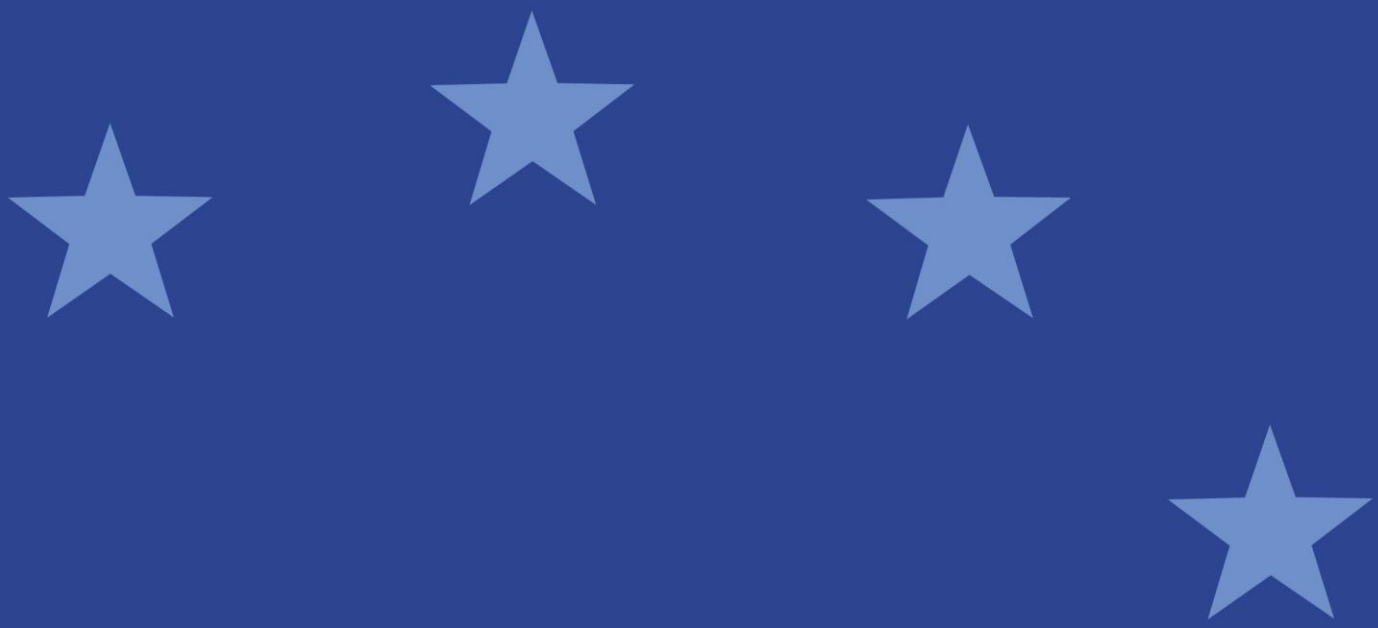
esma European Securities and Markets Authority

Smernice

za zunanje izvajanje ponudnikov storitev v oblaku



10/05/2021 | ESMA50-164-4285 SL

Kazalo

I. Področje uporabe

Kdo?

1. Te smernice so namenjene pristojnim organom in (i) upravljavcem alternativnih investicijskih skladov (UAIS) in depozitarjem alternativnih investicijskih skladov (AIS), (ii) kolektivnim naložbenim podjemom za vlaganja v prenosljive vrednostne papirje (KNPVP), družbam za upravljanje in depozitarjem KNPVP ter investicijskim družbam, ki niso prenesle pooblastil za upravljanje na družbo za upravljanje v skladu z direktivo o KNPVP, (iii) centralnim nasprotnim strankam (CNS), vključno s CNS stopnje 2 iz tretjih držav, ki izpolnjujejo ustrezne zahteve uredbe EMIR, (iv) repozitorijem sklenjenih poslov, (v) investicijskim podjetjem in kreditnim institucijam, kadar izvajajo investicijske storitve in posle, izvajalcem storitev sporočanja podatkov in upravljavcem trga, ki upravljajo mesta trgovanja, (vi) centralnim depotnim družbam, (vii) bonitetnim agencijam, (viii) repozitorijem listinjenja in (ix) upravljavcem ključnih referenčnih vrednosti.

2. Organ ESMA bo te smernice upošteval tudi pri ocenjevanju obsega, v katerem se šteje, da v skladu s členom 25(2b)(a) uredbe EMIR centralne nasprotne stranke stopnje 2 iz tretjih držav izpolnjujejo ustrezne zahteve uredbe EMIR z izpolnjevanjem primerljivih zahtev v tretjih državah.

Kaj?

3. Te smernice veljajo v zvezi z naslednjimi določbami:

   a) členi 15, 18 in 20 ter člen 21(8) direktive o upravljavcih alternativnih investicijskih skladov; členi 13, 22, 38, 39, 40, 44 in 45, člen 57(1)(d), člena 57(2) in 57(3), členi 58, 75, 76, 77, 79, 81, 82 in 98 Delegirane uredbe Komisije (EU) 2013/231;
   b) člen 12(1)(a), člen 13, člen 14(1)(c), člena 22 in 22a, člen 23(2), člena 30 in 31 direktive o KNPVP; člen 4(1) do 4(3), člena 4(5) in 5(2), člena 7 in 9, člen 23(4), členi 32, 38, 39 in 40 Direktive Komisije 2010/43/EU; člen 2(2)(j), člena 3(1) in 13(2), členi 15, 16 in 22 Delegirane uredbe Komisije (EU) 2016/438;
   c) člen 25, členi 26(1), 26(3) in 26(6), členi 34, 35 in 78 do 81 uredbe EMIR; člena 5 in 12 uredbe o poslih financiranja z vrednostnimi papirji; člen 3(1)(f), člen 3(2), člen 4, člen 7(2)(d) in (f), člena 9 in 17 Delegirane uredbe Komisije (EU) št. 153/2013; člena 16 in 21 Delegirane uredbe Komisije (EU) št. 150/2013; člena 16 in 21 Delegirane uredbe Komisije (EU) 2019/359;
   d) člen 16(2), 16(4) in 16(5), člen 18(1), člen 19(3)(a), člen 47(1)(b) in (c), člen 48(1), člen 64(4), 65(5) in 66(3)1 MiFID II; člen 21(1) do (3), člen 23, člen 29(5), členi 30, 31 in 32 Delegirane uredbe Komisije (EU) 2017/565; člena 6 in 15 ter člen 16(6)

[1] Od 1. januarja 2022 je treba sklicevanja na člene 64(4), 65(5) in 66(3) direktive MiFID II razumeti kot sklicevanje na člene 27g(4), 27h(5) in 27i(3) uredbe MiFIR.

Delegirane uredbe Komisije (EU) 2017/584; členi 6, 7, 8 in 9 Delegirane uredbe Komisije (EU) 2017/571;

e) členi 22, 26, 30, 42, 44 in 45 uredbe o centralnih depotnih družbah ter člena 33 in 47, člen 50(1), člen 57(2)(i), členi 66, 68, 75, 76, 78 in 80 Delegirane uredbe Komisije (EU) 2017/392;
f) člen 9 ter točki 4 in 8 oddelka A Priloge I ter točka 17 Priloge II uredbe o bonitetnih agencijah ter člena 11 in 25 Delegirane uredbe Komisije (EU) št. 2012/449;
g) člen 10(2) uredbe o listinjenju;
h) člen 6(3) in člen 10 uredbe o referenčnih merilih in točka 7 Priloge I Delegirane uredbe Komisije (EU) 2018/1646.

Kdaj?

4. Te smernice se uporabljajo od 31. julija 2021 dalje za vse dogovore o zunanjem izvajanju storitev v oblaku, ki so sklenjeni, obnovljeni ali spremenjeni na navedeni datum ali pozneje. Podjetja bi morala pregledati in ustrezno spremeniti obstoječe dogovore o zunanjem izvajanju storitev v oblaku, da bi tako zagotovila skladnost s temi smernicami do 31. decembra 2022. Če pregled dogovorov o zunanjem izvajanju funkcij, ki so odločilnega pomena, ali pomembnih funkcij v oblaku ne bo končan do 31. decembra 2022, bi morala podjetja o tem obvestiti svoj pristojni organ in pri tem navesti ukrepe, načrtovane za dokončanje pregleda, ali morebitno strategijo izstopa.

