

Smernice o oddajanju v zunanje izvajanje ponudnikom storitev v oblaku

Kazalo

Uvod.....	3
Opredelitve pojmov	3
Datum začetka uporabe	4
Smernica 1 – Storitve v oblaku in zunanje izvajanje	5
Smernica 2 – Splošna načela upravljanja za zunanje izvajanje storitev v oblaku.....	5
Smernica 3 – Posodobitev pisne politike za oddajo storitev v zunanje izvajanje	5
Smernica 4 – Pisno obvestilo nadzornemu organu	6
Smernica 5 – Zahteve glede dokumentacije.....	7
Smernica 6 – Analiza pred oddajo storitev v zunanje izvajanje	7
Smernica 7 – Ocena ključnih ali pomembnih operativnih funkcij in dejavnosti	8
Smernica 8 – Ocena tveganja zunanjega izvajanja storitev v oblaku	9
Smernica 9 – Skrbni pregled ponudnika storitev v oblaku	10
Smernica 10 – Pogodbene zahteve	10
Smernica 11 – Pravici do dostopa in revizije	11
Smernica 12 – Varnost podatkov in sistemov	13
Smernica 13 – Zunanje podizvajanje ključnih ali pomembnih operativnih funkcij ali dejavnosti	14
Smernica 14 – Spremljanje in nadzorovanje dogovorov o zunanjem izvajanju storitev v oblaku	14
Smernica 15 – Pravica do odpovedi pogodbe in strategije izstopa	15
Smernica 16 – Nadzor dogovorov o zunanjem izvajanju storitev v oblaku, ki ga izvajajo nadzorni organi	15
Pravila glede skladnosti in poročanja.....	16
Končna določba glede pregleda	16

Uvod

1. V skladu s členom 16 Uredbe (EU) št. 1094/2010¹ organ EIOPA izdaja smernice, s katerimi zavarovalnicam in pozavarovalnicam zagotavlja navodila, kako je treba uporabljati določbe o zunanjem izvajanju iz Direktive 2009/138/ES² (v nadaljnjem besedilu: direktiva Solventnost II) in Delegirane uredbe Komisije (EU) št. 2015/35³ (v nadaljnjem besedilu: delegirana uredba) v primeru oddajanja v zunanje izvajanje ponudnikom storitev v oblaku.
2. Te smernice temeljijo na členih 13(28), 38 in 49 direktive Solventnost II in členu 274 delegirane uredbe. Poleg tega te smernice temeljijo tudi na navodilih iz Smernic o sistemu upravljanja, ki jih je izdal organ EIOPA (EIOPA-BoS-14/253).
3. Te smernice so namenjene pristojnim organom, da bi jim zagotovile navodila, kako bi morale zavarovalnice in pozavarovalnice (v nadaljnjem besedilu skupaj: podjetja) uporabljati zahteve glede zunanjega izvajanja iz navedenih pravnih aktov v okviru oddajanja v zunanje izvajanje ponudnikom storitev v oblaku.
4. Smernice se uporabljajo za posamezna podjetja in smiselno za skupine⁴.
Subjekti, za katere veljajo druge sektorske zahteve in ki so del skupine, so izključeni s področja uporabe teh smernic na posamični ravni, saj morajo upoštevati posebne sektorske zahteve in ustrezne smernice, ki jih izdala Evropski organ za vrednostne papirje in trge ter Evropski bančni organ.
5. V primeru oddajanja v zunanje izvajanje subjektu znotraj skupine in oddajanja v zunanje podizvajanje ponudnikom storitev v oblaku je treba te smernice uporabljati skupaj z določbami o oddajanju v zunanje izvajanje subjektu znotraj skupine iz Smernic o sistemu upravljanja, ki jih je izdal organ EIOPA.
6. Podjetja in pristojni organi bi morali pri izpolnjevanju teh smernic ali nadzoru njihovega izpolnjevanja upoštevati načelo sorazmernosti⁵ ter ključni pomen ali pomembnost storitev, oddanih v zunanje izvajanje ponudnikom storitev v oblaku. Z uporabo načela sorazmernosti bi bilo treba zagotoviti, da so ureditve upravljanja, vključno s tistimi, ki se nanašajo na oddajanje v zunanje izvajanje ponudnikom storitev v oblaku, sorazmerne z naravo, obsegom in kompleksnostjo povezanih tveganj.
7. Te smernice bi bilo treba brati skupaj s Smernicami o sistemu upravljanja, ki jih je izdal organ EIOPA, in regulativnimi obveznostmi iz odstavka 1 ter brez poseganja vanje.

Opredelitve pojmov

8. Če izraz ni opredeljen v teh smernicah, je njegov pomen enak kot v pravnih aktih, navedenih v uvodu.
9. Poleg tega se v teh smernicah uporabljajo naslednje opredelitve:

¹ Uredba (EU) št. 1094/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za zavarovanja in poklicne pokojnine) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/79/ES (UL L 331, 15.12.2010, str. 48).

² Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).

³ Delegirana uredba Komisije (EU) 2015/35 z dne 10. oktobra 2014 o dopolnitvi Direktive 2009/138/ES Evropskega parlamenta in Sveta o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 12, 17.1.2015, str. 1).

⁴ Člen 212(1) direktive Solventnost II.

⁵ Člen 29(3) direktive Solventnost II.

Ponudnik storitev	pomeni subjekt tretje osebe, ki v celoti ali delno izvaja proces, storitev ali dejavnost na podlagi dogovora o zunanjem izvajanju.
Ponudnik storitev v oblaku	pomeni ponudnika storitev, kot je opredeljen zgoraj, ki je odgovoren za izvajanje storitev v oblaku v okviru dogovora o zunanjem izvajanju.
Storitve v oblaku	pomenijo storitve, ponujene prek računalništva v oblaku, tj. modela za zagotavljanje stalnega in priročnega omrežnega dostopa na zahtevo do skupnega nabora prilagodljivih računalniških virov (npr. omrežij, strežnikov, pomnilnikov, aplikacij in storitev), ki so na voljo hitro in z minimalnim trdom ali interakcijo s ponudnikom storitev.
Javni oblak	pomeni infrastrukturo v oblaku, ki jo lahko prosto uporablja splošna javnost.
Zasebni oblak	pomeni infrastrukturo v oblaku, ki jo lahko uporablja izključno eno samo podjetje.
Skupnostni oblak	pomeni infrastrukturo v oblaku, ki jo lahko uporablja izključno določena skupnost podjetij, na primer več podjetij v okviru ene skupine.
Hibridni oblak	pomeni infrastrukturo v oblaku, ki je sestavljena iz dveh ali več ločenih infrastruktur v oblaku.

