrolního orgánu, a funkce odpovědné za IKT, informační bezpečnost, dodržování předpisů, řízení rizik a vnitřní audit;

b. procesy a postupy hlášení požadované pro schválení, provádění, sledování, řízení a případně obnovení ujednání o externím zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností;

c. dohled nad cloudovými službami přiměřený povaze, rozsahu a komplexnosti rizik spojených s poskytovanými službami, včetně i) posouzení rizik ujednání o externím zajištění cloudových služeb a hloubkové kontroly poskytovatelů cloudových služeb, včetně četnosti posouzení rizik; ii) kontrol sledování a řízení (například ověřování dohody o úrovni služeb); iii) bezpečnostních norem a kontrol;

d. s ohledem na externí zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, by měl být uveden odkaz na smluvní požadavky popsané v obecném pokynu 10;

e. požadavky na dokumentaci a písemné oznámení orgánu dohledu, pokud jde o externí zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností;

f. s ohledem na jednotlivá ujednání o externím zajištění cloudových služeb, které zahrnují rozhodující nebo důležité provozní funkce nebo činnosti, požadavek na zdokumentovanou a případně dostatečně vyzkoušenou „strategii odstoupení", která je přiměřená povaze, rozsahu a komplexnosti rizik spojených s poskytovanými službami. Strategie odstoupení může zahrnovat řadu procesů ukončení smluvního vztahu, mimo jiné přerušení, opětovné začlenění nebo převod služeb zahrnutých do ujednání o externím zajištění cloudových služeb.

Obecný pokyn 4 - Písemné oznámení orgánu dohledu

21. Požadavky na písemné oznámení stanovené v čl. 49 odst. 3 směrnice Solventnost II a podrobněji uvedené v obecných pokynech k řídicímu a kontrolnímu systému orgánu EIOPA se vztahují na jakýkoli outsourcing rozhodujících nebo významných provozních funkcí a činností u poskytovatelů cloudových služeb. Pokud se provozní funkce nebo činnost zajištěná externě, která byla dříve klasifikována jako jiná než rozhodující nebo jiná než důležitá, stane rozhodující nebo důležitou, podnik musí vyrozumět orgán dohledu.

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

a. stručný popis provozní funkce nebo činnosti zajištěné externě;

b. datum počátku a případně datum příštího obnovení smlouvy, datum ukončení a/nebo výpovědní lhůty pro poskytovatele cloudových služeb a pro podnik;

c. rozhodné právo dohody o externím zajištění cloudových služeb;

d. jméno poskytovatele cloudových služeb, registrační číslo společnosti, identifikátor právnické osoby (je-li k dispozici), sídlo a jiné příslušné kontaktní údaje a jméno jeho případné mateřské společnosti. V případě skupin údaj o tom, zda je poskytovatel cloudových služeb součástí skupiny;

e. model cloudových služeb a modely zavedení (tj. veřejné/soukromé/hybridní/komunitní) a konkrétní povaha dat, které budou uchovávány, a místa (tj. země nebo regiony), kde taková data budou uložena;

f. stručné shrnutí důvodů, proč je externě zajišťovaná provozní funkce nebo činnost považována za rozhodující nebo důležitou;

g. datum posledního posouzení rozhodující povahy nebo důležitosti externě zajišťované provozní funkce nebo činnosti.

Obecný pokyn 5 – Požadavky na dokumentaci

23. V rámci systému řízení a kontroly a řízení rizik podnik musí vést záznamy o svých ujednáních o externím zajištění cloudových služeb, například ve formě zvláštního rejstříku, který se průběžně aktualizuje. Podnik by měl rovněž uchovávat záznamy o ukončených ujednáních o externím zajištění cloudových služeb po přiměřenou dobu uchovávání, která podléhá vnitrostátní právní úpravě.

