30/09/2025
ESMA65-294529287-4737

Usmernenia

týkajúce sa outsourcingu poskytovateľom cloudových služieb

Obsah

1 Rozsah pôsobnosti

Adresáti usmernení

1. Tieto usmernenia sa vzťahujú na príslušné orgány a i) depozitárov alternatívnych investičných fondov (AIF) uvedených v článku 21 ods. 3 písm. c) a v článku 21 ods. 3 treťom pododseku smernice AIFMD, ak nie sú finančnými subjektmi, na ktoré sa uplatňuje DORA, a ii) depozitárov PKIPCP uvedených v článku 23 ods. 2 písm. c) smernice PKIPCP, ak nie sú finančnými subjektmi, na ktoré sa uplatňuje DORA.[1]

Predmet usmernení

2. Tieto usmernenia sa uplatňujú v súvislosti s týmito ustanoveniami:

   a) Pokiaľ ide o depozitárov AIF: článok 21 smernice AIFMD; článok 98 delegovaného nariadenia Komisie (EÚ) 2013/231;

   b) Pokiaľ ide o depozitárov PKIPCP: články 22, 22a a 23 ods. 2 smernice o PKIPCP; článok 32 smernice Komisie 2010/43/EÚ; článok 2 ods. 2 písm. j), článok 3 ods. 1, článok 13 ods. 2, články 15, 16 a 22 delegovaného nariadenia Komisie (EÚ) 2016/438.

Časové obdobie

3. Tieto usmernenia sa uplatňujú odo dňa ich uverejnenia na webovom sídle orgánu ESMA vo všetkých úradných jazykoch EÚ a na všetky dohody o cloudovom outsourcingu uzavreté, obnovené alebo zmenené k tomuto dátumu alebo po ňom.

4. Vzhľadom na uplatňovanie nariadenia DORA sa predchádzajúce usmernenia orgánu ESMA o externom zabezpečovaní činností poskytovateľmi cloudových služieb prestávajú uplatňovať na tie finančné subjekty, na ktoré sa vzťahuje nariadenie DORA, uvedené v článku 2 toho istého nariadenia. V prípade depozitárov AIF a depozitárov PKIPCP uvedených v odseku 1 sa predchádzajúce usmernenia ESMA o externom zabezpečovaní činností poskytovateľmi cloudových služieb budú naďalej uplatňovať až do dátumu uverejnenia týchto usmernení na webovom sídle ESMA vo všetkých úradných jazykoch EÚ.

[1] Pokiaľ ide o dohody o využívaní cloudových služieb, finančné subjekty definované v článku 2 ods. 1 a 2 nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (nariadenie DORA) podliehajú osobitným pravidlám stanoveným v nariadení DORA a v súvisiacich delegovaných a vykonávacích nariadeniach Komisie.

2 Odkazy na právne predpisy, skratky a vymedzenie pojmov

2.1 Odkazy na právne predpisy

Nariadenie o ESMA	nariadenie Európskeho parlamentu a Rady (EÚ) č. 1095/2010 z 24. novembra 2010, ktorým sa zriaďuje európsky orgán dohľadu (Európsky orgán pre cenné papiere a trhy) a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/77/ES[2]
Smernica o správcoch AIF	smernica Európskeho parlamentu a Rady 2011/61/EÚ z 8. júna 2011 o správcoch alternatívnych investičných fondov a o zmene a doplnení smerníc 2003/41/ES a 2009/65/ES a nariadení (ES) č. 1060/2009 a (EÚ) č. 1095/2010[3]
Delegované nariadenie Komisie (EÚ) 2013/231	delegované nariadenie Komisie (EÚ) 2013/231 z 19. decembra 2012, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2011/61/EÚ, pokiaľ ide o výnimky, všeobecné podmienky výkonu činnosti, depozitárov, pákový efekt, transparentnosť a dohľad[4]
Smernica o PKIPCP	smernica Európskeho parlamentu a Rady 2009/65/ES z 13. júla 2009 o koordinácii zákonov, iných právnych predpisov a správnych opatrení týkajúcich sa podnikov kolektívneho investovania do prevoditeľných cenných papierov (PKIPCP)[5]
Smernica Komisie 2010/43/EÚ	smernica Komisie 2010/43/EÚ z 1. júla 2010, ktorou sa vykonáva smernica Európskeho parlamentu a Rady 2009/65/ES, pokiaľ ide o organizačné požiadavky, konflikty záujmov, pravidlá výkonu činnosti, riadenie rizík a obsah dohody medzi depozitárom a správcovskou spoločnosťou[6]
DORA	nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009,

[2] Ú. v. EÚ L 331, 15.12.2010, s. 84.
[3] Ú. v. EÚ L 174, 1.7.2011, s. 1.
[4] Ú. v. EÚ L 83, 22.3.2013, s. 1.
[5] Ú. v. EÚ L 302, 17.11.2009, s. 32.
[6] Ú. v. EÚ L 176, 10.7.2010, s. 42.

	(EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011[7]
GDPR	nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES[8]

2.2 Skratky

ESMA	Európsky orgán pre cenné papiere a trhy
EÚ	Európska únia
PCS	Poskytovateľ cloudových služieb

2.3 Vymedzenie pojmov

funkcia	je akýkoľvek postup, služba alebo činnosť;
zásadná alebo dôležitá funkcia	je akákoľvek funkcia, ktorej chyba alebo zlyhanie jej vykonávania by podstatne zhoršilo: a) plnenie povinností spoločnosti podľa platných právnych predpisov; b) finančnú výkonnosť spoločnosti alebo c) dobrý stav alebo kontinuitu hlavných služieb a činností spoločnosti;
cloudové služby	sú služby poskytované pomocou cloud computingu;
cloud computing alebo cloud[9]	je paradigma, ktorá umožňuje sieťový prístup ku škálovateľnému a pružnému súboru fyzických alebo virtuálnych zdrojov, ktoré možno zdieľať (napríklad k serverom, operačným systémom, sieťam, softvéru, aplikáciám a úložiskám) so samoobslužným poskytovaním a správou na požiadanie;

