

# **Smjernice o izdvajanju poslova pružateljima usluga računalstva u oblaku**

## Sadržaj

Uvod.....	3
Definicije.....	3
Datum početka primjene .....	4
Smjernica 1. – Usluge računalstva u oblaku i izdvajanje poslova .....	6
Smjernica 2. – Opća načela upravljanja izdvajanjem poslova računalstva u oblaku .....	6
Smjernica 3. – Ažuriranje pisanih pravila o izdvajanju.....	6
Smjernica 4. – Pisana obavijest nadzornom tijelu .....	7
Smjernica 5. – Zahtjevi u pogledu dokumentacije.....	8
Smjernica 6. – Analiza koja prethodi izdvajanju poslova .....	9
Smjernica 7. – Procjena ključnih ili važnih poslovnih funkcija i djelatnosti.....	9
Smjernica 8. – Procjena rizika u pogledu izdvajanja poslova računalstva u oblaku .....	10
Smjernica 9. – Dubinska analiza pružatelja usluga računalstva u oblaku.....	11
Smjernica 10. – Ugovorni zahtjevi .....	11
Smjernica 11. – Pravo na pristup i reviziju.....	13
Smjernica 12. – Sigurnost podataka i sustava .....	14
Smjernica 13. – Podizdvajanje ključnih ili važnih poslovnih funkcija odnosno djelatnosti.....	15
Smjernica 14. – Praćenje i nadzor sporazuma o izdvajanju poslova računalstva u oblaku .....	16
Smjernica 15. – Prava u pogledu raskida i izlazne strategije .....	16
Smjernica 16. – Nadzor sporazuma o izdvajanju poslova računalstva u oblaku koji provode nadzorna tijela .....	17
Pravila o usklađenosti i izvješćivanju.....	18
Završna odredba o pregledu .....	18

## Uvod

1. U skladu s člankom 16. Uredbe (EU) br. 1094/2010<sup>1</sup> EIOPA izdaje smjernice u svrhu pružanja smjernica društvima za osiguranje i društvima za reosiguranje o tome na koji je način potrebno primijeniti odredbe o izdvajanju poslova iz Direktive 2009/138/EZ<sup>2</sup> („Direktiva Solventnost II“) i Delegirane uredbe Komisije (EU) br. 2015/35<sup>3</sup> („Delegirana uredba“) u slučaju izdvajanja poslova pružateljima usluga računalstva u oblaku.
2. Ove se smjernice temelje na članku 13. stavku 28., članku 38. i članku 49. Direktive Solventnost II te na članku 274. Delegirane uredbe. Usto, ove se smjernice oslanjaju i na smjernice pružene u okviru EIOPA-inih Smjernica o sustavu upravljanja (EIOPA-BoS-14/253).
3. Ove smjernice namijenjene su nadležnim tijelima u svrhu davanja smjernica o tome kako bi društva za osiguranje i društva za reosiguranje (zajedno „društva“) trebala primjenjivati zahtjeve u pogledu izdvajanja poslova propisane prethodno spomenutim pravnim aktima u kontekstu izdvajanja poslova pružateljima usluga računalstva u oblaku.
4. Smjernice se primjenjuju *mutatis mutandis* i na pojedinačna društva i na grupe društava<sup>4</sup>.

Subjekti koji podliježu drugim sektorskim zahtjevima, a koji su dio grupe, isključeni su iz područja primjene ovih smjernica na pojedinačnoj razini s obzirom na to da moraju slijediti zahtjeve specifične za njihov sektor te relevantne smjernice koje je izdalo Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala te Europsko nadzorno tijelo za bankarstvo.

5. U slučaju izdvajanja poslova unutar grupe i podizdvajanja poslova pružateljima usluga računalstva u oblaku unutar grupe, ove se smjernice potrebno primjenjivati zajedno s odredbama EIOPA-inih Smjernica o sustavu upravljanja u pogledu izdvajanja poslova unutar grupe.
6. Kad postupaju u skladu s ovim smjernicama ili nadgledaju usklađenost s njima, društva i nadležna tijela trebala bi uzeti u obzir načelo proporcionalnosti<sup>5</sup> te ključno značenje ili važnost usluge koja se izdvaja pružateljima usluga računalstva u oblaku. Načelom proporcionalnosti trebalo bi se zajamčiti da sustavi upravljanja, uključujući one povezane s izdvajanjem poslova pružateljima usluga računalstva u oblaku, budu razmjerni prirodi, opsegu i složenosti temeljnih rizika.
7. Ove bi se smjernice trebale čitati zajedno s EIOPA-inim Smjernicama o sustavu upravljanja i propisima navedenima u stavku 1., ne dovodeći ih u pitanje.

## Definicije

8. Pojmovi koji nisu definirani u ovim smjernicama imaju značenje definirano u pravnim aktima navedenima u uvodu.

---

<sup>1</sup> Uredba (EU) br. 1094/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju Europskog nadzornog tijela (Europsko nadzorno tijelo za osiguranje i strukovno mirovinsko osiguranje), o izmjeni Odluke br. 716/2009/EZ i o stavljanju izvan snage Odluke Komisije 2009/79/EZ (SL L 331, 15.12.2010., str. 48.).

<sup>2</sup> Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).

<sup>3</sup> Delegirana uredba Komisije (EU) 2015/35 od 10. listopada 2014. o dopuni Direktive 2009/138/EZ Europskog parlamenta i Vijeća o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 12, 17.1.2015., str. 1.).

<sup>4</sup> Članak 212. stavak 1. Direktive Solventnost II.

<sup>5</sup> Članak 29. stavak 3. Direktive Solventnost II.

9. Osim toga, za potrebe ovih smjernica primjenjuju se sljedeće definicije:

Pružatelj usluga	znači treća strana koja obavlja određeni postupak, uslugu ili aktivnost ili dijelove postupka, usluge ili aktivnosti, u okviru sporazuma o izdvajanju poslova.
Pružatelj usluga računalstva u oblaku	znači pružatelj usluga kako je prethodno definiran, koji je odgovoran za pružanje usluga računalstva u oblaku u okviru sporazuma o izdvajanju poslova.
Usluge računalstva u oblaku	znači usluge koje se pružaju putem računalstva u oblaku, odnosno modela kojim se na zahtjev omogućuje široko rasprostranjen, pogodan mrežni pristup zajedničkom skupu podesivih računalnih resursa (npr. mreža, poslužitelja, uređaja za pohranu podataka, aplikacija i usluga), koji se mogu brzo pribaviti i otpustiti uz minimalan napor u pogledu upravljanja ili minimalnu interakciju s pružateljem usluga.
Javni oblak	znači infrastruktura za usluge računalstva u oblaku dostupna za uporabu široj javnosti.
Privatni oblak	znači infrastruktura za usluge računalstva u oblaku dostupna za uporabu isključivo jednom društvu.
Zajednički oblak	znači infrastruktura za usluge računalstva u oblaku dostupna za uporabu isključivo određenoj skupini društava, npr. nekoliko društava iz jedne grupe.
Hibridni oblak	znači infrastruktura za usluge računalstva u oblaku sastavljena od dviju ili više različitih infrastruktura za usluge računalstva u oblaku.