Datum začetka uporabe

10. Te smernice se uporabljajo od 1. januarja 2021 za vse dogovore o zunanjem izvajanju storitev v oblaku, ki so sklenjeni ali spremenjeni na navedeni datum ali pozneje.
11. Podjetja bi morala pregledati in ustrezno spremeniti obstoječe dogovore o zunanjem izvajanju storitev v oblaku, povezane s ključnimi ali pomembnimi operativnimi funkcijami ali dejavnostmi, da bi zagotovila skladnost s temi smernicami do 31. decembra 2022.
12. Če pregled dogovorov o zunanjem izvajanju storitev v oblaku, povezanih s ključnimi ali pomembnimi operativnimi funkcijami, ne bo končan do 31. decembra 2022, bi moralo podjetje o tem obvestiti svoj pristojni organ⁶, vključno z navedbo ukrepov, načrtovanih za dokončanje pregleda, ali morebitno strategijo izstopa. Nadzorni organ se lahko, kadar je primerno, s podjetjem dogovori o podaljšanju roka za zaključek tega pregleda.
13. Posodobitev politik in notranjih postopkov podjetja (kadar je potrebna) bi morala biti dokončana do 1. januarja 2021, zahteve v zvezi z dokumentacijo dogovorov o zunanjem izvajanju storitev v oblaku, povezanih s ključnimi ali pomembnimi operativnimi funkcijami ali dejavnostmi, pa bi morale biti izpolnjene do 31. decembra 2022.

⁶ Člen 13(10) direktive Solventnost II.

Smernica 1 – Storitve v oblaku in zunanje izvajanje

14. Podjetje bi moralo ugotoviti, ali dogovor s ponudnikom storitev v oblaku spada v opredelitev zunanjega izvajanja v skladu z direktivo Solventnost II. V okviru ocene bi bilo treba upoštevati:
 - a. ali se operativna funkcija ali dejavnost (ali njen del), oddana v zunanje izvajanje, izvaja periodično ali stalno in
 - b. ali bi ta operativna funkcija ali dejavnost (ali njen del) običajno spadala v okvir operativnih funkcij ali dejavnosti, ki bi jih podjetje opravljalo ali lahko opravljalo v okviru svojih rednih poslovnih dejavnosti, tudi če v preteklosti ni izvajalo te operativne funkcije ali dejavnosti.
15. Če dogovor s ponudnikom storitev zajema več operativnih funkcij ali dejavnosti, bi moralo podjetje v svoji oceni upoštevati vse vidike dogovora.
16. Kadar podjetje odda operativne funkcije ali dejavnosti v zunanje izvajanje ponudnikom storitev, ki niso ponudniki storitev v oblaku, vendar se za zagotavljanje svojih storitev bistveno zanašajo na infrastrukturo v oblaku (če je na primer ponudnik storitev v oblaku del verige podizvajanja), dogovor o takšnem zunanjem izvajanju spada na področje uporabe teh smernic.

Smernica 2 – Splošna načela upravljanja za zunanje izvajanje storitev v oblaku

17. Upravni, upravljalni ali nadzorni organ podjetja bi moral brez poseganja v člen 274(3) delegirane uredbe zagotoviti, da vsaka odločitev o oddaji ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku temelji na podrobni oceni tveganja, ki vključuje vsa zadevna tveganja, ki izhajajo iz dogovora, kot so informacijska in komunikacijska tehnologija (IKT), neprekinjenost poslovanja, pravna tveganja in skladnost, koncentracija, druga operativna tveganja in tveganja, povezana z migracijo podatkov in/ali fazo izvajanja, kadar je to ustrezno.
18. Podjetje bi moralo v primeru oddaje ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku, kadar je to ustrezno, v lastno oceno tveganja in solventnosti (ORSA) vključiti spremembe svojega profila tveganja, ki so posledica dogovora o zunanjem izvajanju storitev v oblaku.
19. Uporaba storitev v oblaku bi morala biti skladna s strategijami podjetja (na primer strategijo IKT, strategijo informacijske varnosti in strategijo obvladovanja operativnega tveganja) ter notranjimi politikami in postopki, ki jih je treba po potrebi posodobiti.

Smernica 3 – Posodobitev pisne politike za oddajo storitev v zunanje izvajanje

20. V primeru oddaje storitev v zunanje izvajanje ponudnikom storitev v oblaku bi moralo podjetje posodobiti pisno politiko za oddajo storitev v zunanje izvajanje (na primer jo pregledati, dodati ločen dodatek ali pripraviti nove namenske politike) in druge ustrezne notranje politike (na primer politiko informacijske varnosti), pri čemer bi moralo upoštevati posebnosti oddajanja storitev v oblaku v zunanje izvajanje vsaj glede:
 - a. vlog in odgovornosti vključenih funkcij podjetja, zlasti upravnega, upravljalnega ali nadzornega organa, ter funkcij, ki so odgovorne za IKT, informacijsko varnost, skladnost, obvladovanje tveganja in notranjo revizijo;

- b. procesov in postopkov poročanja, ki so potrebni za odobritev, izvajanje, spremljanje, upravljanje in obnovitev dogovora o zunanjem izvajanju storitev v oblaku, povezanih s ključnimi ali pomembnimi operativnimi funkcijami ali dejavnostmi, kjer je ustrezno;
- c. nadzora nad storitvami v oblaku, ki je sorazmeren z naravo, obsegom in kompleksnostjo tveganj, ki so del zagotovljenih storitev, vključno z (i) oceno tveganja dogovorov o zunanjem izvajanju storitev v oblaku in skrbnim pregledom ponudnikov storitev v oblaku, vključno s pogostostjo ocene tveganja; (ii) spremljanjem in nadzorom upravljanja (na primer preverjanjem sporazuma o ravni storitve) ter (iii) varnostnimi standardi in kontrolami;
- d. navedbe pogodbenih zahtev v zvezi z zunanjim izvajanjem ključnih ali pomembnih operativnih funkcij ali dejavnosti v oblaku, kot so opisane v smernici 10;
- e. zahtev v zvezi z dokumentacijo in pisnega obvestila nadzornemu organu o oddaji ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje v oblaku;
- f. zahteve po dokumentirani in po potrebi zadostno preskušeni strategiji izstopa, ki je sorazmerna z naravo, obsegom in kompleksnostjo tveganj, ki so del zagotovljenih storitev, v zvezi z vsakim dogovorom o zunanjem izvajanju storitev v oblaku, ki zajema ključne ali pomembne operativne funkcije ali dejavnosti. Strategija izstopa lahko vključuje vrsto postopkov za odpoved dogovora, ki med drugim vključujejo prekinitev, ponovno vključitev ali prenos storitev, vključenih v dogovor o zunanjem izvajanju storitev v oblaku.