24. V případě externího zajištění rozhodujících nebo významných provozních funkcí nebo činností by podnik měl zaznamenat všechny tyto informace:

a. informace uvedené v obecném pokynu 4, které mají být oznámeny orgánu dohledu;

b. v případě skupin, pojišťovny nebo zajišťovny a další podniky v rámci obezřetnostní konsolidace, které využívají cloudové služby;

c. datum posledního hodnocení rizik a stručné shrnutí hlavních výsledků;

d. osoba nebo rozhodovací orgán (například správní, řídící nebo kontrolní orgán) v podniku, která (který) schválila (schválil) ujednání o externím zajištění cloudových služeb;

e. datum posledního a příštího plánovaného auditu, je-li to relevantní;

f. jména veškerých subdodavatelů, jimž je významná část rozhodující nebo důležité provozní funkce nebo činnosti dále externě zadána, včetně zemí, kde jsou subdodavatelé registrováni, kde bude služba poskytována, a případně místa (tj. země nebo regiony), kde budou tato data uložena;

g. výsledek posouzení nahraditelnosti poskytovatele cloudových služeb (např. zda je jednoduchá, složitá nebo nemožná);

h. zda externě zajištěná rozhodující nebo důležitá provozní funkce nebo činnost podporuje obchodní operace, které jsou z časového hlediska kritické;

i. odhadované roční rozpočtové náklady;

j. zda má podnik strategii odstoupení pro případ, že kterákoli ze stran činnost ukončí nebo že dojde k přerušení poskytování služeb poskytovatelem cloudových služeb.

25. V případě externího zajištění jiné než rozhodující nebo jiné než důležité provozní funkce nebo činnosti by měl podnik vymezit informace, které mají být zaznamenány, a to na základě povahy, rozsahu a komplexnosti rizik spojených se službami poskytovanými poskytovatelem cloudových služeb.

26. Podnik by měl na žádost orgánu dohledu poskytnout veškeré informace nezbytné k tomu, aby orgán dohledu mohl vykonávat dohled nad podnikem, včetně kopie dohody o externím zajištění cloudových služeb.

Obecný pokyn 6 – Analýza před outsourcingem

27. Před uzavřením jakéhokoli ujednání s poskytovateli cloudových služeb by podnik měl:

a. posoudit, zda se ujednání o externím zajištění cloudových služeb týká rozhodující nebo důležité provozní funkce nebo činnosti v souladu s obecným pokynem 7;

b. zjistit a vyhodnotit případná rizika ujednání o externím zajištění cloudových služeb v souladu s obecným pokynem 8;

c. provést příslušnou hloubkovou kontrolu potenciálního poskytovatele cloudových služeb v souladu s obecným pokynem 9;

d. identifikovat a posoudit střety zájmů, které může externí zajištění služeb nebo činností způsobit v souladu s požadavky stanovenými v čl. 274 odst. 3 písm. b) nařízení v přenesené pravomoci.

Obecný pokyn 7 – Posouzení rozhodujících nebo významných provozních funkcí a činností

28. Před uzavřením jakéhokoli ujednání o externím zajištění služeb nebo činností s poskytovateli cloudových služeb by podnik měl posoudit, zda se ujednání o externím zajištění cloudových služeb týká provozní funkce nebo činnosti, která je zásadní nebo důležitá. Při provádění takového posouzení by měl podnik případně zvážit, zda se ujednání může v budoucnu stát zásadním nebo důležitým. Podnik by měl rovněž provést nové posouzení rozhodující povahy nebo důležitosti provozní funkce nebo činnosti, která byla dříve externě zajišťována poskytovateli cloudových služeb, pokud se podstatně změní povaha, rozsah a komplexnost rizik spojených s danou dohodou.

29. Při posouzení by podnik měl spolu s výsledkem posouzení rizik vzít v úvahu alespoň tyto faktory:

a. potenciální dopad případného závažného narušení externě zajišťované provozní funkce nebo činnosti nebo neposkytování služeb poskytovatelem cloudových služeb na dohodnutých úrovních služeb na tyto oblasti podniku:

   i. trvalé dodržování jeho regulačních povinností;

   ii. krátkodobá a dlouhodobá finanční odolnost, solventnost a životaschopnost;

   iii. kontinuita činnosti a provozní odolnost;

   iv. operační riziko, včetně rizika interních procesů, IKT a právního rizika;

   v. rizika poškození dobré pověsti.

b. potenciální dopad ujednání o externím zajištění cloudových služeb na schopnost podniku:

   i. identifikovat, monitorovat a řídit všechna příslušná rizika;

   ii. splňovat všechny právní a regulační požadavky;

   iii. provádět příslušné audity, pokud jde o provozní funkce nebo činnosti zajištěné externě.