### Datum početka primjene

10. Ove se smjernice počinju primjenjivati od 1. siječnja 2021. na sve sporazume o izdvajanju poslova računalstva u oblaku zaključene ili izmijenjene na taj datum ili nakon njega.
11. U skladu s tim, društva bi trebala preispitati i na odgovarajući način izmijeniti postojeće sporazume o izdvajanju poslova računalstva u oblaku povezane s ključnim ili važnim poslovnim funkcijama odnosno djelatnostima kako bi osigurala usklađenost s ovim smjernicama do 31. prosinca 2022.
12. Ako preispitivanje sporazuma o izdvajanju poslova računalstva u oblaku povezanih s ključnim ili važnim poslovnim funkcijama odnosno djelatnostima ne bude dovršeno do 31. prosinca 2022., društvo bi o tome trebalo obavijestiti svoje nadzorno tijelo<sup>6</sup>. Usto, društvo nadzorno tijelo treba obavijestiti i o planiranim mjerama za potrebe dovršetka preispitivanja ili o mogućoj izlaznoj strategiji. Nadzorno tijelo prema potrebi može dogovoriti s društvom produljenje roka za dovršetak preispitivanja.
13. Politike i interne procese društva trebalo bi ažurirati (ako je to potrebno) do 1. siječnja 2021., dok bi zahtjeve u pogledu dokumentacije za sporazume o izdvajanju poslova računalstva u oblaku povezane s ključnim ili važnim poslovnim funkcijama odnosno djelatnostima trebalo provesti do 31. prosinca 2022.

---

<sup>6</sup> Članak 13. stavak 10. Direktive Solventnost II.



## **Smjernica 1. – Usluge računalstva u oblaku i izdvajanje poslova**

14. Društvo bi trebalo utvrditi potpada li sporazum s određenim pružateljem usluga računalstva u oblaku pod definiciju izdvajanja poslova u skladu s Direktivom Solventnost II. U okviru ocjene trebalo bi razmotriti sljedeća pitanja:
  - a. obavlja li se izdvojena poslovna funkcija odnosno djelatnost (ili njezin dio) periodično ili kontinuirano; te
  - b. bi li tu poslovnu funkciju odnosno djelatnost (ili njezin dio) obuhvaćale poslovne funkcije odnosno djelatnosti koje bi društvo obavljalo ili moglo obavljati u okviru uobičajenih poslovnih aktivnosti, čak i ako društvo tu poslovnu funkciju odnosno djelatnost nije obavljalo nikada prije.
15. Ako sporazum s pružateljem usluga pokriva više poslovnih funkcija ili djelatnosti, društvo bi u okviru ocjene trebalo razmotriti sve aspekte sporazuma.
16. U slučajevima kada društvo poslovne funkcije ili djelatnosti izdvaja pružateljima usluga koji nisu pružatelji usluga računalstva u oblaku, ali se u svrhu pružanja svojih usluga u velikoj mjeri oslanjaju na infrastrukturu računalstva u oblaku (primjerice, kada je pružatelj usluga računalstva u oblaku dio lanca podizdvajanja poslova), sporazum o takvom obliku izdvajanja poslova isto je tako obuhvaćen područjem primjene ovih smjernica.

## **Smjernica 2. – Opća načela upravljanja izdvajanjem poslova računalstva u oblaku**

17. Ne dovodeći u pitanje članak 274. stavak 3. Delegirane uredbe, upravno, upravljačko ili nadzorno tijelo društva trebalo bi zajamčiti da se svaka odluka o izdvajanju ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružateljima usluga računalstva u oblaku temelji na iscrpnoj procjeni svih relevantnih rizika koje sporazum podrazumijeva, poput rizika informacijske i komunikacijske tehnologije, rizika u pogledu kontinuiteta poslovanja, pravnih rizika, rizika u pogledu usklađenosti, rizika koncentracije i drugih operativnih rizika te rizika povezanih s fazom migracije podataka i/ili provedbe, kada je to primjenjivo.
18. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružateljima usluga računalstva u oblaku, društvo bi, ako je to potrebno, trebalo zajamčiti da njegova vlastita procjena rizika i solventnosti odražava promjene u njegovu profilu rizičnosti koje su nastupile uslijed sporazuma o izdvajanju poslova računalstva u oblaku.
19. Upotreba usluga računalstva u oblaku trebala bi biti usklađena sa strategijama društva (primjerice, strategijom informacijske i komunikacijske tehnologije, strategijom informacijske sigurnosti, strategijom upravljanja operativnim rizicima) te njegovim internim politikama i procesima, koji bi se trebali ažurirati ako je to potrebno.

## **Smjernica 3. – Ažuriranje pisanih pravila o izdvajanju**

20. U slučaju izdvajanja poslova pružateljima usluga računalstva u oblaku društvo bi trebalo ažurirati pisana pravila o izdvajanju (primjerice, na način da ih preispita, priloži im zaseban dodatak ili izradi nova posebna pravila) te druga relevantna interna pravila (primjerice, u pogledu informacijske sigurnosti), pritom uzimajući u obzir posebnosti izdvajanja poslova računalstva u oblaku barem u odnosu na sljedeća područja:
  - a. uloge i odgovornosti uključenih funkcija društva, osobito upravnog, upravljačkog ili nadzornog tijela, te funkcija koje su odgovorne za informacijsku

i komunikacijsku tehnologiju, informacijsku sigurnost, usklađenost, upravljanje rizicima i unutarnju reviziju;