Smernica 4 – Pisno obvestilo nadzornemu organu

- 21. Zahteve glede pisnega obveščanja, ki so določene v členu 49(3) direktive Solventnost II in podrobneje opredeljene v Smernicah o sistemu upravljanja, ki jih je izdal organ EIOPA, se uporabljajo za vse oddajanje ključnih ali pomembnih operativnih funkcij in dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku. Če operativna funkcija ali dejavnost, ki predhodno ni bila razvrščena kot ključna ali pomembna, postane ključna ali pomembna, bi morale podjetje o tem obvestiti nadzorni organ.
- 22. Pisno obvestilo podjetja bi moralo ob upoštevanju načela sorazmernosti vključevati vsaj naslednje informacije:
 - a. kratek opis operativne funkcije ali dejavnosti, ki je oddana v zunanje izvajanje;
 - b. datum začetka in, kadar je ustrezno, datum naslednje obnovitve pogodbe, datum prenehanja in/ali odpovedne roke za ponudnika storitev v oblaku in podjetje;
 - c. pravo, ki ureja pogodbo o zunanjem izvajanju storitev v oblaku;
 - d. ime ponudnika storitev v oblaku, matično številko družbe, identifikator pravnih subjektov (če je na voljo), registrirani naslov in druge pomembne podatke za stik ter ime nadrejene družbe (če obstaja) in v primeru skupin, ali je ponudnik storitev v oblaku del skupine ali ne;
 - e. model storitev v oblaku in model postavitve oblaka, (tj. javni/zasebni/hibridni/skupnostni) ter specifično naravo podatkov, ki bodo shranjeni, in lokacije (države ali regije), kjer bodo shranjeni;
 - f. kratek povzetek razlogov, zakaj se operativna funkcija ali dejavnost, oddana v zunanje izvajanje, šteje za ključno ali pomembno;

- g. datum zadnje ocene operativne funkcije ali dejavnosti, oddane v zunanje izvajanje, ki se šteje za ključno ali pomembno.

Smernica 5 – Zahteve glede dokumentacije

- 23. V okviru sistema upravljanja in obvladovanja tveganja bi morale podjetje voditi evidenco svojih dogovorov o zunanjem izvajanju storitev v oblaku, na primer v obliki namenskega registra, ki se sproti posodablja. Podjetje bi moralo tudi hraniti evidenco odpovedanih dogovorov o zunanjem izvajanju storitev v oblaku za ustrezno obdobje hrambe v skladu z nacionalno ureditvijo.
- 24. V primeru zunanjega izvajanja ključnih ali pomembnih operativnih funkcij ali dejavnosti bi morale podjetje zabeležiti vse naslednje informacije:
 - a. informacije, o katerih je treba obvestiti nadzorni organ v skladu s smernico 4;
 - b. v primeru skupin zavarovalnice ali pozavarovalnice in druga podjetja v okviru bonitetne konsolidacije, ki uporabljajo storitve v oblaku;
 - c. datum najnovejše ocene tveganja in kratek povzetek glavnih rezultatov;
 - d. posameznika ali organ odločanja (na primer upravni, upravljalni ali nadzorni organ) v podjetju, ki je odobril dogovor o zunanjem izvajanju storitev v oblaku;
 - e. datume zadnje revizije in naslednjih načrtovanih revizij, kadar je to ustrezno;
 - f. imena vseh zunanjih podizvajalcev, ki so jim bili oddani bistveni deli ključne ali pomembne operativne funkcije ali dejavnosti, vključno z državo, v kateri so ti podizvajalci registrirani, kjer bo storitev opravljena, in lokacijami (državami ali regijami), kjer bodo shranjeni podatki, kadar je to ustrezno;
 - g. rezultat ocene nadomestljivosti ponudnika storitev v oblaku (na primer lahko nadomestljiv/težko nadomestljiv/nadomestitev ni mogoča);
 - h. ali ključna ali pomembna operativna funkcija ali dejavnost, oddana v zunanje izvajanje, podpira časovno kritične poslovne operacije;
 - i. ocenjeni letni stroški;
 - j. ali ima podjetje strategijo izstopa za primer, če katera izmed strank odpove pogodbo ali če pri ponudniku storitev v oblaku pride do motenj v zagotavljanju storitev.
- 25. V primeru zunanjega izvajanja operativnih funkcij ali dejavnosti, ki niso ključne ali pomembne, bi morale podjetje opredeliti informacije, ki jih je treba zabeležiti, na podlagi narave, obsega in kompleksnosti tveganj, ki so del storitev, ki jih zagotavlja ponudnik storitev v oblaku.
- 26. Podjetje bi moralo nadzornemu organu na zahtevo dati na voljo vse informacije, ki jih ta potrebuje za izvajanje nadzora nad podjetjem, vključno z izvodom sporazuma o zunanjem izvajanju.

Smernica 6 – Analiza pred oddajo storitev v zunanje izvajanje

- 27. Podjetje bi moralo pred sklenitvijo kakršnega koli dogovora s ponudniki storitev v oblaku:
 - a. oceniti, ali dogovor o zunanjem izvajanju v oblaku zadeva ključno ali pomembno operativno funkcijo ali dejavnost v skladu s smernico 7;
 - b. opredeliti in oceniti vsa pomembna tveganja dogovora o zunanjem izvajanju storitev v oblaku v skladu s smernico 8;

- c. izvesti ustrezen skrbni pregled potencialnega ponudnika storitev v oblaku v skladu s smernico 9;
- d. opredeliti in oceniti navzkrižja interesov, ki jih zunanje izvajanje lahko povzroči, v skladu z zahtevami iz člena 274(3)(b) delegirane uredbe.