[7] *Ú. v. EÚ L 333, 27.12.2022, s. 1 – 79.*
[8] Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88.
[9] Cloud computing sa často skracuje na „cloud“. Pre zjednodušenie sa vo zvyšnej časti dokumentu používa pojem „cloud“.

poskytovateľ cloudových služieb	je tretia strana poskytujúca cloudové služby podľa dohody o cloudovom outsourcingu;
dohoda o cloudovom outsourcingu	je dohoda v akejkoľvek forme vrátane dohody o delegovaní uzatvorená medzi: (i) spoločnosťou a poskytovateľom cloudových služieb, na základe ktorej tento poskytovateľ cloudových služieb vykonáva funkciu, ktorú by inak vykonávala samotná spoločnosť; alebo (ii) spoločnosťou a treťou stranou, ktorá nie je poskytovateľom cloudových služieb, no ktorá v značnej miere využíva poskytovateľa cloudových služieb na vykonávanie funkcie, ktorú by inak vykonávala samotná spoločnosť. V tomto prípade sa odkaz na poskytovateľa cloudových služieb v týchto usmerneniach považuje za odkaz na takúto tretiu stranu;
sub-outsourcing	je situácia, keď PCS ďalej presúva funkciu zabezpečovanú prostredníctvom outsourcingu (alebo jej časť) inému poskytovateľovi služieb podľa dohody o outsourcingu;
model zavedenia cloudu	je spôsob, akým možno organizovať cloud na základe kontroly a spoločného využívania fyzických alebo virtuálnych zdrojov. Modely zavedenia cloudu zahŕňajú komunitné[10], hybridné[11], súkromné[12] a verejné[13] cloudy;
spoločnosti	a) depozitári uvedení v článku 21 ods. 3 písm. c) a v článku 21 ods. 3 treťom pododseku smernice AIFMD („depozitári alternatívnych investičných fondov (AIF)“);

[10] Model zavedenia cloudu, pri ktorom cloudové služby podporujú výhradne osobitnú skupinu zákazníkov cloudových služieb, ktorí ich spoločne využívajú a ktorí majú spoločné požiadavky a vzájomný vzťah, a pri ktorom zdroje spravuje aspoň jeden člen tejto skupiny.
[11] Model zavedenia cloudu, pri ktorom sa využívajú aspoň dva rôzne modely zavedenia cloudu.
[12] Model zavedenia cloudu, pri ktorom cloudové služby využíva výhradne jeden zákazník cloudových služieb, ktorý takisto spravuje zdroje.
[13] Model zavedenia cloudu, pri ktorom sú cloudové služby potenciálne dostupné ktorémukoľvek zákazníkovi cloudových služieb a zdroje spravuje poskytovateľ cloudových služieb.

b) depozitári uvedení v článku 23 ods. 2 písm. c) smernice o PKIPCP („depozitári PKIPCP“).

3 Účel

5. Tieto usmernenia sa zakladajú na článku 16 ods. 1 nariadenia o ESMA. Cieľom týchto usmernení je vytvoriť konzistentné, efektívne a účinné postupy dohľadu v rámci Európskeho systému finančného dohľadu (ESFS) a zaistiť spoločné, jednotné a konzistentné uplatňovanie požiadaviek uvedených v oddiele 1.1 v časti Predmet usmernení v prípadoch, keď spoločnosti prostredníctvom outsourcingu využívajú poskytovateľov cloudových služieb. Cieľom týchto usmernení je najmä pomôcť spoločnostiam a príslušným orgánom zistiť, riešiť a monitorovať riziká a výzvy vyplývajúce z dohôd o cloudovom outsourcingu, rozhodnutia využiť outsourcing, výberu poskytovateľa cloudových služieb, monitorovania činností zabezpečovaných prostredníctvom outsourcingu a zabezpečenia stratégií ukončenia angažovanosti.

4 Povinnosti týkajúce sa dodržiavania predpisov a oznamovania

4.1 Štatút týchto usmernení

6. Podľa článku 16 ods. 3 nariadenia o ESMA príslušné orgány a spoločnosti vynaložia všetko úsilie na dodržanie týchto usmernení.

7. Príslušné orgány, na ktoré sa tieto usmernenia vzťahujú, majú zabezpečiť ich dodržiavanie tak, že ich podľa okolností začlenia do svojich vnútroštátnych právnych rámcov a/alebo rámcov pre dohľad vrátane prípadov, ak sú osobitné usmernenia v rámci dokumentu určené najmä spoločnostiam. V takom prípade by mali príslušné orgány prostredníctvom dohľadu zabezpečiť, aby spoločnosti tieto usmernenia dodržiavali.

4.2 Požiadavky na oznamovanie

8. Do dvoch mesiacov od dátumu uverejnenia usmernení na webovom sídle orgánu ESMA vo všetkých úradných jazykoch EÚ príslušné orgány, na ktoré sa tieto usmernenia vzťahujú, musia informovať orgán ESMA o tom, či i) dodržali, ii) nedodržali, ale majú v úmysle dodržať, alebo iii) nedodržali a nemajú v úmysle dodržať tieto usmernenia.

9. V prípade nedodržania musia príslušné orgány do dvoch mesiacov od dátumu uverejnenia usmernení na webovom sídle ESMA vo všetkých úradných jazykoch EÚ

takisto informovať orgán ESMA o svojich dôvodoch nedodržania týchto usmernení. Vzor oznámení je k dispozícii na webovom sídle orgánu ESMA. Po vyplnení sa vzor musí odoslať orgánu ESMA.

10. Spoločnosti nie sú povinné oznámiť, či dodržiavajú tieto usmernenia.

5 Usmernenia týkajúce sa zverenia výkonu činností externým poskytovateľom cloudových služieb

Usmernenie 1. Riadenie, dohľad a dokumentácia

11. Spoločnosť by mala mať definovanú a aktualizovanú stratégiu cloudového outsourcingu, ktorá je v súlade s relevantnými stratégiami a internými politikami a postupmi spoločnosti, a to aj v súvislosti s informačnými a komunikačnými technológiami, informačnou bezpečnosťou a riadením operačného rizika.

