EIOPA-BoS-20-002

Usmernenia týkajúce sa outsourcingu poskytovateľom cloudových služieb

Obsah

Úvod

1. Orgán EIOPA v súlade s článkom 16 nariadenia (EÚ) č. 1094/2010[1] vydáva usmernenia s cieľom poskytnúť poisťovniam a zaisťovniam návod na uplatňovanie ustanovení o outsourcingu (zverení výkonu činností) stanovených v smernici 2009/138/ES[2] (ďalej len „smernica Solventnosť II") a v delegovanom nariadení Komisie (EÚ) č. 2015/35[3] (ďalej len „delegované nariadenie") v prípade outsourcingu poskytovateľom cloudových služieb.

2. Tieto usmernenia vychádzajú z článku 13 ods. 28 a článkov 38 a 49 smernice Solventnosť II a z článku 274 delegovaného nariadenia. Okrem toho sa opierajú aj o pokyny stanovené v usmerneniach orgánu EIOPA týkajúcich sa systému správy a riadenia (EIOPA-BoS-14/253).

3. Tieto usmernenia sú určené príslušným orgánom s cieľom poskytnúť poisťovacím a zaisťovacím podnikom (spoločne „poisťovniam a zaisťovniam") návod na uplatňovanie požiadaviek týkajúcich sa outsourcingu, ktoré sú stanovené v uvedených právnych aktoch, v súvislosti s outsourcingom poskytovateľom cloudových služieb.

4. Usmernenia sa vzťahujú na jednotlivé poisťovne a zaisťovne a *mutatis mutandis* aj na skupiny[4].

   Subjekty, ktoré sú súčasťou skupiny a na ktoré sa vzťahujú iné sektorové požiadavky, sú na individuálnej úrovni vylúčené z rozsahu pôsobnosti týchto usmernení, keďže musia dodržiavať osobitné požiadavky platné v danom sektore, ako aj príslušné usmernenia vydané Európskym orgánom pre cenné papiere a trhy a Európskym orgánom pre bankovníctvo.

5. V prípade outsourcingu vnútri skupiny a sub-outsourcingu poskytovateľom cloudových služieb by sa tieto usmernenia mali uplatňovať v spojení s ustanoveniami o vnútroskupinovom outsourcingu, ktoré sú súčasťou usmernení orgánu EIOPA týkajúcich sa systému správy a riadenia.

6. Poisťovne a zaisťovne a príslušné orgány by mali pri dodržiavaní týchto usmernení alebo pri dohľade nad ich dodržiavaním zohľadňovať zásadu proporcionality[5] a zásadnosť alebo dôležitosť služby outsourcovanej poskytovateľom cloudových služieb. Uplatnením zásady proporcionality by sa malo zabezpečiť, že mechanizmy správy a riadenia vrátane tých, ktoré sa týkajú outsourcingu poskytovateľom cloudových služieb, budú primerané povahe, rozsahu a komplexnosti podkladových rizík.

7. Tieto usmernenia by sa mali vykladať v spojení s usmerneniami orgánu EIOPA týkajúcimi sa systému správy a riadenia a s regulačnými povinnosťami uvedenými v odseku 1, a to bez toho, aby nimi boli dotknuté.

Vymedzenie pojmov

8. Pokiaľ nie sú pojmy vymedzené v týchto usmerneniach, ich význam je vymedzený v právnych aktoch, na ktoré sa odkazuje v úvode.

---

[1] Nariadenie Európskeho parlamentu a Rady (EÚ) č. 1094/2010 z 24. novembra 2010, ktorým sa zriaďuje Európsky orgán dohľadu (Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov), a ktorým sa mení a dopĺňa rozhodnutie č. 716/2009/ES a zrušuje rozhodnutie Komisie 2009/79/ES (Ú. v. EÚ L 331, 15.12.2010, s. 48).

[2] Smernica Európskeho parlamentu a Rady 2009/138/ES z 25. novembra 2009 o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 335, 17.12.2009, s. 1).

[3] Delegované nariadenie Komisie (EÚ) 2015/35 z 10. októbra 2014, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2009/138/ES o začatí a vykonávaní poistenia a zaistenia (Solventnosť II) (Ú. v. EÚ L 12, 17.1.2015, s. 1).

[4] Pozri článok 212 ods. 1 smernice Solventnosť II.

[5] Pozri článok 29 ods. 3 smernice Solventnosť II.

9. Na účely týchto usmernení sa okrem toho uplatňuje toto vymedzenie pojmov:

Poskytovateľ služieb	je tretia strana, ktorá na základe dohody o outsourcingu vykonáva postup, službu alebo činnosť, alebo ich časti.
Poskytovateľ cloudových služieb	je poskytovateľ služby, ako je vymedzené vyššie, ktorý zodpovedá za poskytovanie cloudových služieb na základe dohody o outsourcingu.
Cloudové služby	sú služby poskytované pomocou cloud computingu, teda modelu umožňujúceho všadeprítomný, pohodlný sieťový prístup na požiadanie k spoločne využívaným prostriedkom výpočtovej techniky (napr. siete, servery, úložisko, aplikácie a služby), ktorý sa môže rýchlo zriadiť a zrušiť s minimálnou potrebou riadenia a minimálnou interakciou s poskytovateľom služby.
Verejný cloud	je cloudová infraštruktúra, ktorá je k dispozícii na otvorené použitie širokou verejnosťou.
Súkromný cloud	je cloudová infraštruktúra, ktorá je k dispozícii na výlučné použitie jedným podnikom.
Komunitný cloud	je cloudová infraštruktúra, ktorá je k dispozícii na výlučné použitie konkrétnou komunitou podnikov, t. j. viacerými podnikmi v rámci jednej skupiny.
Hybridný cloud	je cloudová infraštruktúra, ktorá pozostáva z dvoch alebo viacerých odlišných cloudových infraštruktúr.

Dátum uplatňovania

10. Tieto usmernenia sa uplatňujú od 1. januára 2021 na všetky dohody o cloudovom outsourcingu, ktoré boli prijaté alebo zmenené v tento deň alebo po ňom.

11. Poisťovne a zaisťovne by mali preskúmať a zodpovedajúcim spôsobom zmeniť existujúce dohody o cloudovom outsourcingu, ktoré súvisia so zásadnými alebo dôležitými operačnými funkciami alebo činnosťami, s cieľom zabezpečiť súlad s týmito usmerneniami do 31. decembra 2022.