c. souhrnná expozice podniku (a/nebo případně skupiny) vůči stejnému poskytovateli cloudových služeb a potenciální kumulativní dopad ujednání o externím zajištění služeb nebo činností ve stejné oblasti podnikání;

d. velikost a složitost obchodních oblastí podniku ovlivněných ujednáním o externím zajištění cloudových služeb;

e. schopnost, je-li to nutné nebo žádoucí, převést navrhované ujednání o externím zajištění cloudových služeb na jiného poskytovatele cloudových služeb nebo znovu integrovat služby („nahraditelnost“);

f. ochrana osobních a jiných než osobních údajů a potenciální dopad porušení důvěrnosti údajů nebo nezajištění jejich dostupnosti a integrity na podnik, pojistníky nebo jiné příslušné subjekty mimo jiné na základě nařízení (EU)

2016/679[7]. Podnik by měl brát v úvahu zejména údaje, které jsou obchodním tajemstvím nebo citlivými údaji (například údaje o zdravotním stavu pojistníků).

Obecný pokyn 8 – Posouzení rizik externího zajištění cloudových služeb

30. Obecně by podnik měl přijmout přístup přiměřený povaze, rozsahu a komplexnosti rizik spojených se službami zajišťovanými externími poskytovateli cloudových služeb. To zahrnuje posouzení možného dopadu jakéhokoli externího zajištění cloudových služeb, zejména na jeho provozní rizika a rizika poškození dobré pověsti.

31. V případě externího zajištění rozhodujících nebo důležitých provozních funkcí nebo činností u poskytovatelů cloudových služeb by podnik měl přijmout tyto kroky:

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

b. posoudit, je-li to vhodné a přiměřené, rizika, včetně právních rizik, rizik IKT, rizik týkajících se dodržování právních předpisů a rizik poškození dobré pověsti a omezení dohledu vyplývající z:

   i. vybrané cloudové služby a navrhovaných modelů nasazení (tj. veřejné/soukromé/hybridní/komunitní);

   ii. migrace a/nebo provádění;

   iii. činností a souvisejících dat a systémů, u nichž se zvažuje externí zajištění (nebo které již jsou zajišťovány externě), a jejich citlivosti a požadovaných bezpečnostních opatření;

   iv. politické stability a bezpečnostní situace v zemích (uvnitř EU a mimo ni), kde jsou nebo mohou být poskytovány externě zajišťované služby a kde jsou nebo pravděpodobně budou uložena data. Posouzení by mělo zvážit:

      1. platné právní předpisy, včetně právních předpisů o ochraně údajů;

      2. platná ustanovení týkající se prosazování práva;

      3. ustanovení insolvenčního zákona, která by se použila v případě selhání poskytovatele služeb, a případná omezení, která by nastala v souvislosti s naléhavě nutnou obnovou dat podniku;

   v. dalšího externího zajištění, včetně dalších rizik, která mohou vzniknout, pokud se subdodavatel nachází ve třetí zemi nebo v jiné zemi než poskytovatel cloudových služeb, a rizika, že dlouhé a složité řetězce dalšího externího zajištění sníží schopnost podniku kontrolovat jeho rozhodující nebo důležité provozní funkce nebo činnosti a schopnost orgánů dohledu vykonávat nad nimi účinný dohled;

[7] 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).

vi. celkového rizika koncentrace podniků vůči stejnému poskytovateli cloudových služeb, včetně zajištění cloudových služeb u externího poskytovatele, který není snadno nahraditelný, nebo většího počtu ujednání o externím zajištění služeb nebo činností se stejným poskytovatelem cloudových služeb. Při posuzování rizika koncentrace by podnik (a/nebo případně skupina) měl vzít v úvahu všechna ujednání o externím zajištění cloudových služeb s tímto poskytovatelem cloudových služeb.

32. Posouzení rizik by mělo být provedeno před uzavřením dohody o externím zajištění cloudových služeb. Pokud se podnik dozví o závažných nedostatcích a/nebo významných změnách poskytovaných služeb nebo situace poskytovatele cloudových služeb, mělo by být posouzení rizik neprodleně přezkoumáno nebo provedeno znovu. V případě obnovení ujednání o externím zajištění cloudových služeb, pokud jde o jeho obsah a rozsah (například rozšíření rozsahu nebo zahrnutí rozhodujících nebo důležitých provozních funkcí, které dříve nebyly zahrnuty, do rozsahu), by mělo být znovu provedeno hodnocení rizik.