- b. postupke te procedure izvješćivanja koji su potrebni za odobrenje, provedbu, praćenje i obnovu, kada je to primjenjivo, sporazuma o izdvajanju poslova računalstva u oblaku povezanih s ključnim ili važnim poslovnim funkcijama odnosno djelatnostima te upravljanje njima;
- c. nadzor usluga računalstva u oblaku razmjernan prirodi, opsegu i složenosti rizika svojstvenih pruženim uslugama, uključujući i. procjenu rizika sporazumâ o izdvajanju usluga računalstva u oblaku i dubinsku analizu pružatelja usluga računalstva u oblaku, uključujući učestalost procjene rizika; ii. praćenje i upravljačke kontrole (primjerice, provjera sporazuma o razini usluga); iii. sigurnosne standarde i kontrole;
- d. u pogledu izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku, trebalo bi se pozvati na ugovorne zahtjeve, kako je opisano u smjernici 10.;
- e. zahtjeve u pogledu dokumentacije i pisane obavijesti za nadzorno tijelo u vezi s izdvajanjem ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku;
- f. u odnosu na svaki sporazum o izdvajanju poslova računalstva u oblaku koji obuhvaća ključne ili važne poslovne funkcije odnosno djelatnosti, zahtjev za dokumentiranom i, ako je potrebno, dostatno testiranom „izlaznom strategijom“ koja je razmjerna prirodi, opsegu i složenosti rizika svojstvenih pruženim uslugama. Izlazna strategija može podrazumijevati niz postupaka prekida pružanja usluga, uključujući ali ne ograničavajući se na ukidanje, reintegriranje ili prenošenje usluga obuhvaćenih sporazumom o izdvajanju poslova računalstva u oblaku.

#### **Smjernica 4. – Pisana obavijest nadzornom tijelu**

- 21. Zahtjevi u pogledu pisane obavijesti koji su propisani člankom 49. stavkom 3. Direktive Solventnost II i detaljnije razrađeni u EIOPA-inim Smjernicama o sustavu upravljanja primjenjivi su na svako izdvajanje ključnih ili važnih poslovnih funkcija i djelatnosti pružateljima usluga računalstva u oblaku. U slučaju da izdvojena poslovna funkcija ili djelatnost koja prethodno nije bila opisana kao ključna ili važna postane ključna odnosno važna, društvo bi o tome trebalo obavijestiti nadzorno tijelo.
- 22. Uzimajući u obzir načelo proporcionalnosti, pisana obavijest društva trebala bi uključivati barem sljedeće informacije:
  - a. kratak opis poslovne funkcije ili djelatnosti koja se izdvaja;
  - b. datum početka i, prema potrebi, datum sljedećeg produženja ugovora, datum završetka i/ili otkazne rokove za pružatelja usluga računalstva u oblaku i za društvo;
  - c. mjerodavno pravo za ugovor o izdvajanju poslova računalstva u oblaku;
  - d. naziv pružatelja usluga računalstva u oblaku, broj iz registra poslovnih subjekata, identifikacijsku oznaku pravne osobe (ako je dostupna), registriranu adresu i druge relevantne podatke za kontakt te naziv matičnog društva (ako postoji); u slučaju da se radi o grupama, pripada li pružatelj usluga računalstva u oblaku određenoj grupi ili ne;
  - e. model usluge računalstva u oblaku i implementacijske modele računalstva u oblaku (tj. javni/privatni/hibridni/zajednički) te konkretnu prirodu podataka

koje je potrebno čuvati i lokacije (tj. zemlje ili regije) na kojima će se ti podatci pohranjivati;

- f. kratak sažetak razloga zbog kojih se izdvojena poslovna funkcija odnosno djelatnost smatra ključnom ili važnom;
- g. datum posljednje procjene ključnog značenja ili važnosti koju ima izdvojena poslovna funkcija ili djelatnost.

### **Smjernica 5. – Zahtjevi u pogledu dokumentacije**

- 23. U okviru svojeg sustava upravljanja i sustava upravljanja rizicima društvo bi trebalo voditi evidenciju sporazuma o izdvajanju poslova računalstva u oblaku, primjerice u obliku posebnog registra koji će voditi i s vremena na vrijeme ažurirati. Društvo bi trebalo voditi i evidenciju raskinutih sporazuma o izdvajanju poslova računalstva u oblaku tijekom odgovarajućeg razdoblja čuvanja podataka podložno nacionalnim propisima.
- 24. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti, društvo bi trebalo zabilježiti sve sljedeće informacije:
  - a. informacije o kojima mora obavijestiti nadzorno tijelo, kako je propisano smjernicom 4.;
  - b. u slučaju grupa, društva za osiguranje ili društva za reosiguranje te druga društva koja ulaze u obuhvat bonitetne konsolidacije te koja koriste usluge računalstva u oblaku;
  - c. datum posljednje procjene rizika i kratak sažetak glavnih rezultata;
  - d. osobu ili tijelo nadležno za odlučivanje (primjerice, upravno, upravljačko ili nadzorno tijelo) u društvu koje je odobrilo sporazum o izdvajanju poslova računalstva u oblaku;
  - e. datum posljednje i sljedeće planirane revizije, ako je primjenjivo;
  - f. imena svih podizvođača kojima se podizdvajaju značajni dijelovi ključne ili važne poslovne funkcije odnosno djelatnosti, uključujući zemlje u kojima su podizvođači registrirani, zemlje u kojima će se pružati usluga te, ako je primjenjivo, lokacije (tj. zemlje ili regije) na kojima će se podatci pohranjivati;
  - g. ishod procjene zamjenjivosti pružatelja usluga računalstva u oblaku (primjerice, jednostavna, teška ili nemoguća);
  - h. podržava li izdvojena ključna ili važna poslovna funkcija odnosno djelatnost poslovne aktivnosti za koje je pitanje vremena posebno važno;
  - i. procjenu godišnjeg proračunskog troška;
  - j. ima li društvo izlaznu strategiju u slučaju da bilo koja strana raskine ugovor ili u slučaju da pružatelj usluga računalstva u oblaku prestane pružati usluge.
- 25. U slučaju izdvajanja poslovnih funkcija ili djelatnosti koje nisu ključne odnosno važne, društvo bi trebalo definirati informacije koje je potrebno zabilježiti na temelju prirode, opsega i složenosti rizika sadržanih u uslugama koje pruža pružatelj usluga računalstva u oblaku.
- 26. Društvo bi trebalo nadzornom tijelu na zahtjev dati na uvid sve informacije koje su nadzornom tijelu potrebne radi obavljanja nadzora društva, uključujući presliku ugovora o izdvajanju poslova.