12. Spoločnosť by mala:

    a) jasne prideliť zodpovednosť za dokumentáciu, riadenie a kontrolu dohôd o cloudovom outsourcingu v rámci svojej organizácie;
    b) prideliť dostatok zdrojov na zabezpečenie plnenia týchto usmernení a všetkých právnych požiadaviek vzťahujúcich sa na jej dohody o cloudovom outsourcingu;
    c) zriadiť funkciu dohľadu nad cloudovým outsourcingom alebo určiť vedúcich pracovníkov, ktorí sa budú priamo zodpovedať riadiacemu orgánu a budú zodpovední za riadenie rizík súvisiacich s dohodami o cloudovom outsourcingu a za dohľad nad týmito rizikami. Pri dodržiavaní týchto usmernení by mali spoločnosti zohľadňovať povahu, rozsah a komplexnosť svojich podnikateľských činností, a to aj pokiaľ ide o riziká pre finančný systém a riziká súvisiace s funkciami zabezpečovanými prostredníctvom outsourcingu, a zaistiť, že ich riadiaci orgán má dostatok odborných zručností na pochopenie rizík súvisiacich s dohodami o cloudovom outsourcingu. Malé a menej komplexné spoločnosti by mali zaručiť aspoň jasné rozdelenie úloh a zodpovednosti za riadenie dohôd o cloudovom outsourcingu a dohľad nad nimi.

13. Spoločnosť by mala monitorovať vykonávanie činností, bezpečnostné opatrenia a dodržiavanie dohodnutých úrovní poskytovania služieb jej poskytovateľmi cloudových služieb. Toto monitorovanie by malo vychádzať z rizík a malo by sa zameriavať najmä na zásadné alebo dôležité funkcie, ktoré sa zabezpečujú prostredníctvom outsourcingu.

14. Spoločnosť by mala prehodnocovať, či sa jej dohody o cloudovom outsourcingu týkajú zásadnej alebo dôležitej funkcie, a to pravidelne a vždy vtedy, keď sa významne

zmenilo riziko, povaha alebo rozsah funkcie zabezpečovanej prostredníctvom outsourcingu.

15. Spoločnosť by mala viesť aktuálny register informácií o všetkých svojich dohodách o cloudovom outsourcingu a pritom rozlišovať medzi outsourcingom zásadných alebo dôležitých funkcií a inými dohodami o outsourcingu. Pri rozlišovaní medzi outsourcingom zásadných alebo dôležitých funkcií a inými dohodami o outsourcingu by mala stručne zhrnúť dôvody, prečo sa funkcia zabezpečovaná prostredníctvom outsourcingu považuje alebo nepovažuje za zásadnú alebo dôležitú. Pri zohľadnení vnútroštátneho práva by spoločnosť mala primerane dlho viesť aj záznamy o ukončených dohodách o cloudovom outsourcingu.

16. V prípade dohôd o cloudovom outsourcingu, ktoré sa týkajú zásadných alebo dôležitých funkcií, by mali byť v registri obsiahnuté aspoň tieto informácie o každej dohode o cloudovom outsourcingu:

    a) referenčné číslo;
    b) dátum začiatku a prípadne dátum ďalšieho predĺženia zmluvy, dátum ukončenia a/alebo výpovedné lehoty pre poskytovateľa cloudových služieb a pre spoločnosť;
    c) stručný opis funkcie zabezpečovanej prostredníctvom outsourcingu vrátane údajov, ktoré sa zabezpečujú prostredníctvom outsourcingu, a informácie, či tieto údaje obsahujú osobné údaje (napríklad odpovedaním áno alebo nie v samostatnom dátovom poli);
    d) kategória pridelená spoločnosťou, ktorá odráža povahu funkcie zabezpečovanej prostredníctvom outsourcingu (napríklad funkcia informačných technológií, kontrolná funkcia), čo by malo zjednodušiť identifikáciu rôznych druhov dohôd o cloudovom outsourcingu;
    e) informáciu o tom, či funkcia zabezpečovaná prostredníctvom outsourcingu podporuje podnikateľské činnosti, ktoré sú kritické z hľadiska času;
    f) názov a značka (ak existuje) poskytovateľa cloudových služieb, krajina jeho registrácie, jeho registračné číslo, identifikátor právnickej osoby (ak je k dispozícii), adresa sídla, relevantné kontaktné údaje a názov jeho materskej spoločnosti (ak existuje);
    g) rozhodné právo dohody o cloudovom outsourcingu a prípadne voľba jurisdikcie;
    h) druh cloudových služieb a modelov zavedenia a osobitná povaha údajov, ktoré sa majú uchovávať, a miesta (konkrétne regióny alebo krajiny), kde sa môžu takéto údaje uchovávať;
    i) dátum najnovšieho posúdenia zásadnosti alebo dôležitosti funkcie zabezpečovanej prostredníctvom outsourcingu a dátum nasledujúceho plánovaného posúdenia;
    j) dátum najnovšieho posúdenia rizík/auditu poskytovateľa cloudových služieb spolu so stručným zhrnutím hlavných výsledkov a dátum nasledujúceho plánovaného posúdenia rizík/auditu;
    k) názov samostatného alebo rozhodovacieho orgánu v spoločnosti, ktorý schválil dohodu o cloudovom outsourcingu;

l) v príslušných prípadoch názvy všetkých subdodávateľov, ktorí prostredníctvom sub-outsourcingu zabezpečujú zásadnú alebo dôležitú funkciu (alebo jej významné časti) vrátane krajín, kde sú takíto subdodávatelia zaregistrovaní, kde sa bude služba zabezpečovaná prostredníctvom sub-outsourcingu vykonávať a miesta (konkrétne regióny alebo krajiny), kde sa budú údaje uchovávať;
m) odhadované ročné rozpočtové náklady na dohodu o cloudovom outsourcingu.

17. V prípade dohôd o cloudovom outsourcingu týkajúcich sa funkcií, ktoré nie sú zásadné alebo dôležité, by mala spoločnosť definovať informácie, ktoré je potrebné zahrnúť do registra, na základe povahy, rozsahu a komplexnosti rizík súvisiacich s touto funkciou zabezpečovanou prostredníctvom outsourcingu.