II. Sklicevanja na pravne vire, kratice in opredelitev pojmov

Sklicevanje na pravne vire

Uredba ESMA	Uredba (EU) št. 1095/2010 Evropskega parlamenta in Sveta z dne 24. novembra 2010 o ustanovitvi Evropskega nadzornega organa (Evropski organ za vrednostne papirje in trge) in o spremembi Sklepa št. 716/2009/ES ter razveljavitvi Sklepa Komisije 2009/77/ES[2]
Direktiva o UAIS	Direktiva 2011/61/EU Evropskega parlamenta in Sveta z dne 8. junija 2011 o upravljavcih alternativnih investicijskih skladov in spremembah direktiv 2003/41/ES in 2009/65/ES ter uredb (ES) št. 1060/2009 in (EU) št. 1095/2010[3]
Delegirana uredba Komisije (EU) 2013/231	Delegirana uredba Komisije (EU) št. 2013/231 z dne 19. decembra 2012 o dopolnitvi Direktive 2011/61/EU Evropskega parlamenta in Sveta v zvezi z izjemami, splošnimi pogoji poslovanja, depozitarji, finančnim vzvodom, preglednostjo in nadzorom[4]

[2] UL L 331, 15.12.2010, str. 84.
[3] UL L 174, 1.7.2011, str. 1.
[4] UL L 83, 22.3.2013, str. 1.

Direktiva o KNPVP	Direktiva 2009/65/ES Evropskega parlamenta in Sveta z dne 13. julija 2009 o usklajevanju zakonov in drugih predpisov o kolektivnih naložbenih podjemih za vlaganja v prenosljive vrednostne papirje (KNPVP)[5]
Direktiva Komisije 2010/43/EU	Direktiva Komisije 2010/43/EU z dne 1. julija 2010 o izvajanju Direktive 2009/65/ES Evropskega parlamenta in Sveta o organizacijskih zahtevah, navzkrižjih interesov, poslovanju, obvladovanju tveganja ter vsebini sporazuma med depozitarjem in družbo za upravljanje[6]
Delegirana uredba Komisij (EU) 2016/438	Delegirana uredba Komisije (EU) 2016/438 z dne 17. decembra 2015 o dopolnitvi Direktive 2009/65/ES Evropskega parlamenta in Sveta v zvezi z obveznostmi depozitarjev[7]
Uredba EMIR	Uredba (EU) št. 648/2012 Evropskega parlamenta in Sveta z dne 4. julija 2012 o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov[8]
Uredba o poslih financiranja z vrednostnimi papirji	Uredba (EU) št. 2015/2365 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o preglednosti poslov financiranja z vrednostnimi papirji in ponovne uporabe ter spremembi Uredbe (EU) št. 648/2012[9]
Delegirana uredba Komisije (EU) št. 153/2013	Delegirana uredba Komisije (EU) št. 153/2013 z dne 19. decembra 2012 o dopolnitvi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi glede zahtev za centralne nasprotne stranke[10]
Delegirana uredba Komisije (EU) št. 150/2013	Delegirana uredba Komisije (EU) št. 150/2013 z dne 19. decembra 2012 o dopolnitvi Uredbe (EU) št. 648/2012 Evropskega parlamenta in Sveta o izvedenih finančnih instrumentih OTC, centralnih nasprotnih strankah in repozitorijih sklenjenih poslov, kar zadeva regulativne tehnične standarde, ki določajo podrobnosti vloge za registracijo repozitorija sklenjenih poslov[11]
Delegirana uredba Komisije (EU) 2019/359	Delegirana uredba Komisije (EU) 2019/359 z dne 13. decembra 2018 o dopolnitvi Uredbe (EU) 2015/2365 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo podrobnosti vloge za

[5] UL L 302, 17.11.2009, str. 32.
[6] UL L 176, 10.7.2010, str. 42.
[7] UL L 78, 24.3.2016, str. 11.
[8] UL L 201, 27.7.2012, str. 1.
[9] UL L 337, 23.12.2015, str. 1.
[10] UL L 52, 23.2.2013, str. 41.
[11] UL L 52, 23.2.2013, str. 25.

	registracijo in razširitev obsega registracije repozitorija sklenjenih poslov[12]
MiFID II	Direktiva 2014/65/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov ter spremembi Direktive 2002/92/ES in Direktive 2011/61/EU[13]
Uredba MiFIR	Uredba (EU) št. 600/2014 Evropskega parlamenta in Sveta z dne 15. maja 2014 o trgih finančnih instrumentov in spremembi Uredbe (EU) št. 648/2012 ([14])
Delegirana uredba Komisij (EU) 2017/565	Delegirana uredba Komisije (EU) 2017/565 z dne 25. aprila 2016 o dopolnitvi Direktive 2014/65/EU Evropskega parlamenta in Sveta v zvezi z organizacijskimi zahtevami in pogoji poslovanja investicijskih podjetij ter opredeljenimi izrazi za namene navedene direktive[15]
Delegirana uredba Komisije (EU) 2017/584	Delegirana uredba Komisije (EU) 2017/584 z dne 14. julija 2016 o dopolnitvi Direktive 2014/65/EU Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi, ki določajo organizacijske zahteve za mesta trgovanja[16]
Delegirana uredba Komisije (EU) 2017/571	Delegirana uredba Komisije (EU) 2017/571 z dne 2. junija 2016 o dopolnitvi Direktive 2014/65/EU Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o dovoljenju, organizacijskih zahtevah in objavi poslov za izvajalce storitev sporočanja podatkov[17]
Uredba o centralnih depotnih družbah	Uredba (EU) št. 909/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o izboljšanju ureditve poravnav vrednostnih papirjev v Evropski uniji in o centralnih depotnih družbah ter o spremembi direktiv 98/26/ES in 2014/65/EU ter Uredbe (EU) št. 236/2012[18]
Delegirana uredba Komisij (EU) 2017/392	Delegirana uredba Komisije (EU) 2017/392 z dne 11. novembra 2016 o dopolnitvi Uredbe (EU) št. 909/2014 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi o zahtevah glede izdaje dovoljenj, nadzora in poslovanja za centralne depotne družbe[19]
Uredba o bonitetnih agencijah	Uredba (ES) št. 1060/2009 Evropskega parlamenta in Sveta z dne 16. septembra 2009 o bonitetnih agencijah[20]

[12] UL L 81, 22.3.2019, str. 45.
[13] UL L 173, 12.6.2014, str. 349.
[14] UL L 173, 12.6.2014, str. 84.
[15] UL L 87, 31.3.2017, str. 1.
[16] UL L 87, 31.3.2017, str. 350.
[17] UL L 87, 31.3.2017, str. 126.
[18] UL L 257, 28.8.2014, str. 1.
[19] UL L 65, 10.3.2017, str. 48.
[20] UL L 302, 17.11.2009, str. 1.