Smernica 7 – Ocena ključnih ali pomembnih operativnih funkcij in dejavnosti

- 28. Podjetje bi moralo pred sklenitvijo dogovora o zunanjem izvajanju s ponudniki storitev v oblaku oceniti, ali dogovor o zunanjem izvajanju v oblaku zadeva ključno ali pomembno operativno funkcijo ali dejavnost. Pri izvedbi te ocene bi moralo podjetje po potrebi upoštevati, ali bi lahko dogovor v prihodnosti postal ključen ali pomemben. Poleg tega bi moralo ponovno oceniti ključni pomen ali pomembnost operativne funkcije ali dejavnosti, ki je bila predhodno oddana v zunanje izvajanje ponudnikom storitev v oblaku, če se narava, obseg in kompleksnost tveganj, ki so del sporazuma, bistveno spremenijo.
- 29. Pri oceni bi moralo podjetje skupaj z rezultati ocene tveganja upoštevati vsaj naslednje dejavnike:
 - a. možni učinek morebitnih bistvenih motenj operativne funkcije ali dejavnosti, oddane v zunanje izvajanje, ali nezmožnosti ponudnika storitev v oblaku, da storitve zagotovi na dogovorjenih ravneh storitev, na:
 - i. neprekinjeno izpolnjevanje regulativnih obveznosti podjetja;
 - ii. kratkoročno in dolgoročno finančno in plačilno sposobnost ter sposobnost preživetja podjetja;
 - iii. neprekinjeno poslovanje in operativno odpornost;
 - iv. operativno tveganje, vključno z ravnanjem, IKT ter pravnimi tveganji;
 - v. tveganje izgube poslovnega ugleda;
 - b. možni učinek dogovora o zunanjem izvajanju storitev v oblaku na sposobnost podjetja, da:
 - i. odkriva, spremlja in obvladuje vsa zadevna tveganja;
 - ii. ravna v skladu z vsemi pravnimi in regulativnimi zahtevami;
 - iii. izvaja ustrezne revizije operativne funkcije ali dejavnosti, ki je oddana v zunanje izvajanje;
 - c. seštevek izpostavljenosti podjetja (in/ali skupine, kjer je ustrezno) istemu ponudniku storitev v oblaku in možni kumulativni učinek dogovorov o zunanjem izvajanju na istem poslovnem področju;
 - d. velikost in kompleksnost vseh poslovnih področij podjetja, na katera vpliva dogovor o zunanjem izvajanju storitev v oblaku;
 - e. zmožnost, če je potrebna ali zaželeno, da se predlagani dogovor o zunanjem izvajanju storitev v oblaku prenese na drugega ponudnika storitev v oblaku ali ponovno vključijo storitve (zamenljivost);
 - f. varstvo osebnih in neosebnih podatkov ter morebitni vpliv na podjetje, imetnike polic ali druge zadevne posameznike, na katere bi vplivala kršitev zaupnosti ali nezagotovitev razpoložljivosti in celovitosti podatkov, med drugim na podlagi

Uredbe (EU) št. 2016/679⁷. Podjetje bi moralo zlasti upoštevati podatke, ki so poslovna skrivnost in/ali občutljivi (npr. podatki o zdravju imetnikov polic).

Smernica 8 – Ocena tveganja zunanjega izvajanja storitev v oblaku

30. Na splošno bi moralo podjetje sprejeti pristop, ki je sorazmeren z naravo, obsegom in kompleksnostjo tveganj, ki so del storitev, oddanih zunanjim izvajalcem storitev v oblaku. To vključuje oceno potencialnega učinka vsakega zunanjega izvajanja storitev v oblaku, zlasti na operativno tveganje in tveganje izgube ugleda podjetja.
31. V primeru oddaje ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku bi moralo podjetje:
- a. upoštevati pričakovane koristi in stroške predlaganega dogovora o zunanjem izvajanju storitev v oblaku, pri čemer je treba pretehtati vsa bistvena tveganja, ki bi se lahko zaradi predlaganega dogovora o zunanjem izvajanju storitev v oblaku zmanjšala ali bolje obvladovala, skupaj z vsemi bistvenimi tveganji, ki bi lahko zaradi tega dogovora nastala;
 - b. kjer je ustrezno in primerno, oceniti tveganja, vključno s pravnimi tveganji, tveganji glede IKT, skladnosti in izgube ugleda, ter omejitve pri nadzoru, ki izhajajo iz:
 - i. izbranega modela storitve v oblaku in predlaganega modela postavitve oblaka (tj. javni/zasebni/hibridni/skupnostni oblak);
 - ii. migracij in/ali izvajanja;
 - iii. dejavnosti in povezanih podatkov in sistemov, ki bi se lahko oddali v zunanje izvajanje (ali so bili oddani v zunanje izvajanje), ob upoštevanju njihove občutljivosti in zahtevanih varnostnih ukrepov;
 - iv. politične stabilnosti in varnostnih razmer v državah (v EU ali zunaj nje), v katerih se zagotavljajo ali bi se lahko zagotavljale storitve, oddane v zunanje izvajanje, in v katerih se hranijo ali bi se verjetno hranili podatki. Pri oceni bi bilo treba upoštevati:
 1. veljavne zakone, vključno z zakoni o varstvu podatkov;
 2. veljavne določbe glede izvrševanja zakonodaje;
 3. določbe insolvenčnega prava, ki bi se lahko uporabljale v primeru propada ponudnika storitev, in vse morebitne omejitve, ki bi se pojavile v zvezi z nujnim ponovnim prevzemom podatkov podjetja;
 - v. zunanje podizvajanje, vključno z dodatnimi tveganji, ki se lahko pojavijo, če se zunanji podizvajalec nahaja v tretji državi ali drugi državi kot ponudnik storitev v oblaku, ter tveganjem, da se z dolgimi in zapletenimi verigami podizvajalcev zmanjša zmožnost podjetja, da nadzoruje svoje ključne ali pomembne operativne funkcije ali dejavnosti, in zmožnost nadzornih organov, da jih učinkovito nadzorujejo;
 - vi. skupno tveganje koncentracije podjetij na istega ponudnika storitev v oblaku, vključno z oddajanjem storitev v zunanje izvajanje ponudniku storitev v oblaku, ki ni lahko nadomestljiv, ali več

⁷ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

dogovori o zunanjem izvajanju z istim ponudnikom storitev v oblaku. Pri ocenjevanju tveganja koncentracije bi morale podjetje (in/ali skupina, kjer je ustrezno) upoštevati vse svoje dogovore o zunanjem izvajanju storitev v oblaku z zadevnim izvajalcem storitev v oblaku.