## **Smjernica 6. – Analiza koja prethodi izdvajanju poslova**

27. Prije nego što zaključi bilo kakav sporazum s pružateljima usluga računalstva u oblaku, društvo bi trebalo učiniti sljedeće:

- a. procijeniti odnosi li se sporazum o izdvajanju poslova računalstva u oblaku na ključne ili važne poslovne funkcije odnosno djelatnosti u skladu sa smjernicom 7.;
- b. utvrditi i procijeniti sve relevantne rizike koji proizlaze iz sporazuma o izdvajanju poslova računalstva u oblaku u skladu sa smjernicom 8.;
- c. provesti odgovarajuću dubinsku analizu potencijalnog pružatelja usluga računalstva u oblaku u skladu sa smjernicom 9.;
- d. utvrditi i procijeniti sukobe interesa do kojih izdvajanje poslova može dovesti u skladu sa zahtjevima propisanim člankom 274. stavkom 3. točkom (b) Delegirane uredbe.

## **Smjernica 7. – Procjena ključnih ili važnih poslovnih funkcija i djelatnosti**

28. Prije nego što zaključi bilo kakav sporazum o izdvajanju poslova s pružateljima usluga računalstva u oblaku, društvo bi trebalo procijeniti odnosi li se sporazum o izdvajanju poslova računalstva u oblaku na poslovnu funkciju odnosno djelatnost koja je ključna ili važna. Pri obavljanju takve procjene, ako je primjenjivo, društvo bi trebalo razmotriti postoji li mogućnost da takav sporazum postane ključan ili važan u budućnosti. Društvo bi isto tako trebalo ponovno procijeniti ključno značenje ili važnost poslovne funkcije ili djelatnosti koju je prethodno izdvajalo pružateljima usluga računalstva u oblaku ako se priroda, opseg i složenost rizika sadržanih u ugovoru bitno promijene.

29. U okviru procjene društvo bi uz ishod procjene rizika trebalo uzeti u obzir barem sljedeće čimbenike:

- a. potencijalni utjecaj bilo kakvog bitnog prekida izdvojene poslovne funkcije ili djelatnosti odnosno nemogućnosti pružatelja usluga računalstva u oblaku da pruža usluge na dogovorenoj razini usluge na:
  - i. kontinuiranu usklađenost društva s njegovim regulatornim obvezama;
  - ii. kratkoročnu i dugoročnu financijsku otpornost i održivost društva te njegovu kratkoročnu i dugoročnu otpornost i održivost u pogledu solventnosti;
  - iii. kontinuitet poslovanja društva i operativnu otpornost;
  - iv. operativni rizik, uključujući rizik nesavjesnog ponašanja, rizik informacijsko-komunikacijske tehnologije te pravni rizik;
  - v. reputacijske rizike;
- b. potencijalni utjecaj sporazuma o izdvajanju poslova računalstva u oblaku na sposobnost društva da:
  - i. utvrdi i prati sve relevantne rizike te upravlja njima;
  - ii. ispunji sve pravne i regulatorne zahtjeve;
  - iii. provodi odgovarajuće revizije u pogledu poslovne funkcije ili djelatnosti koja se izdvaja;

- c. ukupnu izloženost društva (i/ili grupe, ako je primjenjivo) prema istom pružatelju usluga računalstva u oblaku i potencijalni kumulativni učinak sporazuma o izdvajanju poslova u istom području poslovanja;
- d. veličinu i složenost svih poslovnih područja društva na koje utječe sporazum o izdvajanju poslova računalstva u oblaku;
- e. sposobnost da se, ako je to potrebno i poželjno, predloženi sporazum o izdvajanju poslova računalstva u oblaku prenese na drugog pružatelja usluga računalstva u oblaku ili da se usluge reintegriraju („zamjenjivost“);
- f. zaštitu osobnih i neosobnih podataka te potencijalni utjecaj koji na društvo, ugovaratelje osiguranja i druge relevantne subjekte ima povreda povjerljivosti ili propust da se zajamči dostupnost i cjelovitost podataka na temelju, između ostalog, Uredbe (EU) 2016/679<sup>7</sup>. Društvo bi osobito trebalo uzeti u obzir podatke koji predstavljaju poslovnu tajnu i/ili osjetljive podatke (primjerice, podatke o zdravstvenom stanju ugovaratelja osiguranja).

### **Smjernica 8. – Procjena rizika u pogledu izdvajanja poslova računalstva u oblaku**

- 30. Općenito govoreći, društvo bi trebalo usvojiti pristup razmjernan prirodi, opsegu i složenosti rizika svojstvenih uslugama izdvojenih pružateljima usluga računalstva u oblaku. To uključuje procjenu potencijalnog utjecaja bilo kakvog izdvajanja poslova računalstva u oblaku, osobito na njihove operativne i reputacijske rizike.
- 31. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružateljima usluga računalstva u oblaku, društvo bi trebalo učiniti sljedeće:
  - a. uzeti u obzir očekivane koristi i troškove predloženog sporazuma o izdvajanju poslova računalstva u oblaku te prosuditi sve važne rizike koji se mogu smanjiti ili kojima se može bolje upravljati u odnosu na sve važne rizike koji mogu nastati uslijed predloženog sporazuma o izdvajanju poslova računalstva u oblaku;
  - b. ako je primjenjivo i prikladno, procijeniti rizike, uključujući pravne rizike, rizike informacijsko-komunikacijske tehnologije, rizike u pogledu usklađenosti i reputacijske rizike te ograničenja u pogledu nadzora koji proizlaze iz:
    - i. odabrane usluge računalstva u oblaku i predloženih implementacijskih modela (tj. javni/privatni/hibridni/zajednički),
    - ii. migracije i/ili provedbe,
    - iii. djelatnosti i povezanih podataka i sustava za koje se razmatra mogućnost izdvajanja (ili koji su već izdvojeni) te njihove osjetljivosti i potrebnih mjera sigurnosti,
    - iv. političke stabilnosti i sigurnosnog stanja u zemljama (unutar ili izvan EU-a) u kojima se izdvojene usluge pružaju ili se mogu pružati te u kojima se podatci pohranjuju ili će se vjerojatno pohranjivati. Procjenom bi se trebali uzeti u obzir:
      - 1. zakoni koji su na snazi, uključujući zakone o zaštiti podataka;
      - 2. odredbe o provođenju zakona koje su na snazi;