12. V prípade, že preskúmanie dohôd o cloudovom outsourcingu, ktoré súvisia so zásadnými alebo dôležitými operačnými funkciami alebo činnosťami, nebude ukončené do 31. decembra 2022, poisťovne a zaisťovne by mali o tejto skutočnosti informovať príslušné orgány dohľadu[6], ako aj o plánovaných opatreniach na dokončenie preskúmania, prípadne o možnej stratégii ukončenia angažovanosti. Orgán dohľadu sa v prípade potreby môže s poisťovňami a zaisťovňami dohodnúť na predĺžení lehoty na dokončenie tohto preskúmania.

13. Aktualizácia politík a vnútorných postupov poisťovní a zaisťovní (ak je potrebná) by sa mala vykonať do 1. januára 2021, pričom požiadavky na dokumentáciu pri dohodách o cloudovom outsourcingu, ktoré súvisia so zásadnými alebo dôležitými prevádzkovými funkciami alebo činnosťami, by mali byť splnené do 31. decembra 2022.

[6] Pozri článok 13 ods. 10 smernice Solventnosť II.

Usmernenie 1 – Cloudové služby a outsourcing

14. Poisťovňa alebo zaisťovňa by mala stanoviť, či dohoda s poskytovateľom cloudových služieb patrí pod outsourcing v tom zmysle, ako je vymedzený podľa smernice Solventnosť II. V rámci tohto posúdenia by sa malo zvážiť:

a. či sa outsourcovaná operačná funkcia alebo činnosť (alebo jej časť) vykonáva na opakovanom alebo priebežnom základe, a

b. či by táto operačná funkcia alebo činnosť (alebo jej časť) za normálnych okolností patrila do rozsahu operačných funkcií alebo činností, ktoré by poisťovňa alebo zaisťovňa vykonávala alebo mohla vykonávať v rámci svojej bežnej podnikateľskej činnosti, hoci poisťovňa alebo zaisťovňa túto operačnú funkciu alebo činnosť v minulosti nevykonávala.

15. Ak sa dohoda s poskytovateľom služieb týka viacerých prevádzkových operačných alebo činností, poisťovňa alebo zaisťovňa by mala v rámci posúdenia zvážiť všetky aspekty dohody.

16. V prípadoch, keď poisťovňa alebo zaisťovňa outsourcuje operačné funkcie alebo činnosti poskytovateľom služieb, ktorí nie sú poskytovateľmi cloudových služieb, ale dodávajú služby prostredníctvom cloudových infraštruktúr (poskytovateľ cloudových služieb je napríklad súčasťou sub-outsourcingového reťazca), dohoda o takomto outsourcingu patrí do rozsahu pôsobnosti týchto usmernení.

Usmernenie 2 – Všeobecné zásady riadenia v prípade cloudového outsourcingu

17. Správny, riadiaci alebo kontrolný orgán poisťovne alebo zaisťovne by mal zabezpečiť, bez toho, aby bol dotknutý článok 274 ods. 3 delegovaného nariadenia, aby každému rozhodnutiu outsourcovať poskytovateľom cloudových služieb zásadné alebo dôležité operačné funkcie alebo činnosti predchádzalo dôkladné posúdenie rizika vrátane všetkých relevantných rizík vyplývajúcich z dohody, ako sú informačné a komunikačné technológie („IKT"), kontinuita činností, právny poriadok a súlad, koncentrácia, iné operačné riziká a v prípade potreby aj riziká súvisiace s migráciou údajov a/alebo s fázou vykonávania.

18. Ak poisťovňa alebo zaisťovňa outsourcuje poskytovateľom cloudových služieb zásadné alebo dôležité operačné funkcie alebo činnosti, zmeny vo svojom rizikovom profile vyplývajúce z dohôd o cloudovom outsourcingu by mala podľa potreby zohľadniť vo vlastnom posúdení rizika a solventnosti.

19. Využívanie cloudových služieb by malo byť v súlade so stratégiami poisťovne alebo zaisťovne (napríklad so stratégiou IKT, stratégiou informačnej bezpečnosti, stratégiou riadenia operačného rizika) a s jej vnútornými politikami a postupmi, ktoré by sa mali v prípade potreby aktualizovať.

Usmernenie 3 – Aktualizácia písomnej politiky outsourcingu

20. V prípade outsourcingu poskytovateľom cloudových služieb by poisťovňa alebo zaisťovňa mala aktualizovať písomnú politiku outsourcingu (napríklad jej revidovaním, doplnením samostatného dodatku alebo vytvorením nových cielených politík) a ostatné relevantné vnútorné politiky (napríklad bezpečnosť informácií), pričom by mala zohľadniť špecifiká cloudového outsourcingu aspoň v týchto oblastiach:

a. úlohy a povinnosti zapojených funkcií danej poisťovne alebo zaisťovne, najmä jej správneho, riadiaceho alebo kontrolného orgánu, a funkcií, ktoré

zodpovedajú za IKT, bezpečnosť informácií, dodržiavanie predpisov, riadenie rizík a vnútorný audit,

b. procesy a postupy podávania správ potrebných na schválenie, vykonávanie, monitorovanie, riadenie a prípadné obnovenie dohôd o cloudovom outsourcingu, ktoré súvisia so zásadnými alebo dôležitými operačnými funkciami alebo činnosťami,

c. primeraný dohľad nad cloudovými službami vzhľadom na povahu, rozsah a komplexnosť rizík obsiahnutých v poskytovaných službách vrátane i) posúdenia rizík spojených s dohodami o cloudovom outsourcingu a hĺbkovej analýzy poskytovateľov cloudových služieb vrátane frekvencie posudzovania rizika, ii) kontrol monitorovania a riadenia (napríklad overovanie dohody o úrovni poskytovaných služieb), iii) bezpečnostných noriem a kontrol,

d. pri cloudovom outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností by sa mal uviesť odkaz na zmluvné požiadavky uvedené v usmernení 10,

e. požiadavky na dokumentáciu a písomné oznámenie orgánu dohľadu v súvislosti s cloudovým outsourcingom zásadných alebo dôležitých operačných funkcií alebo činností,

f. požiadavka na zdokumentovanú, prípadne dostatočne overenú „stratégiu ukončenia angažovanosti", ktorá je primeraná povahe, rozsahu a komplexnosti rizík obsiahnutých v poskytovaných službách, a to pri každej dohode o cloudovom outsourcingu, ktorá sa týka zásadných alebo dôležitých operačných funkcií alebo činností. Stratégia ukončenia angažovanosti môže zahŕňať celý rad postupov ukončenia, okrem iného prerušenie, opätovné začlenenie alebo presun služieb obsiahnutých v dohode o cloudovom outsourcingu.