32. Pred sklenitvijo dogovora o zunanjem izvajanju storitev v oblaku bi bilo treba opraviti oceno tveganja. Če podjetje izve za znatne pomanjkljivosti in/ali znatne spremembe zagotovljenih storitev ali položaja ponudnika storitev v oblaku, bi morale nemudoma pregledati ali ponovno izvesti oceno tveganja. V primeru obnovitve dogovora o zunanjem izvajanju storitev v oblaku, pri katerem sta spremenjena njegova vsebina in področje uporabe (na primer razširitev področja uporabe ali vključitev ključnih ali pomembnih operativnih funkcij, ki prej niso bile vključene), je treba ponovno oceniti tveganje.

Smernica 9 – Skrbni pregled ponudnika storitev v oblaku

33. Podjetje bi moralo v postopku izbire in ocenjevanja zagotoviti primernost ponudnika storitev v oblaku glede na merila, opredeljena v pisni politiki podjetja za oddajo storitev v zunanje izvajanje.
34. Skrbni pregled ponudnika storitev v oblaku je treba opraviti pred oddajo katere koli operativne funkcije ali dejavnosti v zunanje izvajanje. Če podjetje sklene drugi sporazum s ponudnikom storitev v oblaku, ki je že bil ocenjen, bi morale s pristopom na podlagi tveganja določiti, ali je potreben drugi skrbni pregled. Če podjetje izve za znatne pomanjkljivosti in/ali bistvene spremembe zagotovljenih storitev ali položaja ponudnika storitev v oblaku, bi morale skrbni pregled nemudoma preveriti ali ponovno izvesti.
35. V primeru zunanjega izvajanja ključnih ali pomembnih operativnih funkcij v oblaku bi moral skrbni pregled vključevati oceno ustreznosti ponudnika storitev v oblaku (na primer spretnosti, infrastrukture, gospodarskih razmer ter poslovnega in pravnega statusa podjetja). Kjer je primerno, lahko podjetje za podporo skrbnega pregleda uporabi dokaze, certifikate na podlagi mednarodnih standardov, revizijska poročila priznanih tretjih oseb ali poročila o notranji reviziji.

Smernica 10 – Pogodbene zahteve

36. Zadevne pravice in obveznosti podjetja in ponudnika storitev v oblaku se jasno razdelijo in opredelijo v pisnem sporazumu.
37. Brez poseganja v zahteve iz člena 274 delegirane uredbe bi morali biti v primeru oddajanja ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudniku storitev v oblaku v pisnem dogovoru med podjetjem in ponudnikom storitev v oblaku določeni:
- jasen opis funkcije, oddane v zunanje izvajanje (storitve v oblaku, vključno z vrsto podpornih storitev);
 - datum začetka in, kjer je ustrezno, datum konca veljavnosti pogodbe ter odpovedni roki za ponudnika storitev v oblaku in podjetje;
 - pristojno sodišče in pravo, ki ureja dogovor;
 - finančne obveznosti pogodbenih strank;
 - ali je dovoljeno zunanje podizvajanje ključne ali pomembne operativne funkcije ali dejavnosti (ali njenih bistvenih delov) in, če je, pogoji, ki veljajo za pomembno zunanje podizvajanje (glej smernico 13);
 - lokacija (ali lokacije) (regije ali države), kjer se bodo hranili in obdelovali ustrezni podatki (lokacija podatkovnih centrov), ter pogoji, ki jih je treba

- izpolniti, vključno z zahtevo, da mora ponudnik storitev obvestiti podjetje, če namerava zamenjati lokacijo (ali lokacije);
- g. določbe glede dostopnosti, razpoložljivosti, celovitosti, zaupnosti, zasebnosti in varnosti ustreznih podatkov, ob upoštevanju specifikacij iz smernice 12;
 - h. pravica podjetja, da redno spremlja uspešnost ponudnika storitev v oblaku;
 - i. dogovorjene ravni storitve, ki bi morale vključevati natančne kvantitativne in kvalitativne cilje uspešnosti, da se omogoči pravočasno spremljanje, na podlagi katerega se lahko brez odlašanja sprejmejo ustrezni popravni ukrepi, če dogovorjene ravni storitve niso dosežene;
 - j. obveznosti ponudnika storitev v oblaku glede poročanja podjetju, po potrebi vključno z obveznostmi predložitve poročil, ki so pomembna za varnostno funkcijo podjetja in ključne funkcije, kot so poročila funkcije notranje revizije ponudnika storitev v oblaku;
 - k. ali bi moral ponudnik storitev v oblaku skleniti obvezno zavarovanje za primer nekaterih tveganj in, če je ustrezno, stopnja zahtevanega zavarovalnega kritja;
 - l. zahteve po izvajanju in preskušanju poslovnih kriznih načrtov;
 - m. zahteva, da ponudnik storitev v oblaku podjetju, njegovim nadzornim organom in kateri koli drugi osebi, ki jo imenuje podjetje ali nadzorni organ, odobri:
 - i. poln dostop do vseh pomembnih poslovnih prostorov (sedežev in operativnih centrov), vključno z vsemi pomembnimi napravami, sistemi, omrežji, informacijami in podatki, ki se uporabljajo za zagotavljanje funkcije, oddane v zunanje izvajanje, vključno s povezanimi finančnimi informacijami, osebjem in zunanjimi revizorji ponudnika storitev v oblaku (pravice do dostopa);
 - ii. neomejene pravice do inšpekcijskega in revizijskega pregleda v zvezi z dogovorom o zunanjem izvajanju storitev v oblaku (pravice do revizije), da se jim omogoči spremljanje dogovora o zunanjem izvajanju ter zagotovi skladnost z vsemi veljavnimi regulativnimi in pogodbenimi zahtevami;
 - n. določbe, ki zagotavljajo, da lahko podjetje v primeru insolventnosti, reševanja ali opustitve poslovnih dejavnosti ponudnika storitev, nemudoma ponovno prevzame podatke, katerih lastnik je.