Usmernenie 2. Predbežná analýza outsourcingu a náležitá starostlivosť

18. Pred uzatvorením akejkoľvek dohody o cloudovom outsourcingu by mala spoločnosť:

a) posúdiť, či sa dohoda o cloudovom outsourcingu týka zásadnej alebo dôležitej funkcie;
b) identifikovať a posúdiť všetky relevantné riziká dohody o cloudovom outsourcingu;
c) vykonať vhodnú náležitú starostlivosť v súvislosti s potenciálnym poskytovateľom cloudových služieb;
d) nájsť a posúdiť akýkoľvek konflikt záujmov, ktorý môže outsourcing spôsobiť.

19. Predbežná analýza outsourcingu a náležitá starostlivosť týkajúce sa potenciálneho poskytovateľa cloudových služieb by mali byť primerané povahe, rozsahu a komplexnosti funkcie, ktorú plánuje spoločnosť zabezpečovať prostredníctvom outsourcingu, a rizikám súvisiacim s touto funkciou. Mala by zahŕňať aspoň posúdenie potenciálneho vplyvu dohody o cloudovom outsourcingu na operačné a právne riziká spoločnosti, riziká nedodržania súladu s predpismi a riziká poškodenia dobrej povesti spoločnosti.

20. Ak sa dohoda o cloudovom outsourcingu týka zásadnej alebo dôležitej funkcie, spoločnosť by mala takisto:

a) posúdiť všetky príslušné riziká, ktoré môžu vzniknúť v dôsledku dohody o cloudovom outsourcingu vrátane rizík v súvislosti s informačnými a komunikačnými technológiami, informačnou bezpečnosťou a kontinuitou činností, právnych rizík a rizík nedodržania súladu s predpismi, rizík poškodenia dobrej povesti, operačných rizík a možných obmedzení súvisiacich s dohľadom pre spoločnosť, ktoré vyplývajú:
   i. z vybranej cloudovej služby a navrhnutých modelov zavedenia;
   ii. z postupov migrácie a/alebo implementácie;

iii. z citlivosti danej funkcie a súvisiacich údajov, o ktorých outsourcingu sa uvažuje, a bezpečnostných opatrení, ktoré by sa museli prijať;

iv. z interoperability systémov a aplikácií spoločnosti a poskytovateľa cloudových služieb, konkrétne ich schopnosti vymieňať si informácie a navzájom používať vymenené informácie;

v. z prenosnosti údajov spoločnosti, konkrétne schopnosti jednoducho prenášať údaje spoločnosti od jedného poskytovateľa cloudových služieb druhému alebo naspäť do spoločnosti;

vi. z politickej stability, bezpečnostnej situácie a právneho systému (vrátane zavedených ustanovení o presadzovaní práva, ustanovení konkurzného práva, ktoré by sa uplatňovali v prípade konkurzu poskytovateľa cloudových služieb, platných zákonov o ochrane údajov a toho, či sú splnené podmienky pre prenos osobných údajov do tretej krajiny podľa nariadenia GDPR) krajín (v rámci EÚ alebo mimo EÚ), kde by sa funkcie zabezpečované prostredníctvom outsourcingu poskytovali a kde by sa uchovávali údaje získané prostredníctvom outsourcingu; v prípade sub-outsourcingu ďalšie riziká, ktoré môžu vzniknúť, ak sa subdodávateľ nachádza v tretej krajine alebo v inej krajine než PCS, a v prípade sub-outsourcingového reťazca všetky ďalšie riziká, ktoré môžu vzniknúť, a to aj v súvislosti s neexistenciou priamej zmluvy medzi spoločnosťou a subdodávateľom vykonávajúcim funkciu zabezpečovanú prostredníctvom outsourcingu;

vii. z možnej koncentrácie v rámci spoločnosti (prípadne na úrovni jej skupiny) spôsobenej viacerými dohodami o cloudovom outsourcingu s tým istým poskytovateľom cloudových služieb ako aj z možnej koncentrácie v rámci finančného sektora EÚ spôsobenej tým, že viaceré spoločnosti využívajú toho istého poskytovateľa cloudových služieb alebo malú skupinu poskytovateľov cloudových služieb. Pri posudzovaní rizika koncentrácie by spoločnosť mala zohľadniť aj všetky svoje dohody o cloudovom outsourcingu (a prípadne dohody o cloudovom outsourcingu na úrovni jej skupiny) s daným poskytovateľom cloudových služieb;

b) zohľadniť očakávané prínosy a náklady dohody o cloudovom outsourcingu vrátane porovnania významných rizík, ktoré je možné znížiť alebo lepšie riadiť, s významnými rizikami, ktoré môžu vzniknúť v dôsledku dohody o cloudovom outsourcingu.

21. V prípade outsourcingu zásadných alebo dôležitých funkcií by náležitá starostlivosť mala zahŕňať vyhodnotenie vhodnosti daného poskytovateľa cloudových služieb. Pri posudzovaní vhodnosti poskytovateľa cloudových služieb by mala spoločnosť zabezpečiť, že daný PCS má dobrú obchodnú povesť, schopnosti, zdroje (vrátane ľudských, IT a finančných), organizačnú štruktúru a prípadne príslušné povolenie/-ia alebo registráciu/-ie na spoľahlivé a profesionálne vykonávanie zásadnej alebo dôležitej funkcie a na plnenie si svojich záväzkov počas celého trvania dohody

o cloudovom outsourcingu. Ďalšie faktory, ktoré treba zvážiť pri vykonávaní náležitej starostlivosti v súvislosti s poskytovateľom cloudových služieb, zahŕňajú okrem iného:

a) riadenie informačnej bezpečnosti a najmä ochrany osobných, dôverných alebo inak citlivých údajov;
b) servisná podpora vrátane plánov podpory a kontaktov a postupy riadenia incidentov;
c) plán kontinuity činností a plán obnovy po havárii.

22. V príslušných prípadoch a s cieľom podporiť vykonávanú náležitú starostlivosť môže spoločnosť použiť aj osvedčenia na základe medzinárodných noriem a správy o internom alebo externom audite.

23. Ak spoločnosť zistí významné nedostatky a/alebo významné zmeny v poskytovaných službách alebo v situácii poskytovateľa cloudových služieb, mala by sa predbežná analýza outsourcingu a náležitá starostlivosť súvisiaca s poskytovateľom cloudových služieb bezodkladne preskúmať alebo v potrebných prípadoch vykonať znovu.

