30/09/2025
ESMA65-294529287-4737

Smjernice

o izdvajanju poslova pružateljima usluga računalstva u oblaku

Sadržaj

1 Područje primjene

Tko?

1. Ove se smjernice primjenjuju na nadležna tijela i i. depozitare alternativnih investicijskih fondova (AIF-ovi) iz članka 21. stavka 3. točke (c) i članka 21. stavka 3. trećeg podstavka Direktive o UAIF-ovima ako nisu financijski subjekti na koje se primjenjuje DORA i ii. depozitare UCITS-a iz članka 23. stavka 2. točke (c) Direktive o UCITS-ovima ako nisu financijski subjekti na koje se primjenjuje DORA.[1]

Što?

2. Ove se smjernice primjenjuju u odnosu na sljedeće odredbe:

   a) u odnosu na depozitare AIF-ova: članak 21. Direktive o UAIF-ovima; članak 98. Delegirane uredbe Komisije (EU) 2013/231;

   b) u odnosu na depozitare UCITS-a: članak 22., članak 22.a, članak 23. stavak 2. Direktive o UCITS-ovima; članak 32. Direktive Komisije 2010/43/EU; članak 2. stavak 2. točka (j), članak 3. stavak 1., članak 13. stavak 2., članci 15., 16. i 22. Delegirane uredbe Komisije (EU) br. 2016/438.

Kada?

3. Ove se smjernice primjenjuju od datuma njihove objave na ESMA-inim internetskim stranicama na svim službenim jezicima EU-a i na sve ugovore o izdvajanju poslova računalstva u oblaku sklopljene, obnovljene ili izmijenjene na taj datum ili nakon njega.

4. S obzirom na primjenu DORA-e, prethodne Smjernice ESMA-e o izdvajanju poslova računalstva u oblaku prestaju se primjenjivati na financijske subjekte koji podliježu DORA-i iz članka 2. te Uredbe. Za depozitare AIF-ova i depozitare UCITS-a iz stavka 1. prethodne Smjernice ESMA-e o izdvajanju poslova računalstva u oblaku nastavit će se primjenjivati do datuma objave ovih smjernica na internetskim stranicama ESMA-e na svim službenim jezicima EU-a.

[1] U vezi s ugovorima o korištenju usluga u oblaku, financijske institucije kako su definirane u članku 2. stavcima 1. i 2. Uredbe (EU) 2022/2554 Europskog parlamenta i Vijeća o digitalnoj operativnoj otpornosti za financijski sektor i o izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (Uredba DORA) podliježu posebnim pravilima utvrđenima u Uredbi DORA i povezanim delegiranim i provedbenim uredbama Komisije.

2 Zakonodavni referentni dokumenti, pokrate i definicije

2.1 Zakonodavni referentni dokumenti

Uredba o ESMA-i	Uredba (EU) br. 1095/2010 Europskog parlamenta i Vijeća od 24. studenoga 2010. o osnivanju europskog nadzornog tijela (Europskog nadzornog tijela za vrijednosne papire i tržišta kapitala), izmjeni Odluke br. 716/2009/EZ i stavljanju izvan snage Odluke Komisije 2009/77/EZ[2]
Direktiva o UAIF-ovima	Direktiva 2011/61/EU Europskog parlamenta i Vijeća od 8. lipnja 2011. o upraviteljima alternativnih investicijskih fondova i o izmjeni direktiva 2003/41/EZ i 2009/65/EZ te uredbi (EZ) br. 1060/2009 i (EU) br. 1095/2010[3]
Delegirana uredba Komisije (EU) br. 231/2013	Delegirana uredba Komisije (EU) br. 231/2013 od 19. prosinca 2012. o dopuni Direktive 2011/61/EU Europskog parlamenta i Vijeća u odnosu na izuzeća, opće uvjete poslovanja, depozitare, financijsku polugu, transparentnost i nadzor[4]
Direktiva o UCITS-ovima	Direktiva 2009/65/EZ Europskog parlamenta i Vijeća od 13. srpnja 2009. o usklađivanju zakona i drugih propisa u odnosu na subjekte za zajednička ulaganja u prenosive vrijednosne papire (UCITS)[5]
Direktiva Komisije 2010/43/EU	Direktiva Komisije 2010/43/EU od 1. srpnja 2010. o provedbi Direktive 2009/65/EZ Europskog parlamenta i Vijeća u pogledu organizacijskih zahtjeva, sukoba interesa, poslovanja, upravljanja rizicima i sadržaja sporazuma između depozitara i društva za upravljanje[6]
DORA	Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011[7]