---

<sup>7</sup> Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

3. odredbe stečajnog zakona koje bi se primjenjivale u slučaju propasti pružatelja usluga te sva ograničenja do kojih bi došlo s obzirom na hitan oporavak podataka društva;
  - v. podizdvajanja poslova te dodatnih rizika do kojih može doći ako se podizvođač nalazi u trećoj zemlji ili u zemlji različitoj od one u kojoj se nalazi pružatelj usluga računalstva u oblaku te iz rizika povezanog s činjenicom da dug i složen lanac podizdvajanja smanjuje sposobnost društva da nadzire svoje ključne ili važne poslovne funkcije odnosno djelatnosti te sposobnost nadzornih tijela da ih na učinkovit način nadziru;
  - vi. ukupnog rizika koncentracije društva prema istom pružatelju usluga računalstva u oblaku uključujući izdvajanje pružatelju usluga računalstva u oblaku koji nije lako zamjenjiv ili veći broj sporazuma o izdvajanju poslova s istim pružateljem usluga računalstva u oblaku. Pri procjeni rizika koncentracije društvo (i/ili grupa, ako je primjenjivo) bi trebalo uzeti u obzir sve sporazume o izdvajanju poslova s tim istim pružateljem usluga računalstva u oblaku.
32. Procjenu rizika potrebno je obaviti prije zaključivanja sporazuma o izdvajanju poslova računalstva u oblaku. Ako društvo primijeti znatne nedostatke i/ili znatne promjene u pogledu pružanih usluga ili situacije u kojoj se nalazi pružatelj usluga računalstva u oblaku, potrebno je što prije preispitati postojeću procjenu rizika ili provesti novu procjenu rizika. U slučaju obnove sporazuma o izdvajanju poslova računalstva u oblaku u pogledu njegovih sadržaja i područja primjene (primjerice, proširenje područja primjene ili uključivanje u područje primjene ključnih ili važnih poslovnih funkcija koje to ranije nisu bile), procjenu rizika potrebno je ponovno provesti.

### **Smjernica 9. – Dubinska analiza pružatelja usluga računalstva u oblaku**

33. Društvo bi u okviru postupka odabira i procjene trebalo zajamčiti da pružatelj usluga računalstva u oblaku zadovoljava kriterije propisane njegovim pisanim pravilima o izdvajanju.
34. Dubinsku analizu pružatelja usluga računalstva u oblaku potrebno je obaviti prije izdvajanja bilo kojih poslovnih funkcija ili djelatnosti. U slučaju da društvo sklapa drugi ugovor s pružateljem usluga računalstva u oblaku za kojega je već obavio procjenu, društvo bi trebalo utvrditi s pomoću pristupa utemeljenog na riziku je li potrebna druga dubinska analiza. Ako društvo primijeti znatne nedostatke i/ili znatne promjene u pogledu pružanih usluga ili situacije u kojoj se nalazi pružatelj usluga računalstva u oblaku, potrebno je što prije preispitati postojeću dubinsku analizu ili provesti novu dubinsku analizu.
35. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija pružatelju usluga računalstva u oblaku dubinska bi analiza trebala uključivati ocjenu primjerenosti pružatelja usluga računalstva u oblaku (primjerice, u pogledu vještina, infrastrukture, ekonomskog položaja, korporativnog i regulatornog statusa). Ako je primjenjivo, društvo se može koristiti dokazima, certifikatima na temelju međunarodnih standarda, revizorskim izvješćima priznatih trećih strana te izvješćima o unutarnjoj reviziji kako bi potkrijepilo obavljenu dubinsku analizu.

### **Smjernica 10. – Ugovorni zahtjevi**

36. Prava i obveze društva i pružatelja usluga računalstva u oblaku trebali bi biti jasno raspodijeljeni i utvrđeni pisanim ugovorom.

37. Ne dovodeći u pitanje zahtjeve propisane člankom 274. Delegirane uredbe, u slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku, pisanim ugovorom između društva i pružatelja usluga računalstva u oblaku trebalo bi biti propisano sljedeće:
- a. jasan opis izdvojene funkcije koja će se pružati (usluge računalstva u oblaku uključujući vrstu usluga podrške);
  - b. datum početka i datum završetka ugovora, ako je primjenjivo, te otkazne rokove za pružatelja usluga računalstva u oblaku i za društvo;
  - c. nadležni sud i mjerodavno pravo za ugovor;
  - d. financijske obveze ugovornih strana;
  - e. je li podizdvajanje ključne ili važne poslovne funkcije odnosno djelatnosti (ili njihovih bitnih dijelova) dopušteno te, ako jest, uvjeti kojima podliježe podizdvajanje znatnog opsega (vidjeti smjernicu 13.);
  - f. lokacija (lokacije) (npr. regije ili zemlje) na kojima će se relevantni podatci pohranjivati i obrađivati (lokacija podatkovnih centara) te uvjeti koje je potrebno ispuniti, uključujući zahtjev za obavješćivanje društva u slučaju da pružatelj usluga predloži promjenu lokacije (lokacija);
  - g. odredbe u pogledu pristupačnosti, dostupnosti, cjelovitosti, povjerljivosti, privatnosti i sigurnosti relevantnih podataka, uzimajući u obzir specifikacije smjernice 12.;
  - h. pravo društva da redovno prati uspješnost pružatelja usluga računalstva u oblaku;
  - i. dogovorene razine usluge, što bi trebalo uključivati precizne kvantitativne i kvalitativne ciljeve u pogledu uspješnosti kako bi se omogućilo pravodobno praćenje te time i poduzimanje odgovarajućih korektivnih mjera bez nepotrebnog odgađanja ako se dogovorene razine usluge ne postignu;
  - j. obveze izvješćivanja pružatelja usluga računalstva u oblaku u odnosu na društvo, uključujući, prema potrebi, obveze podnošenja izvješća koja su važna za sigurnosne funkcije i ključne funkcije društva, kao što su izvješća o unutarnjoj reviziji pružatelja usluga računalstva u oblaku;
  - k. treba li pružatelj usluga računalstva u oblaku ugovoriti obvezno osiguranje od određenih rizika te, ako je primjenjivo, razinu pokriva osiguranja koja se traži;
  - l. zahtjeve u pogledu provedbe i testiranja poslovnih planova za slučaj nepredviđenih okolnosti;
  - m. zahtjev da pružatelj usluga računalstva u oblaku društvu, njegovim nadzornim tijelima i svim drugim osobama koje imenuje društvo ili nadzorno tijelo mora dati sljedeće:
    - i. neograničen pristup svim relevantnim poslovnim prostorima (glavnim uredima i operativnim centrima), uključujući pristup cijelom nizu relevantnih uređaja, sustava, mreža, informacija i podataka koji se upotrebljavaju za pružanje izdvojene funkcije, te svim povezanim financijskim informacijama, osoblju i vanjskim revizorima pružatelja usluga računalstva u oblaku („pravo na pristup”);
    - ii. neograničena prava inspekcije i revizije u vezi sa sporazumom o izdvajanju poslova („pravo na reviziju”) računalstva u oblaku kako bi im se omogućilo da prate sporazum o izdvajanju poslova i zajamče

usklađenost sa svim primjenjivim regulatornim i ugovornim zahtjevima;

- n. odredbe kojima se osigurava da društvo može što prije doći do podataka koji se nalaze u njegovu vlasništvu u slučaju insolventnosti, sanacije ili prestanka poslovnih djelatnosti pružatelja usluga računalstva u oblaku.