Obecný pokyn 9 – Hloubková kontrola poskytovatele cloudových služeb

33. Podnik by měl v rámci svého procesu výběru a posouzení zajistit, aby byl poskytovatel cloudových služeb vhodný podle kritérií definovaných v jeho písemné koncepci outsourcingu.

34. Před externím zajištěním jakékoli provozní funkce nebo činnosti by měla být provedena hloubková kontrola poskytovatele cloudových služeb. Pokud podnik uzavře druhou dohodu s poskytovatelem cloudových služeb, který již byl předmětem posouzení, měl by tento podnik na základě přístupu vycházejícího z rizik stanovit, zda je zapotřebí druhá hloubková kontrola. Pokud se podnik dozví o závažných nedostatcích a/nebo významných změnách poskytovaných služeb nebo situace poskytovatele cloudových služeb, měla by být hloubková kontrola neprodleně přezkoumána nebo provedena znovu.

35. V případě externího zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, by měla hloubková kontrola zahrnovat hodnocení vhodnosti poskytovatele cloudových služeb (například schopnosti, infrastruktura, ekonomická situace, status podniku a právní status). Podnik může případně na podporu prováděné hloubkové kontroly použít důkazy, osvědčení na základě mezinárodních norem, zprávy o auditu uznaných třetích stran nebo zprávy o vnitřním auditu.

Obecný pokyn 10 – Smluvní požadavky

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

37. Aniž jsou dotčeny požadavky stanovené v článku 274 nařízení v přenesené pravomoci, v případě externího zajištění služeb nebo činností, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, u poskytovatelů cloudových služeb by měla písemná dohoda mezi podnikem a poskytovatelem cloudových služeb stanovit:

a. jasný popis externě zajištěné funkce (cloudové služby, včetně typu podpůrných služeb);

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

c. soudní příslušnost a rozhodné právo dohody;

d. finanční závazky smluvních stran;

e. zda je povoleno další externí zajištění zásadní nebo důležité provozní funkce nebo činnosti (nebo jejich podstatných částí), a pokud ano, podmínky, kterým významné další externí zajištění podléhá (viz obecný pokyn 13);

f. místa (tj. regiony nebo země), kde budou uložena a zpracována příslušná data (umístění datových center) a podmínky, které musí být splněny, včetně požadavku informovat podnik v případě, že poskytovatel služeb navrhne změnit uvedená místa;

g. ustanovení týkající se přístupnosti, dostupnosti, integrity, důvěrnosti, ochrany soukromí a bezpečnosti příslušných dat s přihlédnutím ke specifikacím obecného pokynu 12;

h. právo podniku pravidelně sledovat výkonnost poskytovatele cloudových služeb;

i. dohodnuté úrovně služeb, které by měly zahrnovat přesné kvantitativní a kvalitativní výkonnostní cíle za účelem umožnění včasného monitorování, a tudíž i přijetí vhodných nápravných opatření bez zbytečného prodlení v případě, že dohodnuté úrovně služeb nejsou splněny;

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

k. zda by měl poskytovatel cloudových služeb uzavřít povinné pojištění určitých rizik, a případně požadované úrovně pojistného krytí;

l. požadavky provádět a testovat pohotovostní plány;

m. požadavek, aby poskytovatel cloudových služeb udělil podniku, jeho orgánům dohledu a jakékoli jiné osobě jmenované podnikem nebo orgány dohledu:

    i. plný přístup do všech relevantních firemních prostor (sídla a provozních středisek), včetně celé škály příslušných zařízení, systémů, sítí, informací a dat používaných při poskytování externě zajištěné funkce, včetně souvisejících finančních informací, personálu a externích auditorů poskytovatele cloudových služeb („práva na přístup“);

    ii. neomezená práva provádět v souvislosti s ujednáním o externím zajištění cloudových služeb kontroly a audity („práva na audit“) s cílem umožnit jim monitorovat ujednání o externím zajištění služeb nebo činností a zajistit dodržování všech příslušných regulačních a smluvních požadavků;

n. ustanovení s cílem zajistit, aby byla data vlastněná podnikem neprodleně získána podnikem v případě platební neschopnosti, řešení krize nebo ukončení obchodních operací poskytovatele cloudových služeb.

Obecný pokyn 11 – Práva na přístup a na audit

38. Dohoda o externím zajištění cloudových služeb by neměla omezovat účinné uplatňování práv podniku na přístup a na audit, ani možnosti kontroly cloudových služeb za účelem splnění jeho regulačních povinností.