Smernica 11 – Pravici do dostopa in revizije

- 38. Sporazum o zunanjem izvajanju storitev v oblaku ne bi smel omejevati učinkovitega uveljavljanja pravic podjetja do dostopa in revizije ali možnosti nadzora nad storitvami v oblaku, da bi izpolnilo svoje regulativne obveznosti.
- 39. Podjetje bi moralo uveljavljati svoji pravici do dostopa in revizije, določiti pogostost revizij ter področja in storitve, ki jih je treba revidirati, s pristopom na podlagi tveganja v skladu z oddelkom 8 Smernic o sistemu upravljanja, ki jih je izdal organ EIOPA.
- 40. Podjetje bi moralo pri določanju pogostosti in obsega uveljavljanja pravic do dostopa ali revizije upoštevati, ali je zunanje izvajanje storitev v oblaku povezano s ključno ali pomembno operativno funkcijo ali dejavnostjo, naravo in obseg tveganja ter učinek dogovorov o zunanjem izvajanju storitev v oblaku na podjetje.
- 41. Če uveljavljanje pravic podjetja do dostopa ali revizije ali uporaba nekaterih revizijskih tehnik pomeni tveganje za okolje ponudnika storitev v oblaku in/ali drugega naročnika ponudnika storitev v oblaku (na primer vpliv na ravni storitev,

razpoložljivost podatkov, vidike zaupnosti), bi se morala podjetje in ponudnik storitev v oblaku dogovoriti o drugih možnih načinih zagotovitve podobne ravni jamstva in storitev podjetju (na primer vključitev posebnih kontrol, ki se preskusijo v posebnem poročilu/certifikaciji, ki ga/jo pripravi ponudnik storitev v oblaku).

42. Da bi učinkoviteje uporabila revizijska sredstva in zmanjšala organizacijsko breme za ponudnike storitev v oblaku in njihove stranke, lahko podjetja brez poseganja v svojo končno odgovornost glede dejavnosti, ki jih izvajajo njihovi ponudniki storitev v oblaku, uporabijo:
 - a. certifikate, ki jih izdajo tretje osebe, in revizijska poročila tretjih oseb ali notranja revizijska poročila, ki jih zagotovi ponudnik storitev;
 - b. skupne revizije (tj. izvedene skupaj z drugimi strankami istega ponudnika storitev v oblaku) ali skupne revizije, ki jih izvede tretja stran, ki so jo stranke imenovala.
43. V primeru oddaje ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje storitev v oblaku bi morala podjetja uporabiti metodo iz odstavka 42(a) le, če:
 - a. zagotovijo, da področje certifikata oz. revizijskega poročila zajema sisteme (na primer procese, aplikacije, infrastrukturo, podatkovne centre itd.) in kontrole, ki jih opredeli podjetje, ter ocenijo skladnost z ustreznimi regulativnimi zahtevami;
 - b. temeljito in redno ocenjujejo vsebino novih certifikatov ali revizijskih poročil ter se prepričajo, da ti certifikati ali poročila niso zastareli;
 - c. zagotovijo, da so ključni sistemi in kontrole vključeni v prihodnje različice certifikata ali revizijskega poročila;
 - d. so zadovoljna z usposobljenostjo osebe, ki izvaja certificiranje oz. revizijo (na primer glede rotacije podjetja, ki izvaja certificiranje oz. revizijo, kvalifikacij, strokovnega znanja, ponovnega izvajanja revizije/preverjanja dokazov v zadevnem revizijskem dosjeju);
 - e. se prepričajo, da se certifikati izdajo in revizije izvajajo v skladu z ustreznimi standardi ter vključujejo preskus operativne učinkovitosti vzpostavljenih ključnih kontrol;
 - f. imajo pogodbeno pravico, da zahtevajo razširitev področja certifikatov ali revizijskih poročil na druge relevantne sisteme in kontrole, število in pogostost takih zahtev za spremembo obsega pa morata biti razumna in upravičena z vidika obvladovanja tveganja;
 - g. ohranijo pogodbeno pravico do izvajanja posameznih revizij na kraju samem po lastni presoji v zvezi z oddajanjem ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje storitev v oblaku; to pravico bi bilo treba uveljavljati v primeru posebnih potreb, ki jih ni mogoče zadovoljiti z drugimi vrstami stikov s ponudnikom storitev v oblaku.
44. Pri oddajanju ključnih ali pomembnih operativnih funkcij v zunanje izvajanje ponudnikom storitev v oblaku bi moralo podjetje oceniti, ali so certifikati in poročila tretjih oseb iz odstavka 42(a) ustrezni in zadostni za izpolnjevanje njegovih regulativnih obveznosti, in se v skladu s pristopom na podlagi tveganja sčasoma ne bi smelo več zanašati izključno na ta poročila in certifikate.
45. Stranka, ki uveljavlja pravico do dostopa (podjetje, revizor ali tretja stran, ki deluje v imenu podjetja (ali podjetij)), bi morala pred načrtovanim obiskom na kraju samem ponudnika storitev v razumnem času o tem obvestiti, razen če predhodno

obvestilo ni mogoče zaradi izrednih ali kriznih razmer. Obvestilo bi moralo vključevati lokacijo in namen obiska ter uslužbenca, ki se bodo udeležili obiska.

46. Glede na to, da so rešitve v oblaku tehnično precej zapletene, bi moralo podjetje preveriti, ali ima osebje, ki izvaja revizijo – notranji revizorji, skupina revizorjev, ki deluje v njegovem imenu, ali revizorji, ki jih je imenoval ponudnik storitev v oblaku – ali po potrebi osebje, ki pregleduje certifikate tretjih oseb ali revizijska poročila ponudnika storitev, ustrezne spretnosti in znanje za izvedbo zadevnih revizij in/ali ocen.