### **Smjernica 11. – Pravo na pristup i reviziju**

38. Ugovorom o izdvajanju poslova računalstva u oblaku ne bi se trebalo ograničiti učinkovito ostvarivanje prava društva na pristup i reviziju kao ni mogućnosti kontrole usluga računalstva u oblaku u svrhu ispunjavanja njegovih regulatornih obveza.
39. Društvo bi trebalo ostvarivati svoja prava na pristup i reviziju, odrediti učestalost revizije te područja i usluge za koje je potrebno provesti reviziju služeći se pristupom utemeljenim na riziku u skladu s Odjeljkom 8. EIOPA-inih Smjernica o sustavu upravljanja.
40. Pri određivanju učestalosti i opsega ostvarivanja prava na pristup i reviziju društvo bi trebalo razmotriti je li izdvajanje poslova računalstva u oblaku povezano s ključnom ili važnom poslovnom funkcijom ili djelatnošću, prirodu i opseg rizika te utjecaj sporazuma o izdvajanju poslova računalstva u oblaku na društvo.
41. Ako ostvarivanje prava na pristup ili reviziju ili upotreba određenih tehnika revizije dovodi do nastanka rizika za okolinu pružatelja usluga računalstva u oblaku i/ili nekog drugog klijenta pružatelja usluga računalstva u oblaku (primjerice, utjecaj na razinu usluge, dostupnost podataka, aspekte povjerljivosti), društvo i pružatelj usluga računalstva u oblaku trebali bi postići dogovor u pogledu alternativnih načina na koje se može postići slična razina sigurnosti i usluge za društvo (primjerice, uključivanje posebnih kontrola koje je potrebno testirati u okviru posebnog izvješća/certifikata koje/koji podnosi pružatelj usluga računalstva u oblaku).
42. Ne dovodeći u pitanje njihovu konačnu odgovornost u pogledu aktivnosti koje obavljaju njihovi pružatelji usluga računalstva u oblaku, a kako bi se resursima revizije učinkovitije koristili te smanjili organizacijski teret koji snose pružatelj usluga računalstva u oblaku i njegovi kupci, društva se mogu koristiti:
- a. certifikatima trećih strana i revizorskim izvješćima trećih strana ili izvješćima o unutarnjoj reviziji koja je pružatelj usluga računalstva u oblaku stavio na raspolaganje;
  - b. skupnim revizijama (tj. revizijama koje se provode zajednički s drugim klijentima istog pružatelja usluga računalstva u oblaku) ili skupnim revizijama treće strane koju su oni imenovali.
43. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku, društva se mogu koristiti metodom navedenom u stavku 42. točki (a) samo:
- a. ako osiguraju da obuhvat certifikata ili revizorskog izvješća uključuje sustave (primjerice, postupke, aplikacije, infrastrukturu, podatkovne centre itd.) i kontrole koje je društvo utvrdilo te procjenjuje usklađenost s relevantnim regulatornim zahtjevima;
  - b. ako detaljno i redovno ocjenjuju sadržaj novih certifikata ili revizorskih izvješća te provjeravaju da certifikati ili izvješća nisu zastarjeli;
  - c. ako osiguraju da su ključni sustavi i kontrole obuhvaćeni budućim inačicama certifikata ili revizorskih izvješća;

- d. ako su zadovoljna osposobljenostu subjekta koji obavlja certifikaciju ili reviziju (primjerice, u pogledu rotacije društva za certifikaciju ili reviziju, kvalifikacija, stručnosti, ponovnog izvođenja / provjere dokaza u temeljnom revizijskom spisu);
  - e. ako su se uvjerila da se certifikati izdaju i da se revizije provode u skladu s odgovarajućim standardima te da uključuju testiranje operativne učinkovitosti postojećih ključnih kontrola;
  - f. ako imaju ugovorno pravo zatražiti proširenje opsega certifikata ili revizorskih izvješća na druge relevantne sustave i kontrole; broj i učestalost takvih zahtjeva za proširenje opsega trebali bi biti razumni i opravdani sa stajališta upravljanja rizicima;
  - g. ako zadrže ugovorno pravo da prema vlastitom nahođenju provode zasebne neposredne revizije u pogledu izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku; takvo bi se pravo trebalo iskoristiti u posebnim slučajevima kada takvu potrebu nije moguće zadovoljiti putem drugih vrsta interakcije s pružateljem usluga računalstva u oblaku.
44. Kad je riječ o izdvajanju ključnih ili važnih poslovnih funkcija pružateljima usluga računalstva u oblaku, društvo bi trebalo procijeniti jesu li certifikati i izvješća trećih strana, kako se navodi u stavku 42. točki (a), prikladni i dostatni za ispunjavanje njegovih regulatornih obveza te se u skladu s pristupom utemeljenom na riziku ne bi trebalo dugoročno oslanjati samo na ta izvješća i certifikate.
45. Prije planiranog neposrednog posjeta subjekt koji namjerava ostvariti svoje pravo na pristup (društvo, revizor ili treća strana koja djeluje u ime društva/društava) trebao bi o tome poslati prethodnu obavijest u razumnom roku osim ako prethodnu obavijest nije moguće poslati unaprijed zbog izvanredne ili krizne situacije. Takva bi obavijest trebala sadržavati informacije o lokaciji i svrsi posjeta te o osoblju koje će u posjetu sudjelovati.
46. S obzirom na to da su rješenja o izdvajanju poslova računalstva u oblaku tehnički vrlo složena, društvo treba provjeriti imaju li zaposlenici koji provode reviziju – bez obzira na to je li riječ o njegovim unutarnjim revizorima ili skupini revizora koji djeluju u ime društva ili imenovanim revizorima pružatelja usluga računalstva u oblaku – ili, kad je to prikladno, osoblje koje pregledava certifikaciju koju provodi treća strana ili revizorska izvješća pružatelja usluga, primjerene vještine i znanja potrebna za relevantne revizije i/ili procjene.

## **Smjernica 12. – Sigurnost podataka i sustava**

47. Društvo bi trebalo zajamčiti da se pružatelji usluga računalstva u oblaku pridržavaju europskih i nacionalnih propisa te odgovarajućih sigurnosnih standarda iz područja informacijske i komunikacijske tehnologije.
48. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružateljima usluga računalstva u oblaku društvo bi u ugovor o izdvajanju poslova trebalo unijeti dodatne posebne zahtjeve u pogledu informacijske sigurnosti te redovno pratiti usklađenost s tim zahtjevima.
49. U smislu stavka 48., u slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružateljima usluga računalstva u oblaku, primjenjujući pristup utemeljen na riziku i uzimajući u obzir svoje odgovornosti te odgovornosti pružatelja usluga računalstva u oblaku, društvo bi trebalo:
- a. postići dogovor o jasnoj podjeli uloga i odgovornosti između pružatelja usluga računalstva u oblaku i društva u pogledu poslovnih funkcija ili djelatnosti koje

podliježu izdvajanju poslova računalstva u oblaku, na način da one budu jasno razdvojene;

- b. definirati i donijeti odluku o primjerenosti razini zaštite povjerljivih podataka, kontinuitetu izdvojenih djelatnosti, cjelovitosti i sljedivosti podataka i sustava u kontekstu planiranog izdvajanja poslova računalstva u oblaku;
- c. ondje gdje je to potrebno, razmotriti konkretne mjere za podatke u prijenosu, podatke u memoriji i neaktivne podatke, kao što je upotreba tehnologija enkripcije zajedno s odgovarajućim sustavom upravljanja ključevima;
- d. razmotriti mehanizme integriranja usluga računalstva u oblaku i sustava društva, primjerice aplikacijskih programskih sučelja te pouzdanog postupka upravljanja korisnicima i pristupom;
- e. zajamčiti na temelju ugovora da dostupnost i očekivani kapacitet mrežnog prometa zadovoljavaju zahtjeve u pogledu kontinuiteta ako je to primjenjivo i izvedivo;
- f. definirati prikladne zahtjeve u pogledu kontinuiteta poslovanja i donijeti odluku o njima, pritom osiguravajući odgovarajuću razinu kontinuiteta na svakoj razini tehnološkog lanca ako je primjenjivo;
- g. imati pouzdan i dobro dokumentiran postupak upravljanja incidentima s dodijeljenim odgovornostima, primjerice definiranjem modela suradnje u slučaju da dođe do stvarnih incidenata ili do sumnje na pojavu incidenta;
- h. usvojiti pristup utemeljen na riziku u pogledu lokacije (lokacija) pohrane i obrade podataka (tj. zemlje ili regije) te pitanja u vezi s informacijskom sigurnosti;
- i. pratiti ispunjavanje zahtjeva u vezi s učinkovitošću i djelotvornošću mehanizama kontrole koje provodi pružatelj usluga računalstva u oblaku, a kojima se ublažavaju rizici povezani s uslugama koje se pružaju.

### **Smjernica 13. – Podizdvajanje ključnih ili važnih poslovnih funkcija odnosno djelatnosti**

50. Ako je podizdvajanje ključnih ili važnih poslovnih funkcija (ili njihovih dijelova) dopušteno, u ugovoru o izdvajanju poslova između društva i pružatelja usluga računalstva u oblaku trebalo bi:
- a. navesti sve vrste djelatnosti koje su isključene iz potencijalnog podizdvajanja;
  - b. navesti uvjete koje je potrebno ispuniti u slučaju podizdvajanja (primjerice, uvjet da će podizvođač također u potpunosti ispunjavati relevantne obveze pružatelja usluga računalstva u oblaku). Te obveze podrazumijevaju pravo na reviziju i pristup te sigurnost podataka i sustava;
  - c. navesti da pružatelj usluga računalstva u oblaku zadržava punu odgovornost za podizdvojene usluge te nadzor nad njima;
  - d. uključiti odredbu o obvezi pružatelja usluga računalstva u oblaku u pogledu obavješćivanja društva o svim planiranim značajnim promjenama u pogledu podizvođača ili podizdvojenih usluga povezanih s podizdvajanjem koje bi mogle utjecati na sposobnost pružatelja usluga da ispuni svoje obveze u skladu s ugovorom o podizdvajanju poslova računalstva u oblaku. Rok za slanje obavijesti o takvim promjenama trebao bi biti takav da društvo barem može provesti procjenu rizika s obzirom na utjecaj predloženih promjena prije nego što takve promjene u pogledu podizvođača ili podizdvojenih usluga zaista stupe na snagu;

- e. u slučajevima kada pružatelj usluga računalstva u oblaku planira promjene u pogledu podizvođača ili podizdvojenih usluga koje će imati negativan utjecaj na procjenu rizika dogovorenih usluga, zajamčiti da društvo ima pravo prigovora na takve izmjene i/ili pravo raskida i otkazivanja ugovora.

#### **Smjernica 14. – Praćenje i nadzor sporazuma o izdvajanju poslova računalstva u oblaku**

51. Društvo bi trebalo redovno pratiti svoje pružatelje usluga računalstva u oblaku, njihovo obavljanje djelatnosti, mjere sigurnosti i pridržavanje dogovorene razine usluge služeći se pristupom utemeljenim na riziku. Najveći bi se naglasak trebao staviti na izdvajanje ključnih i važnih poslovnih funkcija pružateljima usluga računalstva u oblaku.
52. Kako bi se to moglo učiniti, društvo bi trebalo uspostaviti mehanizme praćenja i nadzora, koji bi trebali biti usmjereni na prisutnost podizdvajanja ključnih ili važnih poslovnih funkcija ili njihovih dijelova, ako je to izvedivo i primjereno.
53. Upravno, upravljačko ili nadzorno tijelo potrebno je redovito obavještavati o utvrđenim rizicima u vezi s izdvajanjem ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku.
54. Kako bi zajamčila prikladno praćenje i nadzor svojih sporazuma o izdvajanju poslova računalstva u oblaku, društva bi trebala zaposliti dovoljan broj osoblja s prikladnim vještinama i znanjem za potrebe praćenja usluga koje se izdvajaju. Osoblje društva zaduženo za takve aktivnosti trebalo bi prema potrebi imati znanja iz područja informacijskih i komunikacijskih tehnologija te poslovanja.

#### **Smjernica 15. – Prava u pogledu raskida i izlazne strategije**

55. U slučaju izdvajanja ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku, društvo bi trebalo zajamčiti da ugovor o izdvajanju poslova sadržava klauzulu s jasno definiranom izlaznom strategijom koja društvu osigurava mogućnost raskida sporazuma ako je to potrebno. Mogućnost raskida trebala bi biti dostupna bez ugrožavanja kontinuiteta i kvalitete pružanja usluga društva ugovarateljima osiguranja. Kako bi se to postiglo, društvo bi trebalo:
- izraditi izlazne planove koji su sveobuhvatni, utemeljeni na uslugama, dokumentirani i dostatno testirani (primjerice, na način da se provede analiza potencijalnih implikacija različitih potencijalnih izlaznih opcija u pogledu troškova, utjecaja, resursa i potrebnog vremena);
  - utvrditi alternativna rješenja i razviti prikladne i izvedive prijelazne planove kako bi se društvu omogućilo uklanjanje postojećih djelatnosti i podataka te njihov prijenos s postojećeg pružatelja usluga računalstva u oblaku na alternativnog pružatelja usluga ili na samo društvo. Ta bi rješenja trebala definirati u pogledu izazova do kojih može doći zbog lokacije podataka, pritom poduzimajući potrebne mjere kako bi se zajamčio kontinuitet poslovanja tijekom prijelazne faze;
  - zajamčiti da pružatelj usluga računalstva u oblaku na prikladan način pruža podršku društvu pri prenošenju izdvojenih podataka, sustava ili aplikacija na drugog pružatelja usluga ili izravno na društvo;
  - postići dogovor s pružateljem usluga računalstva u oblaku da će, nakon što podatci budu ponovno preneseni na društvo, pružatelj usluga računalstva u oblaku sve te podatke na siguran način obrisati u svim regijama.



56. Pri izradi izlaznih strategija društvo treba učiniti sljedeće:
- definirati ciljeve izlazne strategije;
  - definirati događaje (primjerice, ključne pokazatelje rizika koji upućuju na neprihvatljivu razinu usluge) koji bi mogli pokrenuti izlaznu strategiju;
  - provesti analizu učinka na poslovanje proporcionalnu izdvojenim djelatnostima kako bi se utvrdilo koliko bi ljudskih i drugih resursa bilo potrebno za provedbu izlaznog plana i koliko bi to trajalo;
  - dodijeliti uloge i odgovornosti za upravljanje izlaznim planovima i prijelaznim aktivnostima;
  - definirati kriterije uspjeha prijelazne faze.

### **Smjernica 16. – Nadzor sporazuma o izdvajanju poslova računalstva u oblaku koji provode nadzorna tijela**

57. Nadzorna bi tijela trebala provoditi analizu utjecaja koji proizlaze iz sporazuma društva o izdvajanju poslova računalstva u oblaku u okviru svojih postupaka nadzornog pregleda. Analiza utjecaja trebala bi osobito biti usmjerena na sporazume povezane s izdvajanjem ključnih ili važnih poslovnih funkcija odnosno djelatnosti.
58. Nadzorna bi tijela trebala razmotriti sljedeće rizike pri obavljanju nadzora sporazuma o izdvajanju poslova računalstva u oblaku:
- rizike informacijske i komunikacijske tehnologije;
  - druge operativne rizike (uključujući pravni rizik i rizik u pogledu usklađenosti te rizik u pogledu izdvajanja poslova i upravljanja trećim stranama);
  - reputacijski rizik;
  - rizik koncentracije na razini zemlje i sektora.
59. Nadzorna bi tijela u svoju procjenu trebala uključiti sljedeće aspekte služeći se pristupom utemeljenim na riziku:
- prikladnost i učinkovitost postupaka upravljanja i poslovanja društva povezanih s odobrenjem, provedbom, praćenjem, upravljanjem i obnovom sporazuma o izdvajanju poslova računalstva u oblaku;
  - raspoloža li društvo dovoljnim brojem osoblja s prikladnim vještinama i znanjem za potrebe praćenja izdvojenih usluga računalstva u oblaku;
  - je li društvo utvrdilo sve rizike koji su posebno naglašeni u ovim smjernicama te upravlja li tim rizicima.
60. U slučaju grupa, nadzornik grupe trebao bi zajamčiti da nadzorna procjena rizika grupe odražava utjecaje izdvajanja ključnih ili važnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku, pritom uzimajući u obzir zahtjeve navedene u stavku 58. i 59. te pojedinačne značajke upravljanja i poslovanja grupe.
61. Ako izdvajanje ključnih ili važnih poslovnih funkcija odnosno djelatnosti pružatelju usluga računalstva u oblaku uključuje više društava u različitim državama članicama te ako njime centralizirano upravlja matično društvo ili određeno društvo kći grupe (primjerice, jedno od društava kćeri ili pak poduzeće koje pripada grupi, a koje pruža određene usluge, primjerice pružatelj usluga informacijskih i komunikacijskih tehnologija), nadzornik grupe i/ili relevantna nadzorna tijela društava uključenih u izdvajanje poslova računalstva u oblaku trebali bi raspraviti, ako je to primjenjivo, o utjecajima izdvajanja poslova računalstva u oblaku na profil rizičnosti grupe u okviru kolegija nadzornika.

62. Ako se utvrde razlozi za zabrinutost iz kojih se može zaključiti da određeno društvo više ne raspolaže pouzdanim sustavima upravljanja ili nije usklađeno s regulatornim zahtjevima, nadležna bi tijela trebala poduzeti odgovarajuće mjere koje mogu uključivati, primjerice, zahtjev da društvo unaprijedi sustav upravljanja, ograničavanje obujma izdvojenih funkcija ili zahtjev za otkazivanje jednog sporazuma o izdvajanju poslova ili više njih. Konkretno, uzimajući u obzir potrebu da se zajamči kontinuirano poslovanje društva, može se zatražiti raskid ugovora ako se nadzor i ispunjenje regulatornih zahtjeva ne mogu osigurati drugim mjerama.

### **Pravila o usklađenosti i izvješćivanju**

63. Ovaj dokument sadržava smjernice izdane u skladu s člankom 16. Uredbe (EU) br. 1094/2010. U skladu s člankom 16. stavkom 3. spomenute Uredbe, nadležna tijela i financijske institucije moraju uložiti sve napore kako bi poštovali navedene smjernice i preporuke.
64. Nadležna tijela koja su usklađena ili se namjeravaju uskladiti s ovim smjernicama trebaju ih na primjeren način uvrstiti u svoj regulatorni ili nadzorni okvir.
65. Nadležna tijela trebaju potvrditi EIOPA-i jesu li usklađena s ovim smjernicama ili se namjeravaju s njima uskladiti te navesti razloge za neusklađenost u roku od dva mjeseca nakon izdavanja prevedenih verzija.
66. U slučaju da nadležna tijela ne odgovore u navedenom roku, smatrat će se da nisu usklađena s pravilima izvješćivanja te će kao takva biti prijavljena.

### **Završna odredba o pregledu**

67. Ove Preporuke podliježu EIOPA-inu pregledu.