39. Podnik by měl vykonávat svá práva na přístup a na audit, stanovit četnost auditu a oblasti a služby, které mají být na základě přístupu vycházejícího z rizik předmětem auditu, v souladu s oddílem 8 obecných pokynů k řídicímu a kontrolnímu systému orgánu EIOPA.

40. Při stanovení četnosti a rozsahu svého výkonu práv na přístup nebo na audit by měl podnik zvážit, zda je externí zajištění cloudových služeb spojeno s rozhodující nebo důležitou provozní funkcí nebo činností, a povahu a rozsah rizika a dopadu na podnik v důsledku ujednání o externím zajištění cloudových služeb.

41. Pokud výkon práv podniku na přístup nebo na audit nebo použití určitých technik auditu vytváří riziko pro prostředí poskytovatele cloudových služeb a/nebo jiného klienta poskytovatele cloudových služeb (například dopad na úrovně služeb, dostupnost dat, aspekty důvěrnosti), podnik a poskytovatel cloudových služeb by se měli dohodnout na alternativních způsobech poskytování podobné míry jistoty a služeb pro podnik (například zahrnutí konkrétních kontrol, které mají být testovány, do konkrétní zprávy nebo osvědčení, kterou (které) vytvořil poskytovatel cloudových služeb).

42. Aniž je dotčena konečná odpovědnost podniků za činnosti prováděné jejich poskytovateli cloudových služeb, mohou podniky za účelem účinnějšího využití auditních zdrojů a snížení organizační zátěže pro poskytovatele cloudových služeb a jeho zákazníků využít:

a. osvědčení vydaná třetí stranou a zprávy o auditu předložené třetí stranou nebo zprávy o vnitřním auditu zpřístupněné poskytovatelem cloudových služeb;

b. společné audity (tj. prováděné společně s ostatními klienty téhož poskytovatele cloudových služeb), nebo společné audity prováděné třetí stranou, kterou jmenují.

43. V případě externího zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, by podniky měly použít metodu uvedenou v odst. 42 písm. a) pouze v případě, že:

a. zaručí, že do oblasti působnosti osvědčení nebo zprávy o auditu spadají systémy (například procesy, aplikace, infrastruktura, datová centra atd.) a kontroly určené podnikem a posuzuje dodržování příslušných regulačních požadavků;

b. budou pravidelně důkladně posuzovat obsah nových osvědčení nebo zpráv o auditu a ověřovat, zda osvědčení nebo zprávy nejsou zastaralé;

c. zajistí, aby klíčové systémy a kontroly byly zahrnuty v budoucích verzích osvědčení nebo zprávy o auditu;

d. jsou spokojeny se způsobilostí strany, která provádí osvědčení nebo audit (například pokud jde o střídání společností provádějících osvědčení nebo audit, kvalifikaci, odborné znalosti, opakované provádění či ověření důkazních informací uvedených v auditorském spisu);

e. jsou přesvědčeny, že jsou osvědčení vydávána a audity prováděny podle příslušných standardů a zahrnují test provozní účelnosti zavedených klíčových kontrol;

f. mají smluvní právo požadovat rozšíření oblasti působnosti osvědčení nebo zpráv o auditu o další příslušné systémy a kontroly, přičemž počet a četnost takových žádostí o úpravu oblasti působnosti by měl být přiměřený a oprávněný z pohledu řízení rizik;

g. si zachovávají smluvní právo provádět jednotlivé audity na místě podle svého uvážení, pokud jde o externí zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností. Toto právo by mělo být vykonáno v případě zvláštních potřeb, kterým není možné vyhovět prostřednictvím jiných typů interakcí s poskytovatelem cloudových služeb.

44. V případě outsourcingu rozhodujících nebo důležitých provozních funkcí nebo činností u poskytovatelů cloudových služeb by podnik měl posoudit, zda jsou osvědčení vydaná třetí stranou a zprávy uvedené v odst. 42 písm. b) vhodné a postačují ke splnění jeho regulačních povinností, a na základě přístupu vycházejícího z rizik by se v průběhu času neměl spoléhat pouze na tyto zprávy a tato osvědčení.