24. Ak spoločnosť s poskytovateľom cloudových služieb, ktorý už bol posúdený, uzavrie novú dohodu alebo predĺži existujúcu dohodu, mala by na základe prístupu vychádzajúceho z posúdenia rizík určiť, či je potrebná nová náležitá starostlivosť.

Usmernenie 3. Hlavné zmluvné prvky

25. Príslušné práva a povinnosti spoločnosti a jej poskytovateľa cloudových služieb by mali byť jasne stanovené v písomnej dohode.

26. Táto písomná dohoda by mala výslovne umožňovať spoločnosti ju v prípade potreby ukončiť.

27. V prípade outsourcingu zásadných alebo dôležitých funkcií by mala písomná dohoda obsahovať aspoň:

a) jasný opis funkcie, ktorá sa má zabezpečovať prostredníctvom outsourcingu;
b) dátum začiatku a prípadne dátum ukončenia dohody, ako aj výpovedné lehoty pre poskytovateľa cloudových služieb a spoločnosť;
c) rozhodné právo dohody a prípadne voľba jurisdikcie;
d) finančné záväzky spoločnosti a poskytovateľa cloudových služieb;
e) informáciu o tom, či je povolený sub-outsourcing a ak áno, za akých podmienok, so zreteľom na usmernenie 7;
f) miesto alebo miesta (konkrétne regióny alebo krajiny), kde sa funkcia zabezpečovaná prostredníctvom outsourcingu bude poskytovať a kde sa údaje

budú spracovávať a uchovávať, ako aj podmienky, ktoré musia byť splnené, vrátane požiadavky informovať spoločnosť, ak PCS navrhne zmenu miesta alebo miest;

g) ustanovenia týkajúce sa informačnej bezpečnosti a ochrany osobných údajov s ohľadom na usmernenie 4;

h) právo spoločnosti pravidelne monitorovať plnenie dohody o cloudovom outsourcingu poskytovateľom cloudových služieb s ohľadom na usmernenie 6;

i) dohodnuté úrovne poskytovaných služieb, ktoré by mali zahŕňať kvantitatívne a kvalitatívne ciele výkonnosti, aby sa zabezpečilo včasné monitorovanie a mohli sa prijať náležité opravné opatrenia bez zbytočného odkladu, ak dohodnuté úrovne poskytovaných služieb nie sú dodržané;

j) oznamovacie povinnosti poskytovateľa cloudových služieb voči spoločnosti a prípadne povinností predkladať správy relevantné pre bezpečnostnú funkciu spoločnosti a pre kľúčové funkcie, napríklad správy vyhotovené funkciou vnútorného auditu poskytovateľa cloudových služieb;

k) ustanovenia týkajúce sa riadenia incidentov poskytovateľom cloudových služieb vrátane povinnosti poskytovateľa cloudových služieb bezodkladne oznamovať spoločnosti incidenty, ktoré ovplyvnili prevádzku zazmluvnenej služby spoločnosti;

l) skutočnosť, či by PCS mal uzavrieť povinné poistenie proti určitým rizikám a prípadne úroveň požadovaného poistného krytia;

m) požiadavky, aby PCS zaviedol a otestoval plán kontinuity činností a plán obnovy po havárii;

n) požiadavka, aby PCS udelil spoločnosti, jej príslušným orgánom a akejkoľvek inej osobe určenej spoločnosťou alebo príslušnými orgánmi právo na prístup („prístupové práva“) a audit („audítorské práva“) príslušných informácií, priestorov, systémov a zariadení poskytovateľa cloudových služieb do takej miery, aká je potrebná na monitorovanie plnenia dohody o cloudovom outsourcingu poskytovateľom cloudových služieb a na monitorovanie dodržiavania platných regulačných a zmluvných požiadaviek poskytovateľom cloudových služieb s ohľadom na usmernenie 6;

o) ustanovenia, ktorých cieľom je zabezpečiť, že údaje, ktoré PCS spracúva alebo uchováva v mene spoločnosti, budú v prípade potreby dostupné, obnovené a vrátené spoločnosti s ohľadom na usmernenie 5.

Usmernenie 4. Informačná bezpečnosť

28. Spoločnosť by mala vo svojich interných politikách a postupoch a v písomnej dohode o cloudovom outsourcingu stanoviť požiadavky na informačnú bezpečnosť a priebežne monitorovať ich plnenie vrátane požiadaviek na ochranu dôverných, osobných alebo

inak citlivých údajov. Tieto požiadavky by mali byť primerané povahe, rozsahu a komplexnosti funkcie, ktorú pre spoločnosť zabezpečuje PCS prostredníctvom outsourcingu, a rizikám súvisiacim s touto funkciou.

29. Na tento účel by mala spoločnosť v prípade outsourcingu zásadných alebo dôležitých funkcií a bez toho, aby sa to dotklo príslušných požiadaviek podľa nariadenia GDPR, s využitím prístupu vychádzajúceho z hodnotenia rizík aspoň:

a) *organizácia informačnej bezpečnosti:* zabezpečiť, že medzi spoločnosťou a poskytovateľom cloudových služieb sú jasne rozdelené úlohy a zodpovednosť týkajúce sa informačnej bezpečnosti, a to aj v súvislosti so zisťovaním ohrození, riadením incidentov a riadením opráv, a zabezpečiť, že PCS si dokáže účinne plniť svoje úlohy a dodržiavať zodpovednosť;
b) *správa systému identifikačných dát a prístupu*: zabezpečiť zavedenie silných mechanizmov autentifikácie (napríklad viacúrovňová autentifikácia) a kontrol prístupu s cieľom zabrániť neoprávnenému prístupu k údajom spoločnosti a backendovým cloudovým zdrojom;
c) *riadenie šifrovania a kľúčov:* zabezpečiť, aby sa na tranzitné údaje, údaje v pamäti, údaje v pokoji a zálohované údaje v prípade potreby používali príslušné šifrovacie technológie v kombinácii s vhodnými riešeniami správy kľúčov s cieľom obmedziť riziko neoprávneného prístupu k šifrovacím kľúčom; spoločnosť by mala pri výbere riešenia v oblasti riadenia kľúčov zvážiť najmä najmodernejšie technológie a postupy;
d) *prevádzková a sieťová bezpečnosť:* zvážiť príslušné úrovne dostupnosti siete, segregáciu siete [napríklad izoláciu užívateľa v spoločnom prostredí cloudu, prevádzkové oddelenie, pokiaľ ide o web, aplikačnú logiku, prevádzkový systém, sieť, systém riadenia databázy (DBMS) a vrstvy uchovávania] a prostredia spracovávania (napríklad test, testovanie používateľom, vývoj, výroba);
e) *aplikačné programové rozhrania (API):* zvážiť mechanizmy na integráciu cloudových služieb so systémami spoločnosti na zaistenie bezpečnosti rozhraní API (napríklad zriadenie a udržiavanie politík a postupov informačnej bezpečnosti pre API vo viacerých systémových rozhraniach, jurisdikciách a obchodných funkciách na zabránenie neoprávnenému zverejneniu, zmene alebo zničeniu údajov);
f) *kontinuita činností a obnova po havárii:* zabezpečiť, že sú zavedené účinné kontroly kontinuity činností a obnovy po havárii (napríklad stanovením minimálnych požiadaviek na kapacitu, výberom možností hosťovania, ktoré sú geograficky rozptýlené, s možnosťou prechádzať z jednej na druhú, alebo požadovaním a preskúmaním dokumentácie, ktorá znázorňuje trasu prenosu údajov spoločnosti medzi systémami poskytovateľa cloudových služieb, ako aj zvážením možnosti zreprodukovať obrazy zariadenia na nezávislom mieste uchovávania, ktoré je dostatočne izolované od siete alebo je offline);

g) *umiestnenie údajov:* zaujať prístup vychádzajúci z hodnotenia rizík k miestu alebo miestam uchovávania údajov a spracovávania údajov (konkrétne regióny alebo krajiny);
h) *súlad s predpismi a monitorovanie:* overiť, že PCS dodržiava medzinárodne uznávané normy informačnej bezpečnosti a zaviedol príslušné kontroly informačnej bezpečnosti (napríklad požiadaním poskytovateľa cloudových služieb o preukázanie toho, že vykonáva príslušné preskúmania informačnej bezpečnosti, a pravidelným posudzovaním a testovaním dohôd poskytovateľa cloudových služieb o informačnej bezpečnosti).

Usmernenie 5. Stratégie ukončenia angažovanosti

30. V prípade outsourcingu zásadných alebo dôležitých funkcií by mala spoločnosť zabezpečiť, že dokáže ukončiť dohodu o cloudovom outsourcingu bez nenáležitého narušenia svojej obchodnej činnosti a služieb poskytovaných svojim klientom a bez akéhokoľvek narušenia plnenia svojich povinností podľa platných právnych predpisov alebo poškodenia dôvernosti, celistvosti a dostupnosti svojich údajov. Na tento účel by mala spoločnosť:

a) vypracovať komplexné, zdokumentované a dostatočne overené plány ukončenia angažovanosti. Tieto plány by sa mali aktualizovať podľa potreby, a to aj v prípade zmien vo funkcii zabezpečovanej prostredníctvom outsourcingu;
b) identifikovať alternatívne riešenia a vypracovať plány prechodu na odobratie funkcie zabezpečovanej prostredníctvom outsourcingu a údajov poskytovateľovi cloudových služieb a prípadne subdodávateľovi a na ich prenos alternatívnemu poskytovateľovi cloudových služieb, ktorého určí spoločnosť, alebo priamo naspäť spoločnosti. Tieto riešenia by sa mali stanoviť so zreteľom na výzvy, ktoré môžu vzniknúť v súvislosti s umiestnením údajov, pričom by sa mali prijať potrebné opatrenia na zabezpečenie kontinuity činností v prechodnej fáze;
c) zabezpečiť, že písomná dohoda o cloudovom outsourcingu zahŕňa povinnosť poskytovateľa cloudových služieb podporiť riadny prenos funkcie zabezpečovanej prostredníctvom outsourcingu a súvisiaceho spracovania údajov od poskytovateľa cloudových služieb a akéhokoľvek subdodávateľa inému poskytovateľovi cloudových služieb, ktorého určí spoločnosť, alebo priamo spoločnosti v prípade, že spoločnosť aktivuje stratégiu ukončenia angažovanosti. Povinnosť podporiť riadny prenos funkcie zabezpečovanej prostredníctvom outsourcingu a súvisiaceho spracovania údajov by v príslušných prípadoch mala zahŕňať bezpečné vymazanie údajov zo systémov poskytovateľa cloudových služieb a akéhokoľvek subdodávateľa.

31. Pri vypracúvaní plánov a riešení ukončenia angažovanosti uvedených v bodoch a) a b) („stratégia ukončenia angažovanosti“) by mala spoločnosť zvážiť:

a) vymedzenie cieľov stratégie ukončenia angažovanosti;
b) vymedzenie spúšťacích udalostí, ktoré by mohli aktivovať stratégiu ukončenia angažovanosti. Mohli by zahŕňať aspoň ukončenie dohody o cloudovom outsourcingu na iniciatívu spoločnosti alebo poskytovateľa cloudových služieb a pri chybe alebo inom závažnom prerušení podnikateľskej činnosti poskytovateľa cloudových služieb;
c) vykonanie analýzy vplyvu na podnikanie, ktorá by mala zodpovedať funkcii zabezpečovanej prostredníctvom outsourcingu, s cieľom určiť, aké ľudské a iné zdroje by boli potrebné na vykonanie stratégie ukončenia angažovanosti;
d) pridelenie úloh a zodpovednosti za riadenie stratégie ukončenia angažovanosti;
e) otestovanie vhodnosti stratégie ukončenia angažovanosti pomocou prístupu vychádzajúceho z posúdenia rizík (napríklad vykonaním analýzy potenciálnych nákladov, vplyvu, zdrojov a časových dôsledkov presunu služby zabezpečovanej prostredníctvom outsourcingu na alternatívneho poskytovateľa);
f) vymedzenie kritérií úspešnosti prechodu.