Delegirana uredba Komisije (EU) št. 2012/449	Delegirana uredba Komisije (EU) št. 449/2012 z dne 21. marca 2012 o dopolnitvi Uredbe (ES) št. 1060/2009 Evropskega parlamenta in Sveta glede regulativnih tehničnih standardov za informacije za registracijo in certificiranje bonitetnih agencij[21]
Uredba o listinjenju	Uredba (EU) 2017/2402 Evropskega parlamenta in Sveta z dne 12. decembra 2017 o določitvi splošnega okvira za listinjenje in o vzpostavitvi posebnega okvira za enostavno, pregledno in standardizirano listinjenje ter o spremembah direktiv 2009/65/ES, 2009/138/ES in 2011/61/EU ter uredb (ES) št. 1060/2009 in (EU) št. 648/2012[22]
Uredba o referenčnih vrednostih	Uredba (EU) 2016/1011 Evropskega parlamenta in Sveta z dne 8. junija 2016 o indeksih, ki se uporabljajo kot referenčne vrednosti v finančnih instrumentih in finančnih pogodbah ali za merjenje uspešnosti investicijskih skladov, in spremembi direktiv 2008/48/ES in 2014/17/EU ter Uredbe (EU) št. 596/2014[23]
Delegirana uredba Komisije (EU) 2018/1646	Delegirana uredba Komisije (EU) 2018/1646 z dne 13. julija 2018 o dopolnitvi Uredbe (EU) 2016/1011 Evropskega parlamenta in Sveta v zvezi z regulativnimi tehničnimi standardi za informacije, ki se navedejo v vlogi za dovoljenje in v vlogi za registracijo[24]
Splošna uredba o varstvu podatkov	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[25]

Kratice

ESMA	Evropski organ za vrednostne papirje in trge
EU	Evropska unija
PSO	ponudnik storitev v oblaku

Opredelitev pojmov

funkcija	pomeni vsakršne procese, storitve ali dejavnosti.
funkcija odločilnega pomena ali pomembna funkcija	pomeni vsako funkcijo, v zvezi s katero bi napaka v njenem izvajanju ali njeno neizvajanje bistveno ogrozila:

[21] UL L 140, 30.5.2012, str. 32.
[22] UL L 347, 28.12.2017, str. 35.
[23] UL L 171, 29.6.2016, str. 1.
[24] UL L 274, 5.11.2018, str. 43.
[25] UL L 119, 4.5.2016, str. 1–88.

a) izpolnjevanje obveznosti podjetja v skladu z veljavno zakonodajo;
b) finančno uspešnost podjetja ali
c) zanesljivost ali neprekinjenost glavnih storitev in poslov podjetja.

storitve v oblaku	pomenijo storitve, ki se zagotavljajo z uporabo računalništva v oblaku.
računalništvo v oblaku ali oblak[26]	pomeni paradigmo za omogočanje omrežnega dostopa do nadgradljivega in prožnega nabora fizičnih ali virtualnih virov z možnostjo skupne rabe (na primer strežnikov, operacijskih sistemov, omrežij, programske opreme, aplikacij in opreme za shranjevanje) s samopostrežnim zagotavljanjem in upravljanjem na zahtevo.
ponudnik storitev v oblaku	pomeni tretjo osebo, ki zagotavlja storitve v oblaku v okviru dogovora o zunanjem izvajanju storitev v oblaku.
dogovor o zunanjem izvajanju storitev v oblaku	pomeni dogovor v kakršni koli obliki, vključno z dogovori o prenosu, med: (i) podjetjem in ponudnikom storitev v oblaku, pri čemer ponudnik storitev v oblaku opravlja funkcijo, ki bi jo sicer prevzelo podjetje samo, ali (ii) podjetjem in tretjo osebo, ki ni ponudnik storitev v oblaku, vendar se pri opravljanju funkcije, ki bi jo sicer prevzelo podjetje samo, v veliki meri opira na ponudnika storitev v oblaku. V tem primeru je treba sklicevanja na „ponudnika storitev v oblaku“ v teh smernicah razumeti kot sklicevanja na takšno tretjo osebo.
zunanje podizvajanje	pomeni stanje, ko ponudnik storitev v oblaku nadalje prenese funkcijo, oddano v zunanje izvajanje (ali del te funkcije), na drugega izvajalca storitev na podlagi dogovora o zunanjem podizvajanju.
model uvedbe oblaka	pomeni možni način organizacije oblaka na podlagi nadzora in skupne rabe fizičnih ali virtualnih virov. Modeli

[26] Računalništvo v oblaku je pogosto okrajšano na „oblak“. Zaradi lažjega sklicevanja se v preostalem dokumentu uporablja izraz „oblak“.

uvedbe oblaka vključujejo skupnostne [27], hibridne [28], zasebne[29] in javne[30] oblake.

podjetja

a) upravljavci alternativnih investicijskih skladov ali „UAIS“, kot so opredeljeni v členu 4(1)(b) direktive o UAIS, in depozitarji iz člena 21(3) direktive o UAIS (v nadaljnjem besedilu: depozitarji alternativnih investicijskih skladov (AIS));

b) družbe za upravljanje, kot so opredeljene v členu 2(1)(b) direktive o KNPVP („družbe za upravljanje KNPVP“), in depozitarji, kot so opredeljeni v členu 2(1)(a) direktive o KNPVP („depozitarji KNPVP“);

c) centralne nasprotne stranke (CNS), kot so opredeljene v členu 2(1) uredbe EMIR, in CNS stopnje 2 iz tretjih držav v smislu člena 25(2a) uredbe EMIR, ki izpolnjujejo ustrezne zahteve uredbe EMIR v skladu s členom 25(2b)(a) uredbe EMIR;

d) repozitoriji sklenjenih poslov, kot so opredeljeni v členu 2(2) uredbe EMIR in členu 3(1) uredbe o poslih financiranja z vrednostnimi papirji;

e) investicijska podjetja, kot so opredeljena v členu 4(1)(1) MiFID II, in kreditne institucije, kot so opredeljene v členu 4(1)(27) MiFID II, ki opravljajo investicijske storitve in posle v smislu člena 4(1)(2) MiFID II;

f) izvajalci storitev sporočanja podatkov, kot so opredeljeni v členu 4(1)(63) MiFID II[31];

[27] Model uvedbe oblaka, pri katerem storitve v oblaku izključno podpirajo posebno zbirko naročnikov storitev v oblaku, ki imajo skupne zahteve in so med seboj povezani ter katerih vire nadzoruje vsaj en član te zbirke, pri čemer takšna zbirka naročnikov souporablja storitve v oblaku.
[28] Model uvedbe oblaka, ki uporablja vsaj dva različna modela uvedbe oblaka.
[29] Model uvedbe oblaka, pri katerem storitve v oblaku uporablja izključno en naročnik storitev v oblaku, vire pa nadzoruje navedeni naročnik storitev v oblaku.
[30] Model uvedbe oblaka, pri katerem so storitve v oblaku potencialno na voljo vsem naročnikom storitev v oblaku, vire pa nadzoruje ponudnik storitev v oblaku.
[31] Od 1. januarja 2022 bi bilo treba sklicevanje na to določbo razumeti kot sklicevanje na točko 36(a) člena 2(1) uredbe MiFIR.

g) upravljavci trga, ki upravljajo mesta trgovanja v smislu člena 4(1)(24) MiFID II;

h) centralne depotne družbe (CDD), kot so opredeljene v členu 2(1)(1) uredbe o centralnih depotnih družbah;

i) bonitetne agencije, kot so opredeljene v členu 3(1)(b) uredbe o bonitetnih agencijah;

j) repozitoriji listinjenja, kot so opredeljeni v členu 2(23) uredbe o listinjenju;

k) upravljavce ključnih referenčnih vrednosti, kot so opredeljene v členu 3(1)(25) uredbe o referenčnih vrednostih.

III. Namen

5. Te smernice so izdane v skladu s členom 16(1) uredbe ESMA. Njihov namen je vzpostaviti dosledne, učinkovite in uspešne nadzorne prakse v okviru Evropskega sistema finančnega nadzora (ESFS) ter zagotoviti skupno, enotno in usklajeno uporabo zahtev iz oddelka 1.1 pod naslovom „Kaj“, kadar podjetja oddajo storitve v zunanje izvajanje ponudnikom storitev v oblaku. Namen teh smernic je zlasti pomagati podjetjem in pristojnim organom pri opredelitvi, obravnavi in spremljanju tveganj in izzivov, ki izhajajo iz dogovorov o zunanjem izvajanju storitev v oblaku, od odločanja o zunanjem izvajanju, izbire ponudnika storitev v oblaku, spremljanja dejavnosti, oddanih v zunanje izvajanje, do oblikovanja strategij izstopa.