[2] SL L 331, 15.12.2010., str. 84.
[3] SL L 174, 1.7.2011., str. 1.
[4] SL L 83, 22.3.2013., str. 1.
[5] SL L 302, 17.11.2009., str. 32.
[6] SL L 176, 10.7.2010., str. 42.
[7] *SL L 333, 27.12.2022., str. 1.–79.*

Opća uredba o zaštiti podataka	Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ[8]

2.2 Pokrate

CSP	pružatelj usluga računalstva u oblaku
ESMA	Europsko nadzorno tijelo za vrijednosne papire i tržišta kapitala
EU	Europska unija

2.3 Definicije

funkcija	znači sve postupke, usluge ili aktivnosti;
ključna ili važna funkcija	znači sve funkcije čije bi nepravilno ili neuspješno izvršavanje znatno naštetilo: a) ispunjavanju obveza društva na temelju primjenjivog zakonodavstva; b) financijskim rezultatima društva; ili c) stabilnosti ili kontinuitetu glavnih usluga i aktivnosti društva;
usluge računalstva u oblaku	znači usluge koje se pružaju primjenom računalstva u oblaku;
računalstvo u oblaku ili oblak[9]	znači paradigma za omogućivanje mrežnog pristupa nadogradivom i elastičnom skupu djeljivih fizičkih ili virtualnih resursa (primjerice poslužitelji, operacijski sustavi, mreže, softver, aplikacije i oprema za pohranu) uz samoposluživanje i administraciju na zahtjev;

[8] SL L 119, 4.5.2016., str. 1.–88.
[9] Za računalstvo u oblaku često se upotrebljava skraćeni naziv „oblak”. Radi lakšeg snalaženja u ostatku ovog dokumenta upotrebljava se izraz „oblak”.

pružatelj usluga računalstva u oblaku	znači treća strana koja pruža usluge računalstva u oblaku na temelju ugovora o izdvajanju poslova računalstva u oblaku;
ugovor o izdvajanju poslova računalstva u oblaku	znači bilo koji oblik ugovora, među ostalim o delegiranju poslova, između: (i) društva i pružatelja usluga računalstva u oblaku, na temelju kojega taj pružatelj usluga računalstva u oblaku obavlja funkciju koju bi inače društvo samo obavljalo; ili (ii) društva i treće strane koja nije pružatelj usluga računalstva u oblaku, ali se u velikoj mjeri oslanja na takvog pružatelja usluga računalstva u oblaku pri obavljanju funkcije koju bi inače društvo samo obavljalo. U ovom slučaju, upućivanje na „pružatelja usluga računalstva u oblaku" u ovim smjernicama trebalo bi tumačiti kao upućivanje na takvu treću stranu;
podizdvajanje poslova	znači situacija u kojoj pružatelj usluga računalstva u oblaku dalje prenosi izdvojenu funkciju (ili njezin dio) drugom pružatelju usluga na temelju ugovora o izdvajanju poslova;
model uporabe oblaka	znači mogući način organizacije oblaka na temelju kontrole i dijeljenja fizičkih ili virtualnih resursa. Modeli uporabe oblaka uključuju zajednički[10], hibridni[11], privatni[12] i javni[13] oblak;
društva	a) depozitari iz članka 21. stavka 3. točke (c) i članka 21. stavka 3. trećeg podstavka Direktive o UAIF-ovima („depozitari alternativnih investicijskih fondova (AIF-ova)"); b) depozitari iz članka 23. stavka 2. točke (c) Direktive o UCITS-ovima („depozitari UCITS-a").

[10] Model uporabe oblaka u kojem usluge računalstva u oblaku isključivo upotrebljava i dijeli posebna skupina korisnika usluga računalstva u oblaku sa zajedničkim zahtjevima i uzajamnim odnosom i u kojem resurse kontrolira najmanje jedan član skupine.
[11] Model uporabe oblaka koji uključuje najmanje dva različita modela uporabe oblaka.
[12] Model uporabe oblaka u kojem samo jedan korisnik usluga računalstva u oblaku upotrebljava te usluge i kontrolira resurse.
[13] Model uporabe oblaka u kojem su usluge računalstva u oblaku potencijalno dostupne svim korisnicima takvih usluga, a resurse kontrolira pružatelj usluga računalstva u oblaku.