Usmernenie 4 – Písomné oznámenie orgánu dohľadu

21. Požiadavky na písomné oznámenie, ktoré sú stanovené v článku 49 ods. 3 smernice Solventnosť II a podrobnejšie rozpracované v usmerneniach orgánu EIOPA k systému správy a riadenia, sa týkajú akéhokoľvek outsourcingu zásadných alebo dôležitých operačných funkcií a činností poskytovateľom cloudových služieb. Ak sa outsourcovaná operačná funkcia alebo činnosť, ktorá predtým nebola klasifikovaná ako zásadná alebo dôležitá, stane zásadnou alebo dôležitou, poisťovňa alebo zaisťovňa by to mala oznámiť orgánu dohľadu.

22. Písomné oznámenie poisťovne alebo zaisťovne by s prihliadnutím na zásadu proporcionality malo obsahovať aspoň tieto informácie:

a. stručný opis outsourcovanej operačnej funkcie alebo činnosti,

b. dátum začiatku a prípadne dátum ďalšieho obnovenia zmluvy, dátum ukončenia a/alebo výpovedné lehoty pre poskytovateľa cloudových služieb a pre danú poisťovňu alebo zaisťovňu,

c. právo, ktorým sa riadi dohoda o cloudovom outsourcingu,

d. názov poskytovateľa cloudových služieb, identifikačné číslo organizácie, identifikátor právnickej osoby (ak je k dispozícii), adresu sídla a iné relevantné kontaktné údaje a názov materskej spoločnosti (ak existuje), v prípade skupín údaj o tom, či poskytovateľ cloudových služieb patrí do skupiny,

e. modely cloudových služieb a využívania (t. j. verejné/súkromné/hybridné/komunitné) a konkrétnu povahu údajov, ktoré sa

budú uchovávať, ako aj miesto, kde sa tieto údaje budú uchovávať (t. j. v ktorých krajinách alebo regiónoch),

f. stručné zhrnutie dôvodov, prečo sa outsourcovaná operačná funkcia alebo činnosť považuje za zásadnú alebo dôležitú,

g. dátum najnovšieho posúdenia zásadnosti alebo dôležitosti outsourcovanej funkcie alebo činnosti.

Usmernenie 5 – Požiadavky na dokumentáciu

23. Poisťovňa alebo zaisťovňa by si v rámci svojho systému správy a riadenia a systému riadenia rizík mala viesť záznamy o svojich dohodách o cloudovom outsourcingu, napríklad vo forme osobitného registra, ktorý sa priebežne aktualizuje. Podobne by si poisťovňa alebo zaisťovňa počas primerane dlhého obdobia, stanoveného vnútroštátnymi predpismi, mala viesť záznamy o ukončených dohodách o cloudovom outsourcingu.

24. V prípade outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností by poisťovňa alebo zaisťovňa mala zaznamenávať tieto informácie:

a. informácie uvedené v usmernení 4, ktoré oznamuje orgánu dohľadu,

b. v prípade skupín zoznam poisťovní alebo zaisťovní a iných podnikov v rozsahu pôsobnosti prudenciálnej konsolidácie, ktoré využívajú cloudové služby,

c. dátum najnovšieho posúdenia rizika a stručné zhrnutie hlavných výsledkov,

d. názov samostatného alebo rozhodovacieho orgánu poisťovne alebo zaisťovne (napríklad správneho, riadiaceho alebo kontrolného orgánu), ktorý schválil dohodu o cloudovom outsourcingu,

e. dátumy najnovšieho auditu a ďalších naplánovaných auditov, ak sa uplatňujú,

f. mená všetkých subdodávateľov, ktorým sú sub-outsourcované podstatné časti zásadnej alebo dôležitej operačnej funkcie alebo činnosti, vrátane uvedenia krajiny, v ktorej sú subdodávatelia registrovaní a kde sa služba bude vykonávať, prípadne miesto uchovávania údajov (t. j. krajina alebo región),

g. výsledok hodnotenia nahraditeľnosti poskytovateľa cloudových služieb (napríklad, či nahradiť ho je ľahké, náročné alebo nemožné),

h. či outsourcovaná zásadná alebo dôležitá operačná funkcia alebo činnosť podporuje podnikateľské činnosti, ktoré sú časovo kritické,

i. odhadované ročné rozpočtové náklady,

j. či má poisťovňa alebo zaisťovňa stratégiu ukončenia angažovanosti v prípade, že jedna zo strán zmluvu ukončí alebo v prípade prerušenia poskytovania služieb zo strany poskytovateľa cloudových služieb.

25. V prípade outsourcingu operačných funkcií alebo činností, ktoré nie sú zásadné alebo dôležité, by poisťovňa alebo zaisťovňa mala určiť, aké informácie sa budú zaznamenávať, a to na základe povahy, rozsahu a komplexnosti rizík obsiahnutých v službách poskytovateľa cloudových služieb.

26. Poisťovňa alebo zaisťovňa by mala na požiadanie sprístupniť orgánu dohľadu všetky informácie potrebné na vykonanie dohľadu nad touto poisťovňou alebo zaisťovňou vrátane kópie dohody o outsourcingu.

Usmernenie 6 – Predbežná analýza outsourcingu

27. Pred uzavretím akejkoľvek dohody s poskytovateľmi cloudových služieb by poisťovňa alebo zaisťovňa mala:

a. posúdiť, či sa dohoda o cloudovom outsourcingu týka zásadnej alebo dôležitej operačnej funkcie alebo činnosti v súlade s usmernením 7,

b. identifikovať a posúdiť všetky relevantné riziká dohody o cloudovom outsourcingu v súlade s usmernením 8,

c. vykonať náležitú hĺbkovú analýzu potenciálneho poskytovateľa cloudových služieb v súlade s usmernením 9,

d. identifikovať a posúdiť konflikty záujmov, ktoré môže outsourcing spôsobiť, v súlade s požiadavkami stanovenými v článku 274 ods. 3 písm. b) delegovaného nariadenia.