32. Spoločnosť by do svojho priebežného monitorovania služieb dodávaných poskytovateľom cloudových služieb podľa dohody o cloudovom outsourcingu a dohľadu nad nimi mala zahrnúť ukazovatele spúšťacích udalostí, ktoré môžu aktivovať stratégiu ukončenia angažovanosti.

Usmernenie 6. Prístupové a audítorské práva

33. Spoločnosť by mala zabezpečiť, že písomná dohoda o cloudovom outsourcingu neobmedzuje účinné uplatňovanie prístupových a audítorských práv spoločnosti a príslušného orgánu, ani možnosti dohľadu nad poskytovateľom cloudových služieb.

34. Spoločnosť by mala zabezpečiť, že uplatňovanie prístupových a audítorských práv (napríklad frekvencia auditov a auditované oblasti a služby) zohľadňuje to, či outsourcing súvisí so zásadnou alebo dôležitou funkciou, ako aj povahu a rozsah rizík a vplyvu vyplývajúcich spoločnosti z dohody o cloudovom outsourcingu.

35. Ak uplatňovanie prístupových alebo audítorských práv alebo používanie istých audítorských techník vytvára riziko pre prostredie poskytovateľa cloudových služieb a/alebo iného klienta poskytovateľa cloudových služieb (napríklad tým, že ovplyvní úrovne poskytovaných služieb, dôvernosť, celistvosť a dostupnosť údajov), PCS by mal spoločnosti poskytnúť jasné odôvodnenie, prečo by to predstavovalo riziko, a PCS by sa mal so spoločnosťou dohodnúť na alternatívnych spôsoboch dosiahnutia podobného výsledku (napríklad zahrnutie špecifických kontrol, ktoré sa majú otestovať, do osobitnej správy/osvedčenia, ktoré PCS vyhotoví).

36. Bez toho, aby bola dotknutá ich konečná zodpovednosť týkajúca sa dohôd o cloudovom outsourcingu, môžu spoločnosti v záujme efektívnejšieho využívania

zdrojov auditu a zníženia organizačnej záťaže, ktorej je vystavený PCS a jeho zákazníci, využívať:

a) certifikácie tretích strán a správy o externom alebo internom audite sprístupnené poskytovateľom cloudových služieb;
b) skupinové audity vykonávané spoločne s inými klientmi toho istého poskytovateľa cloudových služieb alebo skupinové audity vykonávané audítorom, ktorý je treťou stranou a bol určený viacerými klientmi toho istého poskytovateľa cloudových služieb.

37. V prípade outsourcingu zásadných alebo dôležitých funkcií by mala spoločnosť posúdiť, či sú certifikácie tretích strán a správy o externom alebo internom audite uvedené v ods. 37 písm. a) náležité a dostatočné na splnenie jeho povinností podľa platných právnych predpisov, a mala by sa usilovať o to, aby sa časom nespoliehala len na tieto certifikácie a správy.

38. V prípade outsourcingu zásadných alebo dôležitých funkcií by mala spoločnosť využiť certifikácie tretích strán a správy o externom alebo internom audite uvedené v ods. 37 písm. a) iba vtedy, ak:

a) je presvedčená o tom, že rozsah certifikácií alebo správ o audite zahŕňa kľúčové systémy poskytovateľa cloudových služieb (napríklad procesy, aplikácie, infraštruktúru, dátové centrá), kľúčové kontroly určené spoločnosťou a dodržiavanie príslušných platných právnych predpisov;
b) pravidelne a dôkladne posudzuje obsah certifikácií alebo správ o audite a overuje, či tieto certifikácie alebo správy nie sú zastarané;
c) zabezpečuje, že budúce verzie certifikácií alebo správ o audite budú zahŕňať kľúčové systémy a kontroly poskytovateľa cloudových služieb;
d) je spokojná so stranou, ktorá poskytuje certifikáciu alebo vykonáva audit (napríklad vzhľadom na jej kvalifikáciu, odborné znalosti, opätovné vykonávanie/overovanie dôkazov v základnom audítorskom spise ako aj rotáciu spoločnosti, ktorá poskytuje certifikáciu alebo vykonáva audit);
e) je presvedčená, že certifikácie sa vydávajú a audity sa vykonávajú podľa príslušných noriem a zahŕňajú skúšku účinnosti zavedených kľúčových kontrol;
f) má zmluvné právo požiadať o rozšírenie rozsahu certifikácií alebo správ o audite na iné relevantné systémy a kontroly poskytovateľa cloudových služieb; počet a frekvencia týchto žiadostí o úpravu rozsahu by mali byť primerané a oprávnené z hľadiska riadenia rizík;
g) zachováva si zmluvné právo na výkon individuálnych auditov na mieste podľa svojho voľného uváženia so zreteľom na funkciu zabezpečovanú prostredníctvom outsourcingu.

39. Spoločnosť by mala zabezpečiť, že pred návštevou na mieste, a to aj návštevou tretej strany vymenovanej spoločnosťou (napríklad audítorom), sa poskytovateľovi cloudových služieb v primeranej lehote odošle predchádzajúce oznámenie, ak nie je

včasné predchádzajúce oznámenie nemožné z dôvodu núdzovej alebo krízovej situácie alebo by viedlo k situácii, keď by už audit nebol účinný. Takéto oznámenie by malo obsahovať miesto a účel návštevy a personál, ktorý sa na návšteve zúčastní.

40. Vzhľadom na to, že cloudové služby predstavujú vysokú úroveň technickej zložitosti a vedú k osobitným výzvam v súvislosti s jurisdikciou, mali by mať zamestnanci vykonávajúci audit, či už interní audítori spoločnosti alebo audítori konajúci vo vlastnom mene, správne zručnosti a vedomosti na riadne posúdenie príslušných cloudových služieb a vykonávanie účinného a relevantného auditu. Toto by sa malo vzťahovať aj na zamestnancov spoločnosti, ktorí skúmajú certifikácie alebo správy o audite dodané poskytovateľom cloudových služieb.