3 Svrha

5. Ove se smjernice temelje na članku 16. stavku 1. Uredbe o ESMA-i. Cilj im je uspostaviti dosljedne, učinkovite i djelotvorne nadzorne prakse u okviru Europskog sustava financijskog nadzora (u daljnjem tekstu: ESFS) te osigurati zajedničku, ujednačenu i dosljednu primjenu zahtjeva iz odjeljka 1.1. pod naslovom „Što?" u slučaju izdvajanja poslova društva pružateljima usluga računalstva u oblaku. Konkretno, cilj je ovih smjernica pomoći društvima i nadležnim tijelima da utvrde, riješe i prate rizike i probleme koji proizlaze iz ugovorâ o izdvajanju poslova računalstva u oblaku, od donošenja odluke o izdvajanju poslova, odabira pružatelja usluga računalstva u oblaku, praćenja izdvojenih aktivnosti do osiguravanja izlaznih strategija.

4 Obveze usklađivanja i izvješćivanja

4.1 Status smjernica

6. U skladu s člankom 16. stavkom 3. Uredbe o ESMA-i nadležna tijela i društva moraju ulagati napore da se usklade s ovim smjernicama.

7. Nadležna tijela na koja se ove smjernice primjenjuju trebala bi se s njima uskladiti tako da ih na odgovarajući način ugrade u svoje nacionalne pravne i/ili nadzorne okvire, čak i kad se određene smjernice prvenstveno odnose na društva. U tom bi slučaju nadležna tijela trebala putem nadzora osigurati da društva poštuju smjernice.

4.2 Zahtjevi izvješćivanja

8. U roku od dva mjeseca od datuma objave smjernica na ESMA-inim službenim stranicama na svim službenim jezicima EU-a nadležna tijela na koja se ove smjernice primjenjuju moraju obavijestiti ESMA-u o tome i. jesu li usklađena sa smjernicama, ii. da nisu usklađena, no namjeravaju se uskladiti sa smjernicama ili iii. da nisu usklađena i ne namjeravaju se uskladiti sa smjernicama.

9. U slučaju neusklađenosti nadležna tijela moraju obavijestiti ESMA-u i o razlozima neusklađenosti sa smjernicama, i to u roku od dva mjeseca od objave smjernica na ESMA-inim službenim stranicama na svim službenim jezicima EU-a. Obrazac za obavješćivanje dostupan je na ESMA-inim službenim stranicama. Nakon ispunjavanja obrazac se šalje ESMA-i.

10. Društva nisu obvezna izvješćivati o usklađenosti s ovim smjernicama

5 Smjernice o izdvajanju poslova pružateljima usluga računalstva u oblaku

Smjernica 1. Upravljanje, nadzor i dokumentiranje

11. Društvo bi trebalo imati definiranu i ažuriranu strategiju za izdvajanje poslova računalstva u oblaku, koja je usklađena s relevantnim strategijama te unutarnjim politikama i postupcima društva, među ostalim u pogledu informacijske i komunikacijske tehnologije, informacijske sigurnosti i upravljanja operativnim rizicima.

12. Društvo bi trebalo:

    a) jasno dodijeliti odgovornosti unutar organizacije za dokumentiranje i kontrolu ugovora o izdvajanju poslova računalstva u oblaku te za upravljanje tim ugovorima;
    b) dodijeliti dovoljna sredstva kako bi se zajamčila usklađenost s ovim smjernicama i svim pravnim zahtjevima koji se primjenjuju na njegove ugovore o izdvajanju poslova računalstva u oblaku;
    c) uspostaviti funkciju nadzora izdvajanja poslova računalstva u oblaku ili imenovati članove rukovodećeg osoblja koji izravno odgovaraju upravljačkom tijelu i odgovorni su za nadzor rizika koji proizlaze iz ugovorâ o izdvajanju poslova računalstva u oblaku i upravljanje tim rizicima. Društva bi pri usklađivanju s ovom smjernicom trebala uzeti u obzir prirodu, opseg i složenost svojeg poslovanja, među ostalim u odnosu na rizike za financijski sustav i rizike svojstvene izdvojenim funkcijama, te osigurati da njihovo upravljačko tijelo raspolaže potrebnim tehničkim vještinama i da razumije rizike koji proizlaze iz ugovorâ o izdvajanju poslova računalstva u oblaku. Mala i manje složena društva trebala bi osigurati najmanje jasnu podjelu zadaća i odgovornosti za nadzor nad ugovorima o izdvajanju poslova računalstva u oblaku i upravljanje njima.

13. Društvo bi trebalo pratiti obavljanje aktivnosti, sigurnosne mjere i poštovanje dogovorenih razina usluga pružatelja usluga računalstva u oblaku. Praćenje bi se trebalo temeljiti na riziku te bi u prvom redu trebalo biti usmjereno na izdvojene ključne ili važne funkcije.