Usmernenie 7 – Posudzovanie zásadných alebo dôležitých operačných funkcií a činností

28. Pred uzatvorením akejkoľvek dohody o outsourcingu s poskytovateľmi cloudových služieb by poisťovňa alebo zaisťovňa mala posúdiť, či sa dohoda o cloudovom outsourcingu týka zásadnej alebo dôležitej operačnej funkcie alebo činnosti. Pri vykonávaní takéhoto posúdenia by poisťovňa alebo zaisťovňa mala v prípade potreby zvážiť, či sa daná dohoda môže v budúcnosti stať zásadnou alebo dôležitou. Poisťovňa alebo zaisťovňa by takisto mala prehodnotiť zásadnosť alebo dôležitosť operačnej funkcie alebo činnosti, ktorá bola poskytovateľom cloudových služieb outsourcovaná v minulosti, ak sa zásadne zmení povaha, rozsah a komplexnosť rizík obsiahnutých v tejto dohode.

29. Pri posudzovaní by poisťovňa alebo zaisťovňa okrem výsledkov posúdenia rizika mala zohľadniť aspoň tieto faktory:

a. potenciálny vplyv, ktorý môže mať na poisťovňu alebo zaisťovňu akékoľvek závažné narušenie outsourcovanej operačnej funkcie alebo aktivity, alebo neschopnosť poskytovateľa cloudových služieb poskytovať služby v dohodnutej kvalite, konkrétne vplyv na jej:

   i. nepretržité plnenie regulačných povinností,

   ii. krátkodobú a dlhodobú finančnú odolnosť, solventnosť a životaschopnosť,

   iii. kontinuitu činnosti a prevádzkovú odolnosť,

   iv. operačné riziko vrátane rizika správania, rizika v oblasti informačných a komunikačných technológií a právneho rizika,

   v. riziká poškodenia dobrej povesti;

b. potenciálny vplyv dohody o cloudovom outsourcingu na schopnosť poisťovne alebo zaisťovne:

   i. identifikovať, monitorovať a riadiť všetky relevantné riziká,

   ii. dodržiavať všetky právne a regulačné požiadavky,

   iii. vykonávať primerané audity outsourcovanej operačnej funkcie alebo činnosti;

c. viacnásobné dohody poisťovne alebo zaisťovne (a/alebo skupiny) s jedným poskytovateľom cloudových služieb a potenciálny kumulatívny efekt dohôd o outsourcingu v rámci jednej oblasti činnosti,

d. rozsah a komplexnosť oblastí činnosti danej poisťovne alebo zaisťovne, na ktoré sa vzťahuje dohoda o cloudovom outsourcingu,

e. v prípade potreby alebo nutnosti schopnosť preniesť navrhovanú dohodu o cloudovom outsourcingu na iného poskytovateľa cloudových služieb alebo tieto služby opätovne začleniť („nahraditeľnosť“),

f. ochrana osobných a iných ako osobných údajov a potenciálny vplyv, ktorý na poisťovňu alebo zaisťovňu, poistníkov alebo iné relevantné subjekty môže mať porušenie dôvernosti alebo neschopnosť zabezpečiť dostupnosť a integritu údajov okrem iného v súlade s nariadením (EÚ) 2016/679[7]. Poisťovňa alebo zaisťovňa by mala brať do úvahy najmä údaje, ktoré predstavujú obchodné tajomstvo a/alebo sú citlivé (napríklad zdravotné údaje poistníkov).

Usmernenie 8 – Posudzovanie rizika v súvislosti s cloudovým outsourcingom

30. Poisťovňa alebo zaisťovňa by vo všeobecnosti mala svoj prístup prispôsobiť povahe, rozsahu a komplexnosti rizík spojených so službami, ktoré sú outsourcované poskytovateľom cloudových služieb. Znamená to, že by sa mal posúdiť potenciálny vplyv akéhokoľvek cloudového outsourcingu, a to najmä na operačné riziko a riziko poškodenia dobrej povesti.

31. V prípade outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností poskytovateľom cloudových služieb by poisťovňa alebo zaisťovňa mala:

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

b. posúdiť riziká, ak je to vhodné a primerané, vrátane právneho rizika, rizika súvisiaceho s informačnými a komunikačnými technológiami, rizika súvisiaceho s dodržiavaním predpisov a rizika poškodenia dobrej povesti, ako aj obmedzenia dohľadu, ktoré súvisia:

    i. so zvolenou cloudovou službou a s navrhovanými modelmi využívania (t. j. verejnými/súkromnými/hybridnými/komunitnými),

    ii. s migráciou a/alebo implementáciou,

    iii. s činnosťami a príslušnými údajmi a systémami, ktoré sa plánujú outsourcovať (alebo sa už outsourcujú), s ich citlivosťou a požadovanými bezpečnostnými opatreniami,

    iv. s politickou stabilitou a bezpečnostnou situáciou krajín (v rámci EÚ alebo mimo nej), v ktorých sa poskytujú alebo môžu v budúcnosti poskytovať outsourcované služby a kde sa uchovávajú alebo sa pravdepodobne budú uchovávať údaje. V posúdení by sa mali zvážiť:

        1. platné zákony vrátane zákonov o ochrane údajov,

        2. platné ustanovenia na presadzovanie práva,

        3. ustanovenia o platobnej neschopnosti, ktoré by sa uplatňovali v prípade zlyhania poskytovateľa služieb, a akékoľvek obmedzenia, ktoré by vznikli v súvislosti

[7] 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 (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

s naliehavou potrebou obnovy údajov poisťovne alebo zaisťovne,

v. so sub-outsourcingom vrátane dodatočných rizík, ktoré môžu vzniknúť, ak sa subdodávateľ nachádza v tretej krajine alebo inej krajine ako poskytovateľ cloudových služieb a vzniká riziko, že dlhé a zložité sub-outsourcingové reťazce znižujú schopnosť poisťovne alebo zaisťovne dohliadať na zásadné alebo dôležité operačné funkcie alebo činnosti, ako aj schopnosť orgánov dohľadu vykonávať nad nimi účinný dohľad,

vi. s celkovým rizikom koncentrácie pre danú poisťovňu alebo zaisťovňu vyplývajúcim z dohôd s jedným poskytovateľom cloudových služieb vrátane outsourcingu takému poskytovateľovi cloudových služieb, ktorého nemožno ľahko nahradiť, alebo viacnásobných dohôd o outsourcingu s jedným poskytovateľom cloudových služieb. Pri posudzovaní rizika koncentrácie by poisťovňa alebo zaisťovňa (prípadne skupina) mala vziať do úvahy všetky svoje dohody o cloudovom outsourcingu s týmto poskytovateľom cloudových služieb.