IV. Obveznosti v zvezi s skladnostjo in poročanjem

Vloga teh smernic

6. Pristojni organi in podjetja si v skladu s členom 16(3) uredbe ESMA na vsak način prizadevajo upoštevati te smernice.

7. Pristojni organi, katerim so te smernice namenjene, bi jih morali upoštevati tako, da jih ustrezno vključijo v svoje nacionalne pravne in/ali nadzorne okvire, tudi kadar so posamezne smernice namenjene zlasti podjetjem. V tem primeru bi morali pristojni organi s svojim nadzorom zagotoviti, da podjetja upoštevajo smernice.

8. Organ ESMA bo s stalnim in neposrednim nadzorom ocenil, kako bonitetne agencije, repozitoriji sklenjenih poslov, repozitoriji listinjenja, CNS stopnje 2 iz tretjih držav in od 1. januarja 2022 tudi izvajalci storitev sporočanja podatkov in upravljavci ključnih referenčnih vrednosti EU uporabljajo te smernice.

Zahteve glede poročanja

9. Pristojni organi, katerim so te smernice namenjene, morajo v dveh mesecih od datuma njihove objave v vseh uradnih jezikih EU na spletni strani organa ESMA navedeni organ obvestiti, ali (i) upoštevajo smernice, (ii) ne upoštevajo smernic, vendar jih nameravajo upoštevati, ali (iii) ne upoštevajo smernic in jih tudi ne nameravajo upoštevati.

10. V primeru neupoštevanja morajo pristojni organi organ ESMA v dveh mesecih od datuma objave smernic v vseh uradnih jezikih EU na njegovi spletni strani obvestiti še o razlogih za neupoštevanje. Obrazec za pošiljanje obvestil je na voljo na spletni strani organa ESMA. Izpolnjena predloga se pošlje organu ESMA.

11. Podjetjem ni treba poročati o upoštevanju teh smernic.

V. Smernice za zunanje izvajanje ponudnikov storitev v oblaku

Smernica 1. Upravljanje, nadzor in dokumentacija

12. Podjetje bi moralo imeti opredeljeno in posodobljeno strategijo zunanjega izvajanja storitev v oblaku, ki je skladna z ustreznimi strategijami ter notranjimi pravilniki in postopki podjetja, tudi v zvezi z informacijsko in komunikacijsko tehnologijo, informacijsko varnostjo in obvladovanjem operativnega tveganja.

13. Podjetje bi moralo:

a) jasno dodeliti odgovornosti za dokumentiranje, upravljanje in nadziranje dogovorov o zunanjem izvajanju storitev v oblaku v svoji organizaciji;
b) dodeliti zadostna sredstva za zagotovitev skladnosti s temi smernicami in vsemi pravnimi zahtevami, ki veljajo za njegove dogovore o zunanjem izvajanju storitev v oblaku;
c) vzpostaviti funkcijo nadzora nad zunanjim izvajanjem storitev v oblaku ali imenovati višje člane osebja, ki so neposredno odgovorni upravljalnemu organu ter so odgovorni za obvladovanje in nadziranje tveganj dogovorov o zunanjem izvajanju storitev v oblaku. Pri upoštevanju te smernice bi morala podjetja upoštevati naravo, obseg in zapletenost svojega poslovanja, tudi v smislu tveganj za finančni sistem, in tveganj, povezanih s funkcijami, oddanimi v zunanje izvajanje, ter zagotoviti, da ima njihov upravljalni organ ustrezne tehnične sposobnosti za razumevanje tveganj,

povezanih z dogovori o zunanjem izvajanju storitev v oblaku[32]. Mala in manj kompleksna podjetja bi morala zagotoviti vsaj jasno delitev nalog in odgovornosti za upravljanje in nadziranje dogovorov o zunanjem izvajanju storitev v oblaku.

14. Podjetje bi moralo spremljati, kako njegovi ponudniki storitev v oblaku izvajajo dejavnosti ter ali izvajajo varnostne ukrepe in upoštevajo dogovorjene ravni storitev. To spremljanje bi moralo temeljiti na tveganju, pri čemer bi glavni poudarek moral biti na funkcijah odločilnega pomena ali pomembnih funkcijah, oddanih zunanjim izvajalcem.

15. Podjetje bi moralo redno in ob vsaki pomembni spremembi tveganja, narave ali obsega funkcije, oddane zunanjim izvajalcem, znova oceniti, ali se njegovi dogovori o zunanjem izvajanju storitev v oblaku nanašajo na funkcijo odločilnega pomena ali pomembno funkcijo.

16. Podjetje bi moralo voditi posodobljen register informacij o vseh svojih dogovorih o zunanjem izvajanju storitev v oblaku, pri čemer bi moralo razlikovati med zunanjim izvajanjem funkcij odločilnega pomena ali pomembnih funkcij in drugimi dogovori o zunanjem izvajanju storitev. Pri razlikovanju med zunanjim izvajanjem funkcij odločilnega pomena ali pomembnih funkcij in drugimi dogovori o zunanjem izvajanju storitev bi moralo podjetje na kratko povzeti razloge, zakaj se funkcija, oddana zunanjemu izvajalcu , šteje ali ne šteje za funkcijo odločilnega pomena ali pomembno funkcijo. Ob upoštevanju nacionalne zakonodaje bi moralo podjetje v ustreznem obdobju voditi tudi evidenco prekinjenih dogovorov o zunanjem izvajanju storitev v oblaku.

17. Pri dogovorih o zunanjem izvajanju storitev v oblaku v zvezi s funkcijami odločilnega pomena ali pomembnimi funkcijami bi moral register za vsak dogovor o zunanjem izvajanju storitev v oblaku vključevati vsaj naslednje dodatne informacije:

    a) referenčno številko;
    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) kratek opis funkcije, oddane zunanjemu izvajalcu, vključno s podatki, ki se oddajo v zunanje izvajanje, in navedbo, ali ti podatki vključujejo osebne podatke (na primer z navedbo da ali ne v ločenem podatkovnem polju);
    d) kategorijo, ki jo določi podjetje in odraža naravo funkcije, oddane zunanjemu izvajalcu , (npr. funkcija informacijske tehnologije, funkcija kontrole), kar bi moralo olajšati prepoznavanje različnih vrst dogovorov o zunanjem izvajanju storitev v oblaku;
    e) navedbo, ali funkcija, oddana zunanjemu izvajalcu, podpira časovno kritične poslovne dejavnosti;
    f) ime in trgovsko ime (če obstaja) ponudnika storitev v oblaku, matično državo, matično številko družbe, identifikator pravnih subjektov (če je na voljo), registrirani naslov in druge pomembne podatke za stik ter ime nadrejene družbe (če obstaja);

[32] Za investicijska podjetja in kreditne institucije glej Skupne smernice ESMA in EBA o ocenjevanju primernosti članov upravljalnega organa in nosilcev ključnih funkcij v skladu z Direktivo 2013/36/EU in Direktivo 2014/65/EU (EBA/GL/2017/12).

g) veljavno pravo dogovora o zunanjem izvajanju storitev v oblaku in, če obstaja, izbiro pristojnosti;
h) vrsto storitev v oblaku in modele uvedbe oblaka ter posebno naravo podatkov, ki jih je treba hraniti, in lokacije (tj. regije ali države), kjer se taki podatki lahko hranijo;
i) datum najnovejše ocene odločilnega pomena ali pomembnosti funkcije, oddane zunanjemu izvajalcu , in datum naslednje načrtovane ocene;
j) datum najnovejše ocene tveganja/revizije ponudnika storitev v oblaku skupaj s kratkim povzetkom glavnih rezultatov in datum naslednje načrtovane ocene tveganja/revizije;
k) posameznika ali organ odločanja v podjetju, ki je odobril dogovor o zunanjem izvajanju storitev v oblaku;
l) kadar je ustrezno, imena vseh zunanjih podizvajalcev, ki so jim v zunanje podizvajanje oddane funkcije odločilnega pomena ali pomembne funkcije (ali njihovi pomembni deli), vključno z državami, v katerih so zunanji podizvajalci registrirani, v katerih se bo izvajala storitev, oddana v zunanjemu podizvajalcu , in lokacijami (tj. regijami ali državami), kjer se bodo podatki hranili;
m) ocenjene letne proračunske stroške dogovora o zunanjem izvajanju storitev v oblaku.