14. Društvo bi trebalo periodično i pri svakoj bitnoj promjeni rizika, prirode ili opsega izdvojene funkcije ponovno procijeniti odnose li se njegovi ugovori o izdvajanju poslova računalstva u oblaku na ključnu ili važnu funkciju.

15. Društvo bi trebalo voditi ažuran registar informacija o svim ugovorima o izdvajanju poslova računalstva u oblaku, i to odvojeno za izdvajanje ključnih ili važnih funkcija te za druge ugovore o izdvajanju. Prilikom razlikovanja između izdvajanja ključnih ili važnih funkcija i drugih ugovora o izdvajanju poslova društvo bi trebalo sažeto iznijeti razloge zbog kojih se izdvojena funkcija smatra ili ne smatra ključnom ili važnom.

Uzimajući u obzir nacionalno pravo, društvo bi trebalo tijekom odgovarajućeg vremenskog razdoblja voditi i evidenciju o raskinutim ugovorima o izdvajanju poslova računalstva u oblaku.

16. Za ugovore o izdvajanju poslova računalstva u oblaku koji se odnose na ključne ili važne funkcije, registar bi trebao sadržavati barem sljedeće informacije o svakom ugovoru o izdvajanju poslova računalstva u oblaku:

    a) referentni broj;
    b) datum početka i, ako je primjenjivo, datum sljedećeg produljenja ugovora, datum prestanka ugovora i/ili otkazne rokove za pružatelja usluga računalstva u oblaku i za društvo;
    c) kratak opis izdvojene funkcije, uključujući podatke koji se izdvajaju i napomenu o tome uključuju li ti podatci osobne podatke (primjerice tako da se u posebnom podatkovnom polju označi da ili ne);
    d) kategoriju koju je odredilo društvo i koja odražava prirodu izdvojene funkcije (primjerice funkcija informacijske tehnologije, kontrolna funkcija), čime bi se trebalo olakšati utvrđivanje različitih vrsta ugovora o izdvajanju poslova računalstva u oblaku;
    e) podržava li izdvojena funkcija vremenski kritične poslovne aktivnosti;
    f) naziv i trgovačko ime (ako postoji) pružatelja usluga računalstva u oblaku, zemlju registracije, broj iz registra poslovnih subjekata, identifikacijsku oznaku pravne osobe (ako je dostupna), adresu sjedišta i druge relevantne podatke za kontakt te naziv matičnog društva (ako postoji);
    g) mjerodavno pravo koje se primjenjuje na ugovor o izdvajanju poslova računalstva u oblaku i eventualni izbor sudske nadležnosti;
    h) vrstu usluga u oblaku i modelâ uporabe oblaka, konkretnu prirodu podataka koji se čuvaju i lokacije (regije ili zemlje) na kojima se ti podatci mogu pohranjivati;
    i) datum posljednje ocjene ključnosti ili važnosti izdvojene funkcije i datum sljedeće planirane ocjene;
    j) datum posljednje procjene rizika/revizije pružatelja usluga računalstva u oblaku i kratak sažetak najvažnijih rezultata te datum sljedeće planirane procjene rizika/revizije;
    k) osobu u društvu koja je odobrila ugovor o izdvajanju poslova računalstva u oblaku ili tijelo nadležno za odlučivanje koje je odobrilo takav ugovor;
    l) ako je primjenjivo, imena svih podizvođača kojima je podizdvojena ključna ili važna funkcija (ili njezini bitni dijelovi), uključujući zemlje u kojima su podizvođači registrirani i u kojima se će se pružati podizvojena usluga, te lokacije (regije ili zemlje) na kojima će se podatci pohranjivati;
    m) procjenu godišnjih proračunskih troškova ugovora o izdvajanju poslova računalstva u oblaku.

17. Kada je riječ o ugovorima o izdvajanju poslova računalstva u oblaku koji se odnose na funkcije koje nisu ključne ili važne, informacije koje treba navesti u registru društvo bi

trebalo utvrditi na temelju prirode, opsega i složenosti rizika svojstvenih izdvojenoj funkciji.

Smjernica 2. Analiza i dubinska analiza koje prethode izdvajanju poslova

18. Društvo bi prije sklapanja ugovora o izdvajanju poslova računalstva u oblaku trebalo:

    a) procijeniti odnosi li se ugovor o izdvajanju poslova računalstva u oblaku na ključnu ili važnu funkciju;
    b) utvrditi i procijeniti sve relevantne rizike koji proizlaze iz ugovora o izdvajanju poslova računalstva u oblaku;
    c) provesti odgovarajuću dubinsku analizu potencijalnog pružatelja usluga računalstva u oblaku;
    d) utvrditi i procijeniti sve sukobe interesa koji bi mogli proizaći iz izdvajanja poslova.