32. Pred uzavretím dohody o cloudovom outsourcingu by sa malo vykonať posúdenie rizika. Ak poisťovňa alebo zaisťovňa zistí významné nedostatky a/alebo významné zmeny v poskytovaných službách alebo v situácii poskytovateľa cloudových služieb, posúdenie rizika by sa malo bezodkladne preskúmať alebo vykonať znovu. Ak dôjde k obnoveniu obsahu a rozsahu pôsobnosti dohody o cloudovom outsourcingu (napríklad k rozšíreniu rozsahu pôsobnosti alebo k začleneniu zásadných alebo dôležitých operačných funkcií do rozsahu pôsobnosti), posúdenie rizika by sa malo vykonať znovu.

Usmernenie 9 – Hĺbková analýza poskytovateľa cloudových služieb

33. Poisťovňa alebo zaisťovňa by mala v procese výberu a posudzovania zabezpečiť, aby poskytovateľ cloudových služieb spĺňal kritériá stanovené v písomnej politike outsourcingu.

34. Pred outsourcingom akejkoľvek operačnej funkcie alebo činnosti by poisťovňa alebo zaisťovňa mala vykonať hĺbkovú analýzu poskytovateľa cloudových služieb. Ak poisťovňa alebo zaisťovňa s poskytovateľom cloudových služieb, ktorý už bol posúdený, uzavrie druhú dohodu, na základe prístupu založeného na riziku vyhodnotí, či je potrebná druhá hĺbková analýza. Ak poisťovňa alebo zaisťovňa zistí významné nedostatky a/alebo významné zmeny v poskytovaných službách alebo v situácii poskytovateľa cloudových služieb, hĺbková analýza by sa mala bezodkladne preskúmať alebo vykonať znovu.

35. V prípade cloudového outsourcingu zásadných alebo dôležitých operačných funkcií by hĺbková analýza mala zahŕňať vyhodnotenie vhodnosti poskytovateľa cloudových služieb (napríklad jeho kompetentnosť, infraštruktúru, finančnú situáciu, podnikové a regulačné postavenie). Poisťovňa alebo zaisťovňa môže v prípade potreby použiť na podporu hĺbkovej analýzy dôkazy, certifikácie založené na medzinárodných normách, audítorské správy uznaných tretích strán alebo správy o vnútornom audite.

Usmernenie 10 – Zmluvné požiadavky

36. Príslušné práva a povinnosti poisťovne alebo zaisťovne a poskytovateľa cloudových služieb by mali byť jasne pridelené a stanovené v písomnej dohode.

37. Bez toho, aby boli dotknuté požiadavky stanovené v článku 274 delegovaného nariadenia, v prípade outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností poskytovateľovi cloudových služieb by sa v písomnej dohode uzavretej medzi poisťovňou alebo zaisťovňou a poskytovateľom cloudových služieb mali uviesť tieto informácie:

a. jasný opis outsourcovanej funkcie (cloudové služby vrátane typu podporných služieb),

b. dátum začiatku a prípadne ukončenia dohody, ako aj výpovedné lehoty pre poskytovateľa cloudových služieb a poisťovňu alebo zaisťovňu,

c. súdna príslušnosť a právo, ktorým sa riadi dohoda,

d. finančné záväzky zmluvných strán,

e. či je povolený sub-outsourcing zásadnej alebo dôležitej operačnej funkcie alebo činnosti (alebo jej významných častí), a ak áno, podmienky, ktorým sub-outsourcing takýchto významných funkcií podlieha (pozri usmernenie 13),

f. miesto alebo miesta (t. j. regióny alebo krajiny), kde sa príslušné údaje budú uchovávať a spracúvať (miesto dátových centier), a podmienky, ktoré musia byť splnené, vrátane požiadavky informovať poisťovňu alebo zaisťovňu, ak poskytovateľ služby navrhne zmenu miesta,

g. ustanovenia týkajúce sa prístupnosti, dostupnosti, integrity, dôvernosti, súkromia a bezpečnosti príslušných údajov s prihliadnutím na špecifikácie uvedené v usmernení 12,

h. právo poisťovne alebo zaisťovne pravidelne monitorovať činnosť poskytovateľa cloudových služieb,

i. dohodnuté úrovne poskytovaných služieb, ktoré by mali zahŕňať presné 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 poisťovni alebo zaisťovni vrátane prípadných povinností predkladať správy relevantné pre bezpečnostnú funkciu poisťovne alebo zaisťovne a pre kľúčové funkcie, napríklad správy o funkcii vnútorného auditu poskytovateľa cloudových služieb,

k. či by poskytovateľ cloudových služieb mal uzavrieť povinné poistenie proti určitým rizikám, prípadne úroveň požadovaného poistného krytia,

l. požiadavky na realizáciu a testovanie podnikateľských pohotovostných plánov,

m. povinnosť poskytovateľa cloudových služieb poskytnúť poisťovni alebo zaisťovni, jej orgánom dohľadu a akejkoľvek inej osobe, ktorú určila poisťovňa alebo zaisťovňa alebo ktorú určili orgány dohľadu:

    i. úplný prístup do všetkých relevantných podnikateľských priestorov (ústredia a prevádzkových centier), ako aj k celej škále príslušných zariadení, systémov, sietí, informácií a údajov používaných na poskytovanie outsourcovanej funkcie vrátane súvisiacich finančných informácií, zamestnancov a externých audítorov poskytovateľa cloudových služieb („práva na prístup“),

    ii. neobmedzené práva na previerku a audit v súvislosti s dohodou o cloudovom outsourcingu („práva na audit“), aby mohli monitorovať dohodu o outsourcingu a zabezpečili dodržiavanie všetkých platných regulačných a zmluvných požiadaviek,

n. ustanovenia, ktorými sa zabezpečuje, že v prípade platobnej neschopnosti, riešenia krízovej situácie alebo ukončenia podnikateľských činností poskytovateľa cloudových služieb môže poisťovňa alebo zaisťovňa bezodkladne obnoviť údaje, ktoré má vo svojom vlastníctve.

Usmernenie 11 – Právo na prístup a audit

38. Dohoda o cloudovom outsourcingu by nemala obmedzovať účinný výkon práv poisťovne alebo zaisťovne na prístup a audit ani jej možnosti kontroly cloudových služieb, ktorými si plní svoje regulačné povinnosti.

39. Poisťovňa alebo zaisťovňa by mala uplatňovať svoje práva na prístup a audit, ako aj určovať frekvenciu auditov a oblasti a služby, ktoré majú byť predmetom auditu, na základe prístupu založeného na posúdení rizika v súlade s oddielom 8 usmernení orgánu EIOPA týkajúcimi sa systému správy a riadenia.