18. Za dogovore o zunanjem izvajanju storitev v oblaku v zvezi s funkcijami, ki niso odločilnega pomena, ali nepomembnimi funkcijami bi moralo podjetje opredeliti informacije, ki jih je treba vključiti v register, na podlagi narave, obsega in zapletenosti tveganj, povezanih s funkcijo, oddano zunanjemu izvajalcu.

Smernica 2. Analiza pred zunanjim izvajanjem in skrbni pregled

19. Podjetje bi moralo pred sklenitvijo dogovora o zunanjem izvajanju storitev v oblaku:

a) oceniti, ali se dogovor o zunanjem izvajanju storitev v oblaku nanaša na funkcijo odločilnega pomena ali pomembno funkcijo;
b) opredeliti in oceniti vsa pomembna tveganja dogovora o zunanjem izvajanju storitev v oblaku;
c) opraviti skrbni pregled morebitnih ponudnikov storitev v oblaku;
d) opredeliti in oceniti morebitno navzkrižje interesov, ki bi ga zunanje izvajanje lahko povzročilo.

20. Analiza pred zunanjim izvajanjem in skrbni pregled morebitnega ponudnika storitev v oblaku bi morala biti sorazmerna z naravo, obsegom in zapletenostjo funkcije, ki jo podjetje namerava oddati zunanjemu izvajalcu, ter tveganji, povezanimi s to funkcijo. Vključevati bi morala vsaj oceno morebitnega učinka dogovora o zunanjem izvajanju storitev v oblaku na operativna in pravna tveganja za podjetje ter tveganja za podjetje v zvezi s skladnostjo in izgubo ugleda.

21. Če se dogovor o zunanjem izvajanju storitev v oblaku nanaša na funkcije odločilnega pomena ali pomembne funkcije, bi moralo podjetje tudi:

a) oceniti vsa pomembna tveganja, ki lahko nastanejo zaradi dogovora o zunanjem izvajanju storitev v oblaku, vključno s tveganji v zvezi z informacijsko in

komunikacijsko tehnologijo, informacijsko varnostjo, neprekinjenim poslovanjem, pravnimi vidiki in vidiki skladnosti, tveganji izgube ugleda, operativnimi tveganji in morebitnimi omejitvami nadzora za podjetje, ki izhajajo iz:

i. izbrane storitve v oblaku in predlaganih modelov uvedbe;
ii. procesov migracije in/ali izvajanja;
iii. občutljivosti funkcije in z njo povezanih podatkov, ki se nameravajo oddati zunanjemu izvajalcu, in varnostnih ukrepov, ki bi jih bilo treba sprejeti;
iv. interoperabilnosti sistemov in aplikacij podjetja in ponudnika storitev v oblaku, in sicer njihove zmogljivosti za izmenjavo informacij in vzajemno uporabo izmenjanih informacij;
v. prenosljivosti podatkov podjetja, in sicer zmožnosti za enostaven prenos podatkov podjetja od enega ponudnika storitev v oblaku k drugemu ali nazaj v podjetje;
vi. politične stabilnosti, varnostnih razmer in pravnega sistema (vključno z veljavnimi določbami o kazenskem pregonu, določbami insolvenčnega prava, ki bi se uporabljale v primeru stečaja ponudnika storitev v oblaku, veljavnimi zakoni o varstvu podatkov in tem, ali so izpolnjeni pogoji za prenos osebnih podatkov v tretjo državo v skladu s Splošno uredbo o varstvu podatkov) držav (znotraj ali zunaj EU), v katerih bi se zagotavljale funkcije, oddane zunanjemu izvajalcu, in v katerih bi bili shranjeni podatki, oddani zunanjemu izvajalcu; v primeru zunanjega podizvajanja dodatnih tveganj, ki se lahko pojavijo, če je lokacija zunanjega podizvajalca v tretji državi ali državi, ki se razlikuje od države ponudnika storitev v oblaku, in v primeru verige zunanjega podizvajanja vsakega dodatnega tveganja, ki se lahko pojavi, tudi v zvezi z odsotnostjo neposredne pogodbe med podjetjem in zunanjim podizvajalcem, ki opravlja funkcijo, oddano zunanjemu izvajalcu;
vii. morebitne koncentracije v podjetju (če je ustrezno, tudi na ravni njegove skupine), ki jo povzroči več dogovorov o zunanjem izvajanju storitev v oblaku z istim ponudnikom storitev v oblaku, in morebitne koncentracije v finančnem sektorju EU, ki jo povzroči več podjetij, ki uporabljajo istega ponudnika storitev v oblaku ali majhno skupino ponudnikov storitev v oblaku. Pri ocenjevanju tveganja koncentracije bi moralo podjetje upoštevati vse svoje dogovore o zunanjem izvajanju storitev v oblaku (in, če je ustrezno, dogovore o zunanjem izvajanju storitev v oblaku na ravni svoje skupine) z navedenim ponudnikom storitev v oblaku;

b) upoštevati pričakovane koristi in stroške dogovora o zunanjem izvajanju storitev v oblaku, pri čemer bi bilo treba pretehtati vsa bistvena tveganja, ki bi se lahko zaradi dogovora o zunanjem izvajanju storitev v oblaku zmanjšala ali bolje obvladovala, skupaj z vsemi bistvenimi tveganji, ki bi lahko zaradi navedenega dogovora nastala.

22. V primeru zunanjega izvajanja funkcij odločilnega pomena ali pomembnih funkcij bi moral skrbni pregled vključevati oceno primernosti ponudnika storitev v oblaku. Pri oceni primernosti ponudnika storitev v oblaku bi moralo podjetje zagotoviti, da ima ponudnik storitev v oblaku poslovni ugled, sposobnosti, vire (vključno s človeškimi, IT in finančnimi), organizacijsko strukturo in, če je to ustrezno, ustrezna dovoljenja ali registracijske prijave za zanesljivo in strokovno izvajanje funkcije odločilnega pomena

ali pomembne funkcije ter izpolnjevanje svojih obveznosti v celotnem obdobju veljavnosti dogovora o zunanjem izvajanju storitev v oblaku. Dodatni dejavniki, ki jih je treba upoštevati pri skrbnem pregledu ponudnika storitev v oblaku, med drugim vključujejo:

a) upravljanje informacijske varnosti in zlasti varstvo osebnih, zaupnih ali drugače občutljivih podatkov;
b) podporo za storitve, vključno z načrti in kontaktnimi osebami za podporo, ter postopke obvladovanja incidentov;
c) načrte za neprekinjeno poslovanje in vnovično vzpostavitev delovanja po nepredvidljivih dogodkih.

23. Kadar je to primerno in kot podporo opravljenemu skrbnemu pregledu, lahko podjetje uporabi tudi certifikate, ki temeljijo na mednarodnih standardih in zunanjih ali notranjih revizijskih poročilih.

24. Če podjetje izve za znatne pomanjkljivosti in/ali bistvene spremembe zagotovljenih storitev ali položaja ponudnika storitev v oblaku, bi moralo analizo pred zunanjim izvajanjem in skrbni pregled ponudnika storitev v oblaku nemudoma preveriti ali po potrebi znova izvesti.

25. Če podjetje sklene nov dogovor ali obnovi obstoječi dogovor s ponudnikom storitev v oblaku, ki je že bil ocenjen, bi moralo na podlagi pristopa, ki temelji na tveganju, ugotoviti, ali je potreben nov skrbni pregled.