45. Před plánovanou návštěvou na místě by strana, která má uplatnit své právo na přístup (podnik, auditor nebo třetí strana jednající jménem podniku/podniků), měla v přiměřené lhůtě poskytnout předchozí oznámení, s výjimkou případů, kdy včasné předchozí oznámení nebylo možné provést kvůli mimořádné nebo krizové situaci. Toto oznámení by mělo uvádět místo a účel návštěvy a pracovníky, kteří se návštěvy zúčastní.

46. Vzhledem k tomu, že cloudová řešení jsou po technické stránce značně složitá, podnik by měl ověřit, že zaměstnanci provádějící audit – ať už interní auditoři či skupina auditorů jednající jeho jménem, nebo auditoři jmenovaní poskytovatelem cloudových služeb – nebo případně zaměstnanci, kteří provádějí přezkoumání osvědčení vydaných třetí stranou nebo zpráv o auditu poskytovatele služeb, si osvojili příslušné dovednosti a znalosti potřebné k provádění odpovídajících auditů či posouzení.

Obecný pokyn 12 – Zabezpečení dat a systémů

47. Podnik by měl zajistit, aby poskytovatelé cloudových služeb dodržovali evropské a vnitrostátní právní předpisy a příslušné bezpečnostní normy IKT.

48. Kromě toho by v případě externího zajištění služeb nebo činností, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, u poskytovatelů cloudových služeb měl podnik v dohodě o externím zajištění cloudových služeb vymezit konkrétní požadavky na informační bezpečnost a pravidelně sledovat dodržování těchto požadavků.

49. Pro účely odstavce 48 by v případě externího zajištění služeb nebo činností, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, u poskytovatelů cloudových služeb měl podnik za současného uplatňování přístupu vycházejícího z rizik a zohlednění svých povinností a povinností poskytovatele cloudových služeb učinit tyto kroky:

a. dohodnout se na jasných úlohách a povinnostech poskytovatele cloudových služeb a podniku ve vztahu k provozním funkcím nebo činnostem ovlivněným externím zajištěním cloudových služeb, přičemž by tyto úlohy a povinnosti měly být jasně rozděleny;

b. vymezit a zvolit vhodnou úroveň ochrany důvěrných údajů, kontinuitu externě zajišťovaných činností, integritu a sledovatelnost dat a systémů v souvislosti se zamýšleným externím zajištěním cloudových služeb;

c. zvážit případná zvláštní opatření zaměřená na přenášená data, data v paměti a uložená data, například použití šifrovacích technologií ve spojení s vhodnou správou klíčů;

d. zvážit mechanismy integrace cloudových služeb se systémy podniků, například rozhraní pro programování aplikací a řádný proces správy uživatelů a přístupu;

e. pokud je to možné a proveditelné, smluvně zajistit, aby dostupnost provozu sítě a očekávaná kapacita splňovaly přísné požadavky na kontinuitu;

f. v příslušných případech vymezit a zvolit řádné požadavky na kontinuitu, které zajišťují přiměřené úrovně na každé úrovni technologického řetězce;

g. mít k dispozici řádný a dobře zdokumentovaný postup řešení incidentů včetně příslušných odpovědností, například prostřednictvím vymezení modelu spolupráce v případě výskytu skutečných incidentů nebo podezření na incidenty;

h. přijmout přístup vycházející z rizik, pokud jde o místa ukládání dat a zpracování dat (tj. zemi nebo region), a zvážit informační bezpečnost;

i. sledovat plnění požadavků týkajících se účinnosti a účelnosti kontrolních mechanismů zavedených poskytovatelem cloudových služeb, které by měly zmírňovat rizika spojená s poskytovanými službami.

Obecný pokyn 13 – Další externí zajištění rozhodujících nebo významných provozních funkcí nebo činností

50. Pokud je povoleno další externí zajištění rozhodujících nebo významných provozních funkcí (nebo jejich částí), dohoda o externím zajištění cloudových služeb mezi podnikem a poskytovatelem cloudových služeb by měla:

a. vymezit případné druhy činností, které jsou vyloučeny z případného dalšího externího zajištění;

b. uvádět podmínky, které musí být splněny v případě dalšího externího zajištění (například, že subdodavatel bude také plně dodržovat příslušné povinnosti poskytovatele cloudových služeb). Tyto povinnosti zahrnují právo na audit a na přístup a zabezpečení dat a systémů;

c. uvádět, že poskytovatel cloudových služeb přebírá plnou odpovědnost za služby, které jsou dále externě zajišťovány, a ponechá si dohled nad nimi;