40. Pri určovaní frekvencie a rozsahu uplatňovania svojich práv na prístup alebo audit by poisťovňa alebo zaisťovňa mala zvážiť, či cloudový outsourcing súvisí so zásadnou alebo dôležitou operačnou funkciou alebo činnosťou, povahu a rozsah rizika, ako aj vplyv dohôd o cloudovom outsourcingu na danú poisťovňu alebo zaisťovňu.

41. Ak uplatňovanie práv na prístup alebo audit, alebo použitie určitých audítorských metód predstavuje riziko pre prostredie poskytovateľa cloudových služieb a/alebo pre iného klienta poskytovateľa cloudových služieb (napríklad vplyv na úroveň služieb, dostupnosť údajov, aspekty dôvernosti), poisťovňa alebo zaisťovňa a poskytovateľ cloudových služieb by sa mali dohodnúť na alternatívnych spôsoboch poskytovania podobnej úrovne uistenia a služby poisťovni alebo zaisťovni (napríklad zahrnutie osobitných kontrol, ktoré sa overia v konkrétnej správe/certifikácii, ktorú vypracuje poskytovateľ cloudových služieb).

42. Bez toho, aby bola dotknutá ich konečná zodpovednosť za činnosti, ktoré vykonávajú poskytovatelia cloudových služieb, môžu poisťovne a zaisťovne v záujme efektívnejšieho využívania zdrojov auditu a zníženia organizačnej záťaže, ktorej je vystavený poskytovateľ cloudových služieb a jeho zákazníci, využívať:

a. certifikácie tretích strán a správy tretích strán alebo správy o vnútornom audite sprístupnené poskytovateľom cloudových služieb,

b. združené audity (t. j. vykonávané spoločne s inými klientmi toho istého poskytovateľa cloudových služieb) alebo združené audity vykonané treťou osobou, ktorú samy určili.

43. V prípade cloudového outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností, by poisťovne a zaisťovne mali využiť metódu uvedenú v odseku 42 písm. a) len vtedy, ak:

a. zabezpečia, že rozsah certifikácie alebo správy o audite zahŕňa systémy (napríklad procesy, aplikácie, infraštruktúru, dátové centrá atď.) a kontroly určené poisťovňou alebo zaisťovňou a že sa v rámci tohto rozsahu posudzuje dodržiavanie súladu s príslušnými regulačnými požiadavkami,

b. pravidelne a dôkladne hodnotia obsah nových certifikácií alebo správ o audite a overujú, či správy alebo certifikácie nie sú zastarané,

c. zabezpečia, že kľúčové systémy a kontroly sú pokryté v budúcich verziách certifikácie alebo správy o audite,

d. sú spokojné so schopnosťami strany, ktorá poskytuje certifikáciu alebo vykonáva audit (napríklad vzhľadom na rotáciu spoločnosti, ktorá poskytuje certifikáciu alebo vykonáva audit, na kvalifikáciu, odborné znalosti, opätovné vykonávanie/overovanie dôkazov v základnom audítorskom spise),

e. sú presvedčené, že certifikáty sa vydávajú a audity sa vykonávajú podľa príslušných noriem a zahŕňajú skúšku prevádzkovej účinnosti zavedených kľúčových kontrol,

f. majú zmluvné právo požiadať o rozšírenie rozsahu certifikácií alebo správ o audite na iné relevantné systémy a kontroly; počet a frekvencia týchto žiadostí o úpravu rozsahu by mali byť primerané a oprávnené z hľadiska riadenia rizík,

g. si zachovávajú zmluvné právo na vykonávanie jednotlivých auditov na mieste podľa vlastného uváženia, pokiaľ ide o cloudový outsourcing zásadných alebo dôležitých operačných funkcií alebo činností; takéto právo by sa malo uplatňovať v prípade špecifických potrieb, ktoré sa nedajú naplniť prostredníctvom iných typov interakcií s poskytovateľom cloudových služieb.

44. V prípade outsourcingu zásadných alebo dôležitých operačných funkcií poskytovateľom cloudových služieb by poisťovne a zaisťovne mali posúdiť, či sú certifikácie a správy tretích strán, ako sa uvádza v odseku 42 písm. a), primerané a dostatočné na to, aby poisťovne a zaisťovne dodržali svoje regulačné záväzky, pričom na základe prístupu založeného na riziku by sa dlhodobo nemali spoliehať výhradne na tieto správy.

45. Pred plánovanou návštevou na mieste by strana, ktorá si uplatňuje právo na prístup (poisťovňa alebo zaisťovňa, audítor alebo tretia strana konajúca v mene poisťovne alebo zaisťovne, prípadne poisťovní a zaisťovní), mala v primeranom čase vopred poskytnúť oznámenie s výnimkou prípadu, keď tak nie je možné urobiť v dôsledku výnimočnej alebo krízovej situácie. Takéto oznámenie by malo obsahovať miesto a účel návštevy a personál, ktorý sa na návšteve zúčastní.

46. Vzhľadom na technickú komplexnosť cloudových riešení by poisťovňa alebo zaisťovňa mala overiť, či zamestnanci vykonávajúci audit – či už ide o vlastných vnútorných audítorov alebo o skupinu audítorov konajúcich v jej mene, alebo o audítorov určených poskytovateľom cloudových služieb – prípadne zamestnanci, ktorí skúmajú certifikáciu tretích strán alebo správy poskytovateľa služieb o audite, majú potrebné schopnosti a znalosti na vykonávanie príslušných auditov a/alebo hodnotení.

Usmernenie 12 – Bezpečnosť údajov a systémov

47. Poisťovňa alebo zaisťovňa by mala zaistiť, aby poskytovatelia cloudových služieb dodržiavali európske a vnútroštátne predpisy, ako aj príslušné bezpečnostné normy IKT.

48. V prípade outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností poskytovateľom cloudových služieb by poisťovňa alebo zaisťovňa mala v dohode o outsourcingu dodatočne stanoviť osobitné požiadavky na bezpečnosť informácií a pravidelne monitorovať dodržiavanie týchto požiadaviek.