Smernica 3. Ključni pogodbeni elementi

26. Ustrezne pravice in obveznosti podjetja in ponudnika storitev v oblaku se jasno opredelijo v pisnem sporazumu.

27. Pisni sporazum bi moral podjetju izrecno omogočati, da podjetje po potrebi od njega odstopi.

28. V primeru zunanjega izvajanja funkcij odločilnega pomena ali pomembnih funkcij bi moral pisni sporazum vključevati vsaj:

a) jasen opis funkcije, oddane zunanjemu izvajalcu;
b) datum začetka in, kjer je ustrezno, datum prenehanja sporazuma ter odpovedne roke za ponudnika storitev v oblaku in podjetje;
c) veljavno pravo sporazuma in, če obstaja, izbiro pristojnosti;
d) finančne obveznosti podjetja in ponudnika storitev v oblaku;
e) določbo, ali je zunanje podizvajanje dovoljeno, in če je dovoljeno, pod katerimi pogoji, ob upoštevanju smernice 7;
f) lokacijo (ali lokacije) (tj. regije ali države), kjer se bodo zagotavljale funkcije, oddane zunanjemu izvajalcu, in se bodo obdelovali in hranili podatki, ter pogoji, ki

jih je treba izpolniti, vključno z zahtevo, da mora ponudnik storitev v oblaku obvestiti podjetje, če namerava zamenjati lokacijo (ali lokacije);

g) določbe o informacijski varnosti in varstvu osebnih podatkov, ob upoštevanju smernice 4;

h) pravico podjetja, da redno spremlja uspešnost ponudnika storitev v oblaku v okviru dogovora o zunanjem izvajanju storitev v oblaku, ob upoštevanju smernice 6;

i) dogovorjene ravni storitve, ki bi morale vključevati kvantitativne in kvalitativne cilje uspešnosti, da se omogoči pravočasno spremljanje, na podlagi katerega se lahko brez nepotrebnega odlašanja sprejmejo ustrezni popravni ukrepi, če dogovorjene ravni storitve niso dosežene;

j) obveznosti ponudnika storitev v oblaku glede poročanja podjetju in po potrebi obveznosti predložitve poročil, ki so pomembna za varnostno funkcijo podjetja in ključne funkcije, kot so poročila, ki jih pripravi funkcija notranje revizije ponudnika storitev v oblaku;

k) določbe v zvezi z obvladovanjem incidentov pri ponudniku storitev v oblaku, vključno z obveznostjo ponudnika storitev v oblaku, da podjetju brez nepotrebnega odlašanja poroča o incidentih, ki so vplivali na izvajanje pogodbenih storitev podjetja;

l) določbo, ali bi moral ponudnik storitev v oblaku skleniti obvezno zavarovanje za primer nekaterih tveganj in, če je to ustrezno, stopnjo zahtevanega zavarovalnega kritja;

m) zahteve, da mora ponudnik storitev v oblaku izvesti in preizkusiti načrte za neprekinjeno poslovanje in vnovično vzpostavitev delovanja po nepredvidljivih dogodkih;

n) zahtevo, da ponudnik storitev v oblaku podjetju, njegovim pristojnim organom in kateri koli drugi osebi, ki jo imenuje podjetje ali pristojni organi, podeli pravico dostopa do (pravice dostopa) in pregleda (pravice do revizije) ustreznih informacij, prostorov, sistemov in naprav ponudnika storitev v oblaku v obsegu, ki je potreben za spremljanje uspešnosti ponudnika storitev v oblaku v okviru dogovora o zunanjem izvajanju storitev v oblaku in njegove skladnosti z veljavnimi regulativnimi in pogodbenimi zahtevami, ob upoštevanju smernice 6;

o) določbe, ki zagotavljajo, da se lahko podatki, ki jih ponudnik storitev v oblaku obdela ali hrani v imenu podjetja, po potrebi pridobijo, obnovijo in vrnejo podjetju, ob upoštevanju smernice 5.

Smernica 4. Informacijska varnost

29. Podjetje bi moralo v svojih notranjih pravilnikih in postopkih ter v okviru pisnega sporazuma o zunanjem izvajanju storitev v oblaku določiti zahteve glede informacijske varnosti in stalno spremljati skladnost s temi zahtevami, vključno z varstvom zaupnih, osebnih ali drugih občutljivih podatkov. Te zahteve bi morale biti sorazmerne z naravo,

obsegom in zapletenostjo funkcije, ki jo podjetje odda zunanjemu izvajalcu ponudnika storitev v oblaku, ter tveganji, povezanimi s to funkcijo.

30. V ta namen bi moralo podjetje v primeru zunanjega izvajanja funkcij odločilnega pomena ali pomembnih funkcij in brez poseganja v veljavne zahteve iz Splošne uredbe o varstvu podatkov z uporabo pristopa na podlagi tveganj vsaj:

a) *organizacija informacijske varnosti:* zagotoviti jasno razdelitev vlog in odgovornosti na področju informacijske varnosti med podjetjem in ponudnikom storitev v oblaku, tudi v zvezi z odkrivanjem groženj, obvladovanjem incidentov in upravljanjem popravkov, ter zagotoviti, da je ponudnik storitev v oblaku sposoben učinkovito izpolnjevati svoje vloge in odgovornosti;
b) *upravljanje identitete in dostopa:* zagotoviti, da so vzpostavljeni močni mehanizmi avtentikacije (na primer večfaktorska avtentikacija) in kontrole dostopa, da se prepreči nepooblaščen dostop do podatkov podjetja in zalednih virov v oblaku;
c) *upravljanje šifriranja in ključev:* zagotoviti, da se po potrebi uporabljajo ustrezne tehnologije šifriranja za podatke v tranzitu, podatke v pomnilniku, podatke v mirovanju in varnostne kopije podatkov v kombinaciji z ustreznimi rešitvami upravljanja ključev, da se omeji tveganje nepooblaščenega dostopa do šifrirnih ključev; podjetje bi moralo pri izbiri rešitve za upravljanje ključev zlasti upoštevati najsodobnejšo tehnologijo in postopke;
d) *varnost operacij in omrežja:* upoštevati ustrezne ravni razpoložljivosti omrežja, ločevanja omrežja (na primer izolacija najemnikov v okolju oblaka v skupni rabi, operativno ločevanje v zvezi s spletom, aplikacijska logika, operacijski sistem, omrežje, sistem za upravljanje podatkovnih baz (DBMS) in plasti shranjevanja) in okolja za obdelavo (na primer preskus, uporabniški test sprejemljivosti, razvoj, produkcija);
e) *vmesniki za aplikacijsko programiranje (API):* razmisliti o mehanizmih za povezovanje storitev v oblaku s sistemi podjetja, da se zagotovi varnost vmesnikov za aplikacijsko programiranje (na primer vzpostavitev in vzdrževanje pravilnikov in postopkov za informacijsko varnost za vmesnike API v več sistemskih vmesnikih, pristojnostih in poslovnih funkcijah, da se prepreči nepooblaščeno razkritje, spreminjanje ali uničenje podatkov);
f) *neprekinjeno poslovanje in vnovična vzpostavitev delovanja po nepredvidljivih dogodkih:* zagotoviti, da so vzpostavljene učinkovite kontrole glede neprekinjenega poslovanja in vnovične vzpostavitve delovanja po nepredvidljivih dogodkih (na primer z določitvijo minimalnih zahtev glede zmogljivosti, izbiro geografsko razporejenih možnosti gostovanja, z možnostjo prehoda z ene na drugo, ali zahtevo za pridobitev in pregledom dokumentacije, iz katere je razvidna pot prenosa podatkov podjetja med sistemi ponudnika storitev v oblaku, ter preučitvijo možnosti za kopiranje slik virtualnega okolja na neodvisno lokacijo za shranjevanje, ki je dovolj izolirana iz omrežja ali prenesena na mesto brez povezave);-
g) *lokacija podatkov:* sprejeti pristop na podlagi tveganj k lokaciji (ali lokacijam) (tj. regijam ali državam) shranjevanja in obdelave podatkov;
h) *skladnost in spremljanje:* preveriti, ali ponudnik storitev v oblaku dosega mednarodno priznane standarde informacijske varnosti in ali izvaja ustrezne

kontrole glede informacijske varnosti (na primer tako, da od ponudnika storitev v oblaku zahteva, da predloži dokaze o izvajanju ustreznih pregledov informacijske varnosti, ter o izvajanju redne ocene in preizkuse dogovorov ponudnika storitev v oblaku o informacijski varnosti).