Usmernenie 7. Sub-outsourcing

41. Ak je povolený sub-outsourcing zásadných alebo dôležitých funkcií (alebo ich významných častí), v písomnej dohode o cloudovom outsourcingu medzi spoločnosťou a poskytovateľom cloudových služieb je potrebné:

    a) stanoviť všetky časti alebo aspekty funkcie zabezpečovanej prostredníctvom outsourcingu, ktoré sú vylúčené z potenciálneho sub-outsourcingu;
    b) uviesť podmienky, ktoré musia byť splnené v prípade sub-outsourcingu;
    c) stanoviť, že PCS zostáva zodpovedný a je povinný dohliadať na tie služby, ktoré zadal subdodávateľovi, aby sa zabezpečilo, že všetky zmluvné záväzky medzi poskytovateľom cloudových služieb a spoločnosťou budú sústavne splnené;
    d) zahŕňať povinnosť, aby PCS oznamoval spoločnosti každý zamýšľaný sub-outsourcing alebo jeho významné zmeny, najmä ak to môže ovplyvniť schopnosť poskytovateľa cloudových služieb plniť si svoje povinnosti podľa dohody o cloudovom outsourcingu uzatvorenej so spoločnosťou. Lehota na oznámenie stanovená v písomnej dohode by mala umožniť spoločnosti dostatok času aspoň na posúdenie rizík navrhovaného sub-outsourcingu alebo jeho významných zmien a na ich namietanie alebo výslovné schválenie, ako je uvedené ďalej v písm. e);
    e) zabezpečiť, že spoločnosť má právo namietať zamýšľaný sub-outsourcing alebo jeho významné zmeny, alebo že je potrebné výslovné schválenie predtým, než navrhnutý sub-outsourcing alebo významné zmeny nadobudnú účinnosť;
    f) zabezpečiť, že spoločnosť má zmluvné právo ukončiť dohodu o cloudovom outsourcingu s poskytovateľom cloudových služieb, ak namieta navrhovaný sub-outsourcing alebo jeho významné zmeny, a v prípade nenáležitého sub-outsourcingu (napríklad ak PCS vykonáva sub-outsourcing bez toho, že by to oznámil spoločnosti, alebo vážne poruší podmienky sub-outsourcingu uvedené v dohode o outsourcingu).

42. Spoločnosť by mala zabezpečiť, že PCS bude náležite dohliadať na subdodávateľa.

Usmernenie 8. Písomné oznámenie príslušným orgánom

43. Spoločnosť by mala svojmu príslušnému orgánu včas písomne oznámiť plánované dohody o cloudovom outsourcingu, ktoré sa týkajú zásadnej alebo dôležitej funkcie. Spoločnosť by mala svojmu príslušnému orgánu takisto včas písomne oznámiť tie dohody o cloudovom outsourcingu, ktoré sa týkajú funkcie, ktorá predtým nebola označená za zásadnú alebo dôležitú, no neskôr sa zásadnou alebo dôležitou stala.

44. Písomné oznámenie spoločnosti by s prihliadnutím na zásadu proporcionality malo obsahovať aspoň tieto informácie:

    a) dátum začiatku a prípadne dátum ďalšieho predĺženia dohody o cloudovom outsourcingu, dátum ukončenia a/alebo výpovedné lehoty pre poskytovateľa cloudových služieb a pre spoločnosť;
    b) stručný opis funkcie, ktorá sa má zabezpečovať prostredníctvom outsourcingu;
    c) stručné zhrnutie dôvodov, prečo sa funkcia zabezpečovaná prostredníctvom outsourcingu považuje za zásadnú alebo dôležitú;
    d) názov a značka (ak existuje) poskytovateľa cloudových služieb, krajina jeho registrácie, jeho registračné číslo, identifikátor právnickej osoby (ak je k dispozícii), adresa sídla, relevantné kontaktné údaje a názov jeho materskej spoločnosti (ak existuje);
    e) rozhodné právo dohody o cloudovom outsourcingu a prípadne voľba jurisdikcie;
    f) modely zavedenia cloudu a osobitnú povahu údajov, ktoré má PCS uchovávať, a miesta (konkrétne regióny alebo krajiny), kde sa môžu takéto údaje uchovávať;
    g) dátum najnovšieho posúdenia zásadnosti alebo dôležitosti funkcie zabezpečovanej prostredníctvom outsourcingu;
    h) dátum najnovšieho posúdenia rizík alebo auditu poskytovateľa cloudových služieb spolu so stručným zhrnutím hlavných výsledkov a dátum nasledujúceho plánovaného posúdenia rizík alebo auditu;
    i) názov samostatného alebo rozhodovacieho orgánu v spoločnosti, ktorý schválil dohodu o cloudovom outsourcingu;
    j) v príslušných prípadoch mená akýchkoľvek subdodávateľov zabezpečujúcich podstatné časti zásadnej alebo dôležitej funkcie prostredníctvom sub-outsourcingu vrátane krajiny alebo regiónu, v ktorej sú títo subdodávatelia registrovaní, v ktorej sa bude služba zabezpečovaná prostredníctvom sub-outsourcingu vykonávať a v ktorej sa budú údaje uchovávať.

Usmernenie 9. Dohľad nad dohodami o cloudovom outsourcingu

45. Príslušné orgány by v rámci svojho postupu dohľadu mali posúdiť riziká vyplývajúce z dohôd spoločností o cloudovom outsourcingu. Toto posúdenie by sa malo zameriavať najmä na dohody týkajúce sa outsourcingu zásadných alebo dôležitých funkcií.

46. Príslušné orgány by mali byť presvedčené, že sú schopné vykonávať účinný dohľad, najmä ak spoločnosti prostredníctvom outsourcingu zabezpečujú zásadné alebo dôležité funkcie, ktoré sa vykonávajú mimo EÚ.

47. Príslušné orgány by mali na základe prístupu vychádzajúceho z posúdení rizík posúdiť, či spoločnosti:

    a) majú zavedené príslušné postupy týkajúce sa riadenia, zdrojov a prevádzky na to, aby náležite a účinne uzatvárali a vykonávali dohody o cloudovom outsourcingu a dohliadali na ne;
    b) identifikujú a riadia všetky relevantné riziká súvisiace s cloudovým outsourcingom.

48. Ak sa zistia riziká koncentrácie, príslušné orgány by mali monitorovať vývoj takýchto rizík a vyhodnotiť ich potenciálny vplyv na iné spoločnosti, na ktoré dohliadajú, a na stabilitu finančného trhu.