d. zahrnovat závazek pro poskytovatele cloudových služeb, že bude podnik informovat o všech plánovaných významných změnách ohledně subdodavatelů nebo služeb, které jsou dále externě zajišťovány a které by mohly ovlivnit schopnost poskytovatele služeb plnit jeho povinnosti vyplývající ze dohody o externím zajištění cloudových služeb. Oznamovací lhůta pro tyto změny by měla podniku umožnit alespoň vypracovat posouzení rizik plynoucích z dopadů navrhovaných změn předtím, než skutečná změna týkající se subdodavatelů či služeb, které jsou dále externě zajišťovány, vstoupí v platnost;

e. zajistit, že má podnik v případech, kdy poskytovatel cloudových služeb plánuje provést změny subdodavatele nebo služeb, které jsou dále externě zajišťovány, jež by měly nepříznivý dopad na posouzení rizik dohodnutých služeb, právo vznést proti takovým změnám námitky a/nebo právo ukončit smlouvu a odstoupit od ní.

Obecný pokyn 14 – Sledování ujednání o externím zajištění cloudových služeb a dohled nad nimi

51. Podnik by měl pravidelně sledovat výkon činností, bezpečnostní opatření a dodržování dohodnutých úrovní služeb ze strany poskytovatelů cloudových služeb na základě přístupu vycházejícího z rizik. Hlavní důraz by měl být kladen na externí zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí.

52. Za tímto účelem by měl podnik zřídit mechanismy sledování a dohledu, které by měly, pokud je to možné a vhodné, zohledňovat existenci dalšího externího zajištění rozhodujících nebo významných provozních funkcí nebo jejich částí.

53. Správní, řídící nebo kontrolní orgán by měl pravidelně dostávat aktuální informace o rizicích zjištěných při externím zajišťování cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností.

54. S cílem zajistit odpovídající sledování a dohled nad ujednáními o externím zajištění cloudových služeb by podniky měly využívat dostatečné zdroje s odpovídajícími dovednostmi a znalostmi pro sledování služeb zajišťovaných prostřednictvím cloudu. Zaměstnanci podniku odpovědní za tyto činnosti by měli mít podle potřeby znalosti jak v oblasti IKT, tak v oblasti obchodu.

Obecný pokyn 15 – Právo na ukončení a strategie odstoupení

55. V případě externího zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, by podnik měl mít v rámci dohody o externím zajištění cloudových služeb jasně vymezenou doložku o strategii odstoupení, která zajišťuje, že v případě potřeby bude moci ujednání ukončit. Mělo by být možné ujednání ukončit, aniž by to mělo škodlivý vliv na kontinuitu a kvalitu poskytování služeb pojistníkům. Za tímto účelem by podnik měl:

a. vypracovat plány odstoupení, které jsou komplexní, založené na službách, zdokumentované a dostatečně testované (například provedením analýzy potenciálních nákladů, dopadů, zdrojů a časových dopadů jednotlivých potenciálních možností odstoupení);

b. určit alternativní řešení a vyvinout vhodné a proveditelné plány přechodu, které umožní podniku odstranit a převést stávající činnosti a data od poskytovatele cloudových služeb k alternativním poskytovatelům služeb nebo zpět do podniku. Tato řešení by měla být stanovena s ohledem na výzvy, které mohou nastat v důsledku umístění dat, a přijímat nezbytná opatření s cílem zajistit kontinuitu činnosti během přechodné fáze;

c. zajistit, aby poskytovatel cloudových služeb přiměřeně podporoval podnik při předávání externě zajištěných dat, systémů nebo aplikací jinému poskytovateli služeb nebo přímo podniku;

d. uzavřít dohodu s poskytovatelem cloudových služeb, že jakmile budou data podniku znovu přenesena do podniku, budou poskytovatelem cloudových služeb zcela a bezpečně vymazána, a to ve všech regionech.

56. Při vytváření strategií odstoupení by měl podnik zvážit, zda přichází v úvahu:

a. stanovit cíle strategie odstoupení;

b. stanovit rozhodné události (například klíčové ukazatele rizik vykazující nepřijatelnou úroveň služeb), které by mohly vést k aktivaci strategie odstoupení;

c. provést analýzu dopadů přiměřenou externě zajištěným činnostem, aby bylo možné určit, jaké lidské a další zdroje by byly potřebné k provedení plánu odstoupení a jak dlouho by to trvalo;

d. přidělit úlohy a povinnosti v rámci správy plánů odstoupení a přechodových činností;

e. definovat kritéria úspěšnosti přechodu.