Smernica 5. Strategije izstopa

31. V primeru oddajanja funkcij odločilnega pomena ali pomembnih funkcij v zunanje izvajanje bi moralo podjetje zagotoviti, da lahko izstopi iz dogovora o zunanjem izvajanju storitev v oblaku brez nepotrebnih motenj za poslovne dejavnosti in storitve za svoje stranke ter brez škode za izpolnjevanje obveznosti v skladu z veljavno zakonodajo, pa tudi zaupnost, celovitost in razpoložljivost svojih podatkov. V ta namen bi moralo podjetje:

    a) oblikovati načrte izstopa, ki so celoviti, dokumentirani in ustrezno preizkušeni. Navedene načrte bi bilo treba po potrebi posodobiti, tudi v primeru sprememb funkcije, oddane zunanjemu izvajalcu;
    b) opredeliti nadomestne rešitve in razviti prehodne načrte za odstranitev funkcije, oddane zunanjemu izvajalcu, in podatkov od ponudnika storitev v oblaku in, kjer je ustrezno, vseh zunanjih podizvajalcev ter jih prenesti na nadomestnega ponudnika storitev v oblaku, ki ga navede podjetje, ali neposredno nazaj podjetju. Navedene 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 pisni sporazum o zunanjem izvajanju storitev v oblaku vključuje obveznost za ponudnika storitev v oblaku, da podpira urejen prenos funkcije, oddane zunanjemu izvajalcu, in s tem povezane obdelave podatkov od ponudnika storitev v oblaku in vseh zunanjih podizvajalcev k drugemu ponudniku storitev v oblaku, ki ga navede podjetje, ali neposredno podjetju, če podjetje sproži strategijo izstopa. Obveznost podpore urejenemu prenosu funkcije, oddane zunanjemu izvajalcu, in s tem povezane obdelave podatkov bi morala po potrebi vključevati varen izbris podatkov iz sistemov ponudnika storitev v oblaku in vseh zunanjih podizvajalcev.

32. Pri pripravi načrtov izstopa in rešitev iz točk (a) in (b) zgoraj („strategija izstopa“) bi moralo podjetje upoštevati naslednje:

    a) opredeliti cilje strategije izstopa;
    b) opredeliti sprožilne dogodke, ki bi lahko aktivirali strategijo izstopa. To bi moralo vključevati vsaj prekinitev dogovora o zunanjem izvajanju storitev v oblaku na pobudo podjetja ali ponudnika storitev v oblaku in neizvajanje ali drugo resno prenehanje poslovne dejavnosti ponudnika storitev v oblaku;
    c) opraviti analizo učinka na poslovanje, sorazmerno s funkcijo, oddano zunanjemu izvajalcu, s katero bi ugotovilo, kakšne človeške in druge vire bi potrebovalo za izvedbo strategije izstopa;
    d) dodeliti vloge in odgovornosti za upravljanje strategije izstopa;

e) preizkusiti primernost strategije izstopa z uporabo pristopa na podlagi tveganj (npr. z analizo morebitnih stroškov, učinka, virov in časovnih posledic prenosa storitve, oddane zunanjemu izvajalcu, na nadomestnega ponudnika);
f) opredeliti merila uspešnosti prehoda.

33. Podjetje bi moralo v svoje stalno spremljanje in nadzor nad storitvami, ki jih zagotavlja ponudnik storitev v oblaku v okviru dogovora o zunanjem izvajanju storitev v oblaku, vključiti kazalnike sprožilnih dogodkov za strategijo izstopa.

Smernica 6. Pravici do dostopa in revizije

34. Podjetje bi moralo zagotoviti, da pisni sporazum o zunanjem izvajanju storitev v oblaku ne omejuje učinkovitega uveljavljanja pravic podjetja in pristojnega organa do dostopa in revizije ter možnosti nadzora nad ponudnikom storitev v oblaku.

35. Podjetje bi moralo zagotoviti, da se pri uveljavljanju pravic do dostopa in revizije (na primer pogostost revizij ter področja in storitve, ki jih je treba revidirati) upošteva, ali je zunanje izvajanje povezano s funkcijo odločilnega pomena ali pomembno funkcijo ter naravo in obsegom tveganj in učinka, ki izhajajo iz dogovora o zunanjem izvajanju v oblaku za podjetje.

36. Če uveljavljanje pravic do dostopa ali revizije ali uporaba nekaterih revizijskih tehnik pomeni tveganje za okolje ponudnika storitev v oblaku in/ali drugo stranko ponudnika storitev v oblaku (na primer z vplivanjem na ravni storitev, zaupnost, celovitost in razpoložljivost podatkov), bi moral ponudnik storitev v oblaku podjetju zagotoviti jasno utemeljitev, zakaj bi to ustvarilo tveganje, pri čemer bi se moral ponudnik storitev v oblaku s podjetjem dogovoriti o nadomestnih načinih za doseganje podobnega rezultata (na primer vključitev posebnih kontrol, ki jih je treba preizkusiti v posebnem poročilu/certifikat, ki ga zagotovi ponudnik storitev v oblaku).

37. Da bi podjetja učinkoviteje uporabila revizijska sredstva in zmanjšala organizacijsko breme za ponudnika storitev v oblaku in njegove stranke, lahko brez poseganja v svojo končno odgovornost glede dogovorov o zunanjem izvajanju storitev v oblaku uporabijo:

a) certifikate tretjih oseb in zunanja ali notranja revizijska poročila, ki jih zagotovi ponudnik storitev v oblaku;
b) skupne revizije, izvedene skupaj z drugimi strankami istega ponudnika storitev v oblaku, ali skupne revizije, ki jih izvede tretji revizor, ki ga imenuje več strank istega ponudnika storitev v oblaku.

38. V primeru zunanjega izvajanja funkcij odločilnega pomena ali pomembnih funkcij bi moralo podjetje oceniti, ali so certifikati tretjih oseb in zunanja ali notranja revizijska poročila iz odstavka 37(a) ustrezna in zadostna za izpolnjevanje obveznosti iz veljavne zakonodaje, pri čemer bi si podjetje moralo prizadevati, da se sčasoma ne bi zgolj zanašalo na te certifikate in poročila.

39. V primeru zunanjega izvajanja funkcij odločilnega pomena ali pomembnih funkcij bi moralo podjetje certifikate tretjih oseb in zunanja ali notranja revizijska poročila iz odstavka 37(a) uporabiti samo, če se:

    a) prepriča, da področje certifikata oz. revizijskih poročil zajema ključne sisteme ponudnika storitev v oblaku (na primer procese, aplikacije, infrastrukturo, podatkovne centre itd.), ključne kontrole, ki jih opredeli podjetje, in skladnost z ustrezno veljavno zakonodajo;
    b) temeljito in redno ocenjuje vsebino certifikatov ali revizijskih poročil ter se prepriča, da ti certifikati ali poročila niso zastareli;
    c) zagotovi, da so ključni sistemi in kontrole ponudnika storitev v oblaku vključeni v prihodnje različice certifikata ali revizijskih poročil;
    d) prepriča o ustreznosti subjekta za certificiranje ali revizijo (na primer v zvezi z njegovimi kvalifikacijami, strokovnim znanjem, ponovno izvedbo/preverjanjem dokazil v zadevni revizijski dokumentaciji ter menjavo družbe za certificiranje ali revizijo);
    e) prepriča, da se certifikati izdajo in se revizije izvajajo v skladu z ustreznimi standardi ter vključujejo preizkus učinkovitosti vzpostavljenih ključnih kontrol;
    f) ima pogodbeno pravico, da zahteva razširitev področja certifikatov ali revizijskih poročil na druge ustrezne sisteme in kontrole ponudnika storitev v oblaku, pri čemer morata biti število in pogostost takih zahtev za spremembo obsega razumna in upravičena z vidika obvladovanja tveganja;
    g) obdrži pogodbeno pravico za izvajanje posameznih revizij na kraju samem po lastni presoji v zvezi s funkcijo, oddano zunanjemu izvajalcu.