Smernica 12 – Varnost podatkov in sistemov

47. Podjetje bi moralo zagotoviti, da ponudniki storitev v oblaku izpolnjujejo evropske in nacionalne predpise ter ustrezne varnostne standarde IKT.
48. V primeru oddaje ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku bi moralo podjetje v sporazumu o zunanjem izvajanju dodatno opredeliti posebne zahteve glede informacijske varnosti in redno spremljati izpolnjevanje teh zahtev.
49. V primeru oddaje ključnih ali pomembnih operativnih funkcij ali dejavnosti v zunanje izvajanje ponudnikom storitev v oblaku bi moralo podjetje za namene odstavka 48 s pristopom na podlagi tveganja ter ob upoštevanju svojih odgovornosti in odgovornosti ponudnika storitev v oblaku:
- a. doseči dogovor o jasni razdelitvi in opredelitvi vlog in odgovornosti ponudnika storitev v oblaku in podjetja v zvezi z operativnimi funkcijami ali dejavnostmi, na katere vpliva zunanje izvajanje storitev v oblaku;
 - b. opredeliti in določiti ustrezno stopnjo varstva zaupnih podatkov, neprekinjenosti dejavnosti, oddanih v zunanje izvajanje, in celovitosti ter sledljivosti podatkov in sistemov v okviru načrtovanega zunanjega izvajanja v oblaku;
 - c. po potrebi razmisliti o posebnih ukrepih za podatke med prenašanjem, podatke v pomnilniku in podatke med shranjevanjem, kot je uporaba tehnologij šifriranja v kombinaciji z ustreznim upravljanjem ključev;
 - d. razmisliti o mehanizmi vključevanja storitev v oblaku v sisteme podjetij, kot so vmesniki za aplikacijsko programiranje, in zanesljivem postopku upravljanja uporabnikov in dostopa;
 - e. s pogodbo zagotoviti, da razpoložljivost in pričakovana zmogljivost omrežnega prometa izpolnjujeta zahteve glede stroge neprekinjenosti, kjer je to primerno in izvedljivo;
 - f. opredeliti in določiti ustrezne zahteve glede neprekinjenosti, da bi bile zagotovljene ustrezne ravni na vsaki stopnji tehnološke verige, kjer je to ustrezno;
 - g. imeti zanesljiv in dobro dokumentiran proces obvladovanja incidentov, vključno z zadevnimi odgovornostmi, na primer z opredelitvijo modela sodelovanja v primeru dejanskih ali domnevnih incidentov;
 - h. sprejeti pristop na podlagi tveganja za obravnavo lokacij, kjer se podatki hranijo in obdelujejo (države ali regije), in vidikov varnosti informacij;
 - i. spremljati izpolnjevanje zahtev v zvezi z učinkovitostjo in uspešnostjo nadzornih mehanizmov, ki jih izvaja ponudnik storitev v oblaku, s katerimi bi se zmanjšala tveganja, povezana z zagotovljenimi storitvami.

Smernica 13 – Zunanje podizvajanje ključnih ali pomembnih operativnih funkcij ali dejavnosti

50. Če je zunanje podizvajanje ključnih ali pomembnih operativnih funkcij (ali njihovih delov) dovoljeno, bi moralo biti v sporazumu o zunanjem izvajanju storitev v oblaku med podjetjem in ponudnikom storitev v oblaku:
- a. določeno, katere vrste dejavnosti so izključene iz morebitnega zunanjega podizvajanja;
 - b. navedeni pogoji, ki morajo biti izpolnjeni v primeru zunanjega podizvajanja (na primer, da tudi zunanji podizvajalec v celoti izpolnjuje zadevne obveznosti ponudnika storitev v oblaku). Te obveznosti vključujejo pravice do revizije in dostopa ter varnost podatkov in sistemov;
 - c. navedeno, da ponudnik storitev v oblaku ohrani popolno odgovornost za storitve, oddane v zunanje podizvajanje, in nadzor nad njimi;
 - d. vključena obveznost ponudnika storitev v oblaku, da podjetje obvesti o morebitnih načrtovanih bistvenih spremembah zunanjih podizvajalcev ali storitev, oddanih v zunanje podizvajanje, ki bi lahko vplivale na zmožnost ponudnika storitev, da izpolni svoje obveznosti iz pogodbe o zunanjem izvajanju storitev v oblaku. Rok za obveščanje o teh spremembah bi moral podjetju omogočiti, da oceni tveganja učinkov predlaganih sprememb, preden se sprememba glede zunanjih podizvajalcev ali storitev, oddanih v zunanje podizvajanje, dejansko zgodi;
 - e. zagotovljeno, da ima podjetje, kadar ponudnik storitev v oblaku načrtuje spremembe zunanjega podizvajalca ali storitev, oddanih v zunanje podizvajanje, ki bi negativno vplivale na oceno tveganja dogovorjenih storitev, pravico, da ugovarja tem spremembam in/ali pravico, da odpove pogodbo in izstopi iz pogodbenega razmerja.

Smernica 14 – Spremljanje in nadzorovanje dogovorov o zunanjem izvajanju storitev v oblaku

51. Podjetje bi moralo s pristopom na podlagi tveganja redno spremljati, ali njegovi ponudniki storitev v oblaku izvajajo dejavnosti in varnostne ukrepe ter upoštevajo dogovorjeno raven storitev. Glavni poudarek bi moral biti na zunanjem izvajanju ključnih in pomembnih operativnih funkcij v oblaku.
52. V ta namen bi moralo podjetje vzpostaviti mehanizme za spremljanje in nadzor, ki bi morali, kadar je to izvedljivo in ustrezno, upoštevati morebitno zunanje podizvajanje ključnih ali pomembnih operativnih funkcij ali njihovih delov.
53. Upravni, upravljalni ali nadzorni organ je treba redno obveščati o ugotovljenih tveganjih v zvezi z zunanjim izvajanjem ključnih ali pomembnih operativnih funkcij ali dejavnosti v oblaku.
54. Da bi podjetja zagotovila ustrezno spremljanje in nadzor nad dogovori o zunanjem izvajanju storitev v oblaku, bi morala imeti dovolj zaposlenih z ustreznimi spretnostmi in znanjem za spremljanje storitev, oddanih v zunanje izvajanje storitev v oblaku. Osebe podjetja, odgovorno za te dejavnosti, bi morale imeti tako znanje o IKT kot tudi poslovno znanje, ki se šteje za potrebno.