Obecný pokyn 16 – Dohled nad ujednáními o externím zajištění cloudových služeb ze strany orgánů dohledu

57. Orgány dohledu by měly v rámci procesu kontroly orgánem dohledu provádět analýzu dopadů vyplývajících z ujednání podniků o externím zajištění cloudových

služeb. Analýza dopadů by se měla zaměřit zejména na ujednání týkající se externího zajištění rozhodujících nebo významných provozních funkcí nebo činností.

58. Orgány dohledu by měly při dohledu nad ujednáními podniků o externím zajištění cloudových služeb zvážit tato rizika:

a. rizika IKT;

b. další operační rizika (včetně právního rizika a rizika týkajícího se dodržování právních předpisů, rizika externího zajištění služeb nebo činností a rizika řízení třetích stran);

c. riziko poškození dobré pověsti;

d. riziko koncentrace, a to i na úrovni země/odvětví.

59. Orgány dohledu by do svého posouzení měly zahrnout následující aspekty přístupu vycházejícího z rizik:

a. přiměřenost a účinnost procesů řízení a kontroly a provozních procesů podniku, které souvisejí se schvalováním, prováděním, sledováním, řízením a obnovou ujednání o externím zajištění cloudových služeb;

b. skutečnost, zda má podnik dostatečné zdroje s odpovídajícími dovednostmi a znalostmi pro sledování služeb zajišťovaných prostřednictvím cloudu;

c. skutečnost, zda podnik určuje a řídí všechna rizika, na něž upozorňují tyto obecné pokyny.

60. V případě skupin by měl orgán dohledu nad skupinou zajistit, aby se dopady externího zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, odrážely v posouzení rizik dohledu nad skupinou, a měl by zohlednit požadavky uvedené v odstavcích 58–59 a individuální vlastnosti řízení a kontroly a provozní vlastnosti skupiny.

61. Pokud externí zajištění cloudových služeb, které se týkají rozhodujících nebo důležitých provozních funkcí nebo činností, zahrnuje více než jeden podnik v různých členských státech a je řízeno centrálně mateřskou společností nebo dceřinou společností skupiny (například podnikem nebo společností poskytující služby skupině, jako je poskytovatel IKT skupiny), orgán dohledu nad skupinou a/nebo příslušné orgány dohledu nad podniky, které se podílejí na externím zajištění cloudových služeb, by měly v kolegiu orgánů dohledu případně projednat dopady externího zajištění cloudových služeb na rizikový profil skupiny.

62. Jsou-li zjištěny problémy, které vedou k závěru, že podnik přestal mít stabilní systém správy a řízení nebo že nedodržuje regulační požadavky, měly by orgány dohledu přijmout vhodná opatření, která mohou zahrnovat například nařízení, aby podniky zlepšily systém správy a řízení, omezení rozsahu nebo zákaz externě zajišťovaných funkcí nebo požadavek ukončit jedno nebo více ujednání o externím zajištění služeb. S přihlédnutím k potřebě zajistit nepřetržitý provoz podniku by mohlo být ukončení smluv vyžadováno zejména v případě, že není možné dohled nad regulačními požadavky a jejich prosazování zajistit jinými způsoby.

Pravidla pro dodržování předpisů a oznamování

63. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení Evropského parlamentu a Rady (EU) č. 1094/2010. V souladu s čl. 16 odst. 3 tohoto nařízení musí příslušné orgány a finanční instituce vynaložit veškeré úsilí, aby se obecnými pokyny a doporučeními řídily.

64. Příslušné orgány, které se těmito obecnými pokyny řídí nebo hodlají řídit, by je měly vhodným způsobem začlenit do svého rámce regulace nebo dohledu.

65. Příslušné orgány musí orgánu EIOPA potvrdit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést důvody, proč se jimi neřídí nebo nehodlají řídit, a to do dvou měsíců od vydání přeložených znění doporučení.

66. Pokud v této lhůtě nebude obdržena odpověď, bude se mít za to, že příslušné orgány nedodržely oznamovací povinnost, a budou jako takové vykazovány.

Závěrečné ustanovení o přezkoumání

67. Tyto obecné pokyny podléhají přezkoumání ze strany orgánu EIOPA.