49. Na účely odseku 48, v prípade outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností poskytovateľom cloudových služieb by poisťovňa alebo zaisťovňa na základe prístupu založeného na riziku a pri zohľadnení svojich povinností a povinností poskytovateľa cloudových služieb mala:

a. dohodnúť sa s poskytovateľom cloudových služieb na jasne definovaných úlohách a povinnostiach v súvislosti s operačnými funkciami alebo činnosťami, ktoré sú ovplyvnené cloudovým outsourcingom a ktoré by sa mali jasne rozdeliť,

b. rozhodnúť o primeranej úrovni ochrany dôverných údajov, kontinuite outsourcovaných činností, integrite a vysledovateľnosti údajov a systémov v kontexte plánovaného cloudového outsourcingu a vymedziť ich,

c. v prípade potreby zvážiť špecifické opatrenia pre prenášané údaje, údaje v pamäti a uložené údaje, napríklad použitie šifrovacích technológií v kombinácii s vhodnou štruktúrou správy kľúčov,

d. zvážiť mechanizmy integrácie cloudových služieb so systémami poisťovní a zaisťovní, napríklad aplikačné programové rozhrania a spoľahlivý proces riadenia používateľov a prístupu,

e. zmluvne zabezpečiť, aby dostupnosť siete a očakávaná kapacita spĺňali požiadavky na silnú kontinuitu, ak je to uplatniteľné a uskutočniteľné,

f. v prípade potreby rozhodnúť o vhodných požiadavkách na kontinuitu, ktorými sa zabezpečia primerané úrovne na každom stupni technologického reťazca, a vymedziť tieto požiadavky,

g. zabezpečiť spoľahlivý a dobre zdokumentovaný proces riadenia incidentov vrátane určenia príslušných povinností, napríklad vymedzením modelu spolupráce v prípade skutočného alebo predpokladaného výskytu incidentov,

h. prijať prístup založený na posúdení rizika, pokiaľ ide o uchovávanie údajov a miesto alebo miesta spracúvania údajov (t. j. krajinu alebo región), ako aj aspekty bezpečnosti informácií,

i. monitorovať plnenie požiadaviek týkajúcich sa účinnosti a efektívnosti kontrolných mechanizmov zavedených poskytovateľom cloudových služieb, ktoré by zmiernili riziká súvisiace s poskytovanými službami.

Usmernenie 13 – Sub-outsourcing zásadných alebo dôležitých operačných funkcií a činností

50. Ak je povolený sub-outsourcing zásadných alebo dôležitých operačných funkcií (alebo ich časti), v dohode o cloudovom outsourcingu medzi poisťovňou alebo zaisťovňou a poskytovateľom cloudových služieb treba:

a. stanoviť všetky druhy činností, ktoré sú vylúčené z potenciálneho sub-outsourcingu,

b. uviesť podmienky, ktoré je nutné dodržiavať v prípade sub-outsourcingu (napríklad to, že aj subdodávateľ musí v plnej miere dodržiavať príslušné záväzky poskytovateľa cloudových služieb). Tieto záväzky zahŕňajú práva na audit a prístup a bezpečnosť údajov a systémov,

c. uviesť, že poskytovateľ cloudových služieb si zachováva plnú zodpovednosť a dohľad nad sub-outsourcovanými službami,

d. zahrnúť povinnosť poskytovateľa cloudových služieb informovať poisťovňu alebo zaisťovňu o všetkých plánovaných významných zmenách v subdodávateľoch alebo v sub-outsourcovaných službách, ktoré by mohli ovplyvniť schopnosť poskytovateľa služieb plniť si povinnosti podľa dohody o cloudovom outsourcingu. Lehota na oznámenie týchto zmien by mala byť taká, aby poisťovňa alebo zaisťovňa mohla vykonať aspoň posúdenie rizika vplyvov navrhovaných zmien pred tým, ako samotná zmena v subdodávateľoch alebo v sub-outsourcovaných službách nadobudne účinnosť,

e. v prípadoch, keď poskytovateľ cloudových služieb plánuje zmeny subdodávateľa alebo sub-outsourcovaných služieb, ktoré by mali nepriaznivý vplyv na posudzovanie rizika dohodnutých služieb, zabezpečiť, aby poisťovňa

alebo zaisťovňa mala právo namietať takéto zmeny a/alebo právo odstúpiť od zmluvy a zmluvu ukončiť.

Usmernenie 14 – Monitorovanie a dohľad nad dohodami o cloudovom outsourcingu

51. Poisťovňa alebo zaisťovňa by mala pravidelne monitorovať vykonávanie činností, bezpečnostné opatrenia a dodržiavanie dohodnutej úrovne služieb zo strany poskytovateľov cloudových služieb na základe prístupu založeného na posúdení rizík. Hlavný dôraz by sa mal klásť na cloudový outsourcing zásadných a dôležitých operačných funkcií.

52. Na tento účel by poisťovňa alebo zaisťovňa mala zaviesť mechanizmy monitorovania a dohľadu, v rámci ktorých by sa zohľadňovalo, ak je to uskutočniteľné a vhodné, či sa zásadné alebo dôležité operačné funkcie alebo ich časť vykonávajú prostredníctvom sub-outsourcingu.

53. Správny, riadiaci alebo kontrolný orgán by si mal pravidelne zisťovať aktuálny stav rizík zistených pri cloudovom outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností.

54. Aby poisťovne a zaisťovne zabezpečili primerané monitorovanie svojich dohôd o cloudovom outsourcingu a dohľad nad nimi, mali by využívať dostatok zdrojov s primeranými schopnosťami a vedomosťami v oblasti monitorovania služieb poskytovaných externe v cloudovom prostredí. Zamestnanci poisťovne alebo zaisťovne zodpovední za tieto činnosti by mali mať potrebné znalosti v oblasti IKT aj v oblasti podnikania.

Usmernenie 15 – Právo na ukončenie zmluvy a stratégie ukončenia angažovanosti

55. V prípade cloudového outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností, by dohoda o cloudovom outsourcingu mala obsahovať doložku o jasne vymedzenej stratégii ukončenia angažovanosti, na základe ktorej by poisťovňa alebo zaisťovňa v prípade potreby mohla dohodu ukončiť. Takéto ukončenie by malo byť možné bez narušenia kontinuity a kvality poskytovania služieb poistníkom. Na dosiahnutie tohto cieľa by poisťovňa alebo zaisťovňa mala:

a. vypracovať plány ukončenia, ktoré budú komplexné, založené na službách, zdokumentované a dostatočne overené (napríklad vykonaním analýzy potenciálnych nákladov, vplyvov, zdrojov a časových dôsledkov rôznych potenciálnych možností ukončenia dohody),

b. určiť alternatívne riešenia a vypracovať vhodné a uskutočniteľné plány prechodu, aby poisťovňa alebo zaisťovňa mohla odstrániť a presunúť existujúce činnosti a údaje od poskytovateľa cloudových služieb k iným poskytovateľom služieb alebo späť danej poisťovni alebo zaisťovni. Tieto riešenia by sa mali stanoviť so zreteľom na výzvy, ktoré môže spôsobiť umiestnenie údajov, pričom by sa mali prijať potrebné opatrenia na zabezpečenie kontinuity činností v prechodnej fáze,

c. zabezpečiť, aby poskytovateľ cloudových služieb primerane pomáhal poisťovni alebo zaisťovni s presunom outsourcovaných údajov, systémov alebo aplikácií k inému poskytovateľovi služieb alebo priamo danej poisťovni alebo zaisťovni,

d. dohodnúť sa s poskytovateľom cloudových služieb, že po presune údajov na poisťovňu alebo zaisťovňu tieto údaje úplne a bezpečne vymaže vo všetkých regiónoch.