19. Analiza i dubinska analiza potencijalnog pružatelja usluga računalstva u oblaku koje prethode izdvajanju poslova trebale bi biti razmjerne prirodi, opsegu i složenosti funkcije koju društvo namjerava izdvojiti i rizicima svojstvenima toj funkciji. Trebale bi uključivati barem procjenu potencijalnog učinka ugovora o izdvajanju poslova računalstva u oblaku na operativne, pravne i reputacijske rizike te rizike usklađenosti društva.

20. Ako se ugovor o izdvajanju poslova računalstva u oblaku odnosi na ključne ili važne funkcije, društvo bi isto tako trebalo:

    a) procijeniti sve relevantne rizike koji mogu proizići iz ugovora o izdvajanju poslova računalstva u oblaku, uključujući rizike koji se odnose na informacijsku i komunikacijsku tehnologiju, informacijsku sigurnost i kontinuitet poslovanja, pravne rizike, rizike usklađenosti, reputacijske i operativne rizike te moguća ograničenja društva u pogledu nadzora koja proizlaze iz:
        i. odabrane usluge računalstva u oblaku i predloženih modela uporabe;
        ii. postupaka premještanja i/ili implementacije;
        iii. osjetljivosti funkcije i povezanih podataka čije se izdvajanje razmatra te sigurnosnih mjera koje bi trebalo poduzeti;
        iv. interoperabilnosti sustava i aplikacija društva i pružatelja usluga računalstva u oblaku, odnosno njihova kapaciteta za razmjenu informacija i zajedničku uporabu razmijenjenih informacija;
        v. prenosivosti podataka društva, odnosno kapaciteta za jednostavan prijenos podataka društva od jednog pružatelja usluga računalstva u oblaku k drugom i zatim natrag u društvo;
        vi. političke stabilnosti, sigurnosnog stanja i pravnog sustava (uključujući važeće odredbe o izvršavanju zakonodavstva, odredbe stečajnog prava koje bi se primjenjivale u slučaju stečaja pružatelja usluga računalstva u

oblaku, važeće zakone o zaštiti podataka te ispunjenost uvjeta za prijenos osobnih podataka u treću zemlju u skladu s Općom uredbom o zaštiti podataka) zemalja (unutar ili izvan EU-a) u kojima bi se obavljale izdvojene funkcije i pohranjivali izdvojeni podatci; u slučaju podizdvajanja, dodatnih rizika koji mogu nastati ako se podizvođač nalazi u trećoj zemlji ili zemlji različitoj od zemlje pružatelja usluga računalstva u oblaku i, u slučaju lanca podizdvajanja, svih eventualnih dodatnih rizika, među ostalim u odnosu na nepostojanje izravnog ugovora između društva i podizvođača koji obavlja izdvojenu funkciju;

vii. moguće koncentracije unutar društva (među ostalim, ako je primjenjivo, na razini njegove grupe) koja bi nastala sklapanjem više ugovora o izdvajanju poslova računalstva u oblaku s istim pružateljem usluga računalstva u oblaku te moguće koncentracije unutar financijskog sektora EU-a koja bi nastala ako bi više društava upotrebljavalo istog pružatelja usluga računalstva u oblaku ili malu skupinu takvih pružatelja. Društvo bi pri procjeni rizika koncentracije trebalo uzeti u obzir sve svoje ugovore o izdvajanju poslova računalstva u oblaku (i, ako je primjenjivo, ugovore o izdvajanju poslova računalstva u oblaku na razini svoje grupe) s predmetnim pružateljem usluga računalstva u oblaku;

b) uzeti u obzir očekivane koristi i troškove ugovora o izdvajanju poslova računalstva u oblaku te prosuditi sve važne rizike koji se mogu smanjiti ili kojima se može bolje upravljati u odnosu na sve važne rizike koji mogu nastati kao posljedica ugovora o izdvajanju poslova računalstva u oblaku.

21. Ako se izdvajaju ključne ili važne funkcije, dubinska analiza trebala bi uključivati evaluaciju primjerenosti pružatelja usluga računalstva u oblaku. Društvo bi pri procjeni primjerenosti pružatelja usluga računalstva u oblaku trebalo osigurati da pružatelj usluga računalstva u oblaku ima dobar poslovni ugled, vještine, resurse (uključujući ljudske, IT i financijske resurse), organizacijsku strukturu i, ako je primjenjivo, relevantna odobrenja ili registracije za pouzdano i profesionalno obavljanje ključne