40. Podjetje bi moralo zagotoviti, da pred obiskom na kraju samem, tudi obiskom tretje osebe, ki jo imenuje podjetje (na primer revizorja), ponudnik storitev v oblaku prejme predhodno obvestilo v razumnem roku, razen če zgodnje predhodno obvestilo ni mogoče zaradi izrednih ali kriznih razmer ali bi privedlo do stanja, v katerem revizija ne bi bila več učinkovita. Obvestilo bi moralo vključevati lokacijo in namen obiska ter uslužbence, ki se bodo obiska udeležili.

41. Ker storitve v oblaku predstavljajo visoko raven tehnične kompleksnosti in prinašajo posebne izzive glede pristojnosti, bi moralo imeti osebje, ki opravlja revizijo – kot notranji revizor podjetja ali revizorji, ki delujejo v njegovem imenu – primerne sposobnosti in znanje za ustrezno oceno zadevnih storitev v oblaku ter učinkovito in ustrezno revizijo. To bi moralo veljati tudi za zaposlene v podjetjih, ki pregledujejo certifikate ali revizijska poročila, ki jih zagotovi ponudnik storitev v oblaku.

Smernica 7. Zunanje podizvajanje

42. Če je zunanje podizvajanje funkcij odločilnega pomena ali pomembnih funkcij (ali njihovih pomembnih delov) dovoljeno, bi bilo treba v pisnem sporazumu o zunanjem izvajanju storitev v oblaku med podjetjem in ponudnikom storitev v oblaku:

    a) opredeliti vse dele ali vidike funkcije, oddane v zunanje izvajanje, ki so izključeni iz morebitnega zunanjega podizvajanja;
    b) navesti pogoje, ki jih je treba izpolnjevati v primeru zunanjega podizvajanja;
    c) navesti, da ponudnik storitev v oblaku ostaja odgovoren za storitve, ki jih je oddal v zunanje podizvajanje, in jih mora nadzorovati, da zagotovi neprekinjeno izpolnjevanje vseh pogodbenih obveznosti med sabo in podjetjem;
    d) vključiti obveznost za ponudnika storitev v oblaku, da podjetje obvesti o vsakem nameravanem zunanjem podizvajanju ali njegovih pomembnih spremembah, zlasti kadar bi to lahko vplivalo na zmožnost ponudnika storitev v oblaku, da izpolni svoje obveznosti v okviru dogovora o zunanjem izvajanju storitev v oblaku s podjetjem. Rok za obveščanje, določen v pisnem sporazumu, bi moral podjetju omogočiti dovolj časa vsaj za izvedbo ocene tveganja predlaganega zunanjega podizvajanja ali njegovih pomembnih sprememb ter za nasprotovanje navedenemu ali izrecno odobritev navedenega, kot je navedeno v točki (e) spodaj;
    e) zagotoviti, da ima podjetje pravico nasprotovati nameravanemu zunanjemu podizvajanju ali njegovim pomembnim spremembam ali da je potrebna izrecna odobritev pred začetkom veljavnosti predlaganega zunanjega podizvajanja ali pomembnih sprememb;
    f) zagotoviti, da ima podjetje pogodbeno pravico do prekinitve dogovora o zunanjem izvajanju storitev v oblaku s ponudnikom storitev v oblaku, če nasprotuje predlaganemu zunanjemu podizvajanju ali njegovim pomembnim spremembam, in v primeru neupravičenega zunanjega podizvajanja (na primer, kadar ponudnik storitev v oblaku storitev odda v zunanje podizvajanje, ne da bi o tem obvestil podjetje, ali resno krši pogoje zunanjega podizvajanja, določene v sporazumu o zunanjem izvajanju).

43. Podjetje bi moralo zagotoviti, da ponudnik storitev v oblaku ustrezno nadzoruje zunanjega podizvajalca.

Smernica 8. Pisno obvestilo pristojnim organom

44. Podjetje bi moralo svoj pristojni organ pravočasno pisno obvestiti o načrtovanih dogovorih o zunanjem izvajanju storitev v oblaku, ki zadevajo funkcijo odločilnega pomena ali pomembno funkcijo. Podjetje bi moralo svoj pristojni organ prav tako pravočasno in pisno obvestiti o dogovorih o zunanjem izvajanju storitev v oblaku, ki se nanašajo na funkcijo, ki je bila prej razvrščena kot funkcija, ki ni odločilnega pomena, ali kot nepomembna funkcija in je nato postala funkcija odločilnega pomena ali pomembna funkcija.

45. Pisno obvestilo podjetja bi moralo ob upoštevanju načela sorazmernosti vključevati vsaj naslednje informacije:

    a) datum začetka sporazuma o zunanjem izvajanju storitev v oblaku in, kadar je ustrezno, datum naslednje obnovitve pogodbe, datum prenehanja in/ali odpovedne roke za ponudnika storitev v oblaku in podjetje;
    b) kratek opis funkcije, oddane v zunanje izvajanje;
    c) kratek povzetek razlogov, zakaj se funkcija, oddana v zunanje izvajanje, šteje za funkcijo odločilnega pomena ali pomembno funkcijo;
    d) ime in trgovsko ime (če obstaja) ponudnika storitev v oblaku, matično državo, matično številko družbe, identifikator pravnih subjektov (če je na voljo), registrirani naslov in druge pomembne podatke za stik ter ime nadrejene družbe (če obstaja);
    e) veljavno pravo sporazuma o zunanjem izvajanju storitev v oblaku in, če obstaja, izbiro pristojnosti;
    f) modele uvedbe oblaka in posebno naravo podatkov, ki jih bo hranil ponudnik storitev v oblaku, in lokacije (tj. regije ali države), kjer se bodo taki podatki hranili;
    g) datum najnovejše ocene odločilnega pomena ali pomembnosti funkcije, oddane v zunanje izvajanje;
    h) datum najnovejše ocene tveganja ali revizije ponudnika storitev v oblaku skupaj s kratkim povzetkom glavnih rezultatov in datum naslednje načrtovane ocene tveganja ali revizije;
    i) posameznika ali organ odločanja v podjetju, ki je odobril dogovor o zunanjem izvajanju storitev v oblaku;
    j) kadar je to ustrezno, imena vseh zunanjih podizvajalcev, ki so jim v zunanje podizvajanje oddani pomembni deli funkcije odločilnega pomena ali pomembne funkcije, vključno z državo ali regijo, v kateri so ti zunanji podizvajalci registrirani, kjer bo storitev, oddana v zunanje podizvajanje, opravljena in kjer bodo shranjeni podatki.

Smernica 9. Nadzor nad dogovori o zunanjem izvajanju storitev v oblaku

46. Pristojni organi bi morali v okviru svojega nadzornega postopka oceniti tveganja, ki izhajajo iz dogovorov podjetij o zunanjem izvajanju storitev v oblaku. Ta ocena bi morala biti osredotočena zlasti na dogovore, ki se nanašajo na zunanje izvajanje funkcij odločilnega pomena ali pomembnih funkcij.

47. Pristojni organi bi se morali prepričati, da so sposobni izvajati učinkovit nadzor, zlasti če podjetja v zunanje izvajanje oddajo funkcije odločilnega pomena ali pomembne funkcije, ki se izvajajo zunaj EU.

48. Pristojni organi bi morali na podlagi pristopa na podlagi tveganj oceniti, ali:

    a) imajo podjetja vzpostavljene ustrezno upravljanje, vire in operativne postopke za ustrezno in učinkovito sklepanje, izvajanje in nadziranje dogovorov o zunanjem izvajanju storitev v oblaku;

b) so podjetja opredelila in obvladujejo vsa pomembna tveganja v zvezi z zunanjim izvajanjem storitev v oblaku.

49. Kadar se ugotovijo tveganja koncentracije, bi morali pristojni organi spremljati razvoj takih tveganj in oceniti njihov morebitni učinek na druga podjetja, ki jih nadzorujejo, ter stabilnost finančnega trga.