56. Pri vytváraní stratégií ukončenia angažovanosti by poisťovňa alebo zaisťovňa mala zvážiť tieto skutočnosti:

a. vymedzenie cieľov stratégie ukončenia angažovanosti,

b. vymedzenie spúšťacích udalostí (napríklad kľúčové indikátory rizika, ktoré vykazujú neprijateľnú úroveň služby), ktoré by mohli aktivovať stratégiu ukončenia angažovanosti,

c. vykonanie analýzy vplyvu na podnikanie, ktorá zodpovedá outsourcovaným činnostiam, s cieľom určiť, aké ľudské a materiálne zdroje by boli potrebné na vykonanie plánu ukončenia angažovanosti a koľko času by to zabralo,

d. pridelenie úloh a povinností pri riadení plánov ukončenia angažovanosti a prechodných činností,

e. vymedzenie kritérií úspešnosti prechodu.

Usmernenie 16 – Dohľad nad dohodami o cloudovom outsourcingu zo strany orgánov dohľadu

57. Orgány dohľadu by v rámci procesu preskúmania mali vykonať analýzu vplyvov vyplývajúcich z dohôd poisťovní a zaisťovní o cloudovom outsourcingu. Analýza vplyvov by mala byť zameraná najmä na dohody o cloudovom outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností.

58. Orgány dohľadu by pri vykonávaní dohľadu nad dohodami o cloudovom outsourcingu mali zvážiť tieto riziká:

a. riziká súvisiace s IKT,

b. iné operačné riziká (vrátane právneho rizika a rizika nedodržania súladu s predpismi, rizika súvisiaceho s outsourcingom a rizika riadenia treťou stranou),

c. riziko poškodenia dobrej povesti,

d. riziko koncentrácie, a to aj na úrovni krajiny/sektora.

59. Pri posudzovaní by orgány dohľadu mali zvoliť prístup založený na posúdení rizík a zahrnúť tieto aspekty:

a. primeranosť a účinnosť postupov riadenia a prevádzkových postupov poisťovne alebo zaisťovne, ktoré súvisia so schvaľovaním, vykonávaním, monitorovaním, riadením a obnovou dohôd o cloudovom outsourcingu,

b. či má poisťovňa alebo zaisťovňa dostatočné zdroje s primeranými schopnosťami a vedomosťami v oblasti monitorovania služieb poskytovaných externe v cloudovom prostredí,

c. či poisťovňa alebo zaisťovňa identifikuje a riadi všetky riziká zdôraznené v týchto usmerneniach.

60. V prípade skupín by orgán dohľadu nad skupinou mal zabezpečiť, aby sa vplyvy cloudového outsourcingu zásadných alebo dôležitých operačných funkcií alebo činností zohľadnili v posúdení rizika na úrovni skupiny s prihliadnutím na požiadavky uvedené v odsekoch 58 – 59 a na konkrétne riadiace a operačné vlastnosti skupiny.

61. Ak sa cloudový outsourcing zásadných alebo dôležitých operačných funkcií alebo činností vzťahuje na viac ako jednu poisťovňu alebo zaisťovňu v rôznych členských

štátoch a je riadený centrálne materskou spoločnosťou alebo dcérskou skupinou (napríklad poisťovňou alebo zaisťovňou alebo spoločnosťou poskytujúcou služby skupine, ako je napríklad skupinový poskytovateľ IKT), orgán dohľadu nad skupinou a/alebo príslušné orgány dohľadu vykonávajúce dohľad nad poisťovňami a zaisťovňami, ktoré sa podieľajú na cloudovom outsourcingu, by mali v prípade potreby prerokovať vplyv cloudového outsourcingu na rizikový profil skupiny v rámci kolégia orgánov dohľadu.

62. Ak sú zistené obavy, ktoré vedú k záveru, že poisťovňa alebo zaisťovňa už nemá zavedené solídne mechanizmy riadenia alebo nedodržiava regulačné požiadavky, orgány dohľadu by mali prijať primerané opatrenia, akými môže byť napríklad požiadavka, aby poisťovňa alebo zaisťovňa zlepšila mechanizmy správy a riadenia, znížila alebo obmedzila rozsah outsourcovaných funkcií, alebo ukončila jednu alebo viacero dohôd o outsourcingu. Vzhľadom na nutnosť zabezpečiť prevádzkovú kontinuitu poisťovne alebo zaisťovne sa môže vyžadovať najmä zrušenie zmlúv, ak dohľad nad regulačnými požiadavkami a ich presadzovanie nie je možné zabezpečiť inými opatreniami.

Pravidlá dodržiavania odporúčaní a oznamovania

63. Tento dokument obsahuje usmernenia vydané v zmysle článku 16 nariadenia (EÚ) č. 1094/2010. V súlade s článkom 16 ods. 3 tohto nariadenia musia príslušné orgány a finančné inštitúcie vynaložiť všetko úsilie na dodržiavanie usmernení a odporúčaní.

64. Príslušné orgány, ktoré dodržiavajú alebo majú v úmysle dodržiavať tieto usmernenia, by ich mali vhodným spôsobom začleniť do regulačného rámca alebo rámca dohľadu.

65. Príslušné orgány musia do dvoch mesiacov od dátumu vydania preložených verzií potvrdiť orgánu EIOPA, či usmernenia dodržiavajú alebo majú v úmysle dodržiavať, a v prípade, že usmernenia nedodržiavajú, uvedú dôvody.

66. V prípade neposkytnutia odpovede do tohto termínu sa príslušné orgány budú považovať za orgány, ktoré nedodržiavajú povinnosť informovať, a táto skutočnosť bude zverejnená.

Záverečné ustanovenie o preskúmaní

67. Tieto odporúčania budú predmetom preskúmania orgánom EIOPA.