Smernica 15 – Pravica do odpovedi pogodbe in strategije izstopa

55. V primeru zunanjega izvajanja ključnih ali pomembnih operativnih funkcij ali dejavnosti v oblaku bi morale podjetje imeti v sporazumu o zunanjem izvajanju storitev v oblaku klavzulo o jasno opredeljeni izhodni strategiji, v kateri bi bila po potrebi zagotovljena možnost odpovedi dogovora. Odpoved bi morala biti mogoča, ne da bi škodila neprekinjenosti in kakovosti zagotavljanja storitev imetnikom polic. V ta namen bi podjetje moralo:
- a. pripraviti načrte za izstop, ki temeljijo na storitvah in so izčrpni, dokumentirani ter ustrezno preskušeni (na primer z analizo morebitnih stroškov, učinkov, virov in časovnih posledic za različne možnosti izstopa);
 - b. opredeliti nadomestne rešitve ter pripraviti ustrezne in izvedljive načrte prehoda, ki podjetju omogočajo, da ponudniku storitev v oblaku vzame obstoječe dejavnosti in podatke in jih prenese na druge ponudnike storitev ali nazaj v podjetje. Te rešitve bi bilo treba opredeliti ob upoštevanju izzivov, ki se lahko pojavijo zaradi lokacije podatkov, in sprejeti potrebne ukrepe za zagotovitev neprekinjenega poslovanja v prehodnem obdobju;
 - c. zagotoviti, da ponudnik storitev v oblaku ustrezno podpira podjetje pri prenosu podatkov, sistemov ali aplikacij, ki so bili oddani v zunanje izvajanje, na drugega ponudnika storitev ali neposredno na podjetje;
 - d. se dogovoriti s ponudnikom storitev v oblaku, da bo po prenosu podatkov nazaj podjetju v celoti in varno izbrisal podatke podjetja v vseh regijah.
56. Pri oblikovanju strategije izstopa bi morale podjetje:
- a. opredeliti cilje strategije izstopa;
 - b. opredeliti sprožilne dogodke (na primer ključne kazalnike tveganja, ki kažejo nesprejemljivo raven storitve), ki lahko sprožijo strategijo izstopa;
 - c. opraviti analizo vpliva na poslovanje, sorazmerno z dejavnostmi, oddanimi v zunanje izvajanje, s katero bi ugotovilo, kakšne človeške in druge vire ter koliko časa bi potrebovalo za izvedbo načrta izstopa;
 - d. dodeliti vloge in odgovornosti za upravljanje načrtov izstopa in dejavnosti prehoda;
 - e. opredeliti merila uspešnosti prehoda.

Smernica 16 – Nadzor dogovorov o zunanjem izvajanju storitev v oblaku, ki ga izvajajo nadzorni organi

57. Nadzorni organi bi morali v okviru svojega postopka nadzornega pregleda opraviti analizo učinkov, ki izhajajo iz dogovorov o zunanjem izvajanju storitev v oblaku. Analiza učinkov bi morala biti osredotočena zlasti na dogovore, povezane z zunanjim izvajanjem ključnih ali pomembnih operativnih funkcij ali dejavnosti.
58. Nadzorni organi bi morali pri nadzoru dogovorov o zunanjem izvajanju storitev v oblaku obravnavati naslednja tveganja:
- a. tveganja v zvezi z IKT;
 - b. druga operativna tveganja (vključno s pravnim tveganjem in tveganjem glede skladnosti ter tveganjem glede zunanjega izvajanja in upravljanja tretjih strani);
 - c. tveganje izgube poslovnega ugleda;
 - d. tveganje koncentracije, vključno z ravno države/sektorja.

59. Nadzorni organi bi morali v svojo oceno s pristopom na podlagi tveganja vključiti naslednje vidike:
- a. ustreznost in uspešnost postopkov upravljanja in operativnih postopkov podjetja, povezanih z odobritvijo, izvajanjem, spremljanjem, upravljanjem in obnovitvijo dogovorov o zunanjem izvajanju storitev v oblaku;
 - b. ali ima podjetje dovolj virov z ustreznimi spretnostmi in znanjem za spremljanje storitev, oddanih v zunanje izvajanje storitev v oblaku;
 - c. ali podjetje ugotavlja in obvladuje vsa tveganja, ki so bila izpostavljena v teh smernicah.
60. V primeru skupin bi moral nadzornik skupine zagotoviti, da so učinki zunanjega izvajanja ključnih ali pomembnih operativnih funkcij ali dejavnosti v oblaku vključeni v nadzorni oceni tveganja skupine, pri čemer je treba upoštevati zahteve iz odstavkov 58–59 ter posamezne značilnosti skupine v zvezi z upravljanjem in njene operativne značilnosti.
61. Če zunanje izvajanje ključnih ali pomembnih operativnih funkcij ali dejavnosti v oblaku vključuje več podjetij v različnih državah članicah in ga centralno upravlja matična družba ali hčerinska družba skupine (na primer podjetje ali storitvena družba skupine, kot je ponudnik IKT skupine), bi moral nadzornik skupine in/ali ustrezni nadzorni organi podjetij, vključenih v zunanje izvajanje storitev v oblaku, po potrebi razpravljati o učinkih zunanjega izvajanja storitev v oblaku na profil tveganja skupine v kolegiju nadzornikov.
62. Če se pojavijo pomisleki, ki vodijo do zaključka, da podjetje nima več trdnih ureditev upravljanja ali ne izpolnjuje regulativnih zahtev, bi morali nadzorni organi ustrezno ukrepati, kar lahko vključuje na primer zahtevo, da podjetje izboljša ureditev upravljanja, zmanjšanje ali omejitev obsega funkcij, oddanih v zunanje izvajanje, ali zahtevo po izstopu iz enega ali več dogovorov o zunanjem izvajanju. Ob upoštevanju potrebe po zagotovitvi neprekinjenosti delovanja podjetja bi se lahko zahtevala zlasti odpoved pogodb, če nadzora in izvrševanja regulativnih zahtev ni mogoče zagotoviti z drugimi ukrepi.

Pravila glede skladnosti in poročanja

63. Ta dokument vsebuje smernice, izdane v skladu s členom 16 Uredbe (EU) št. 1094/2010. V skladu s členom 16(3) navedene uredbe si morajo pristojni organi in finančne institucije na vsak način prizadevati za spoštovanje smernic in priporočil.
64. Pristojni organi, ki upoštevajo ali nameravajo upoštevati te smernice, jih morajo ustrezno vključiti v svoj zakonodajni ali nadzorni okvir.
65. Pristojni organi morajo v dveh mesecih po objavi prevedenih različic potrditi organu EIOPA, ali ravnajo oziroma nameravajo ravnati v skladu s temi smernicami, oziroma navedejo razloge za njihovo neupoštevanje.
66. Če pristojni organi v tem roku ne bodo odgovorili, se bo štelo, da ne ravnajo v skladu s pravili glede poročanja, in se bo o njih tako tudi poročalo.

Končna določba glede pregleda

67. Za pregled teh smernic je pristojen organ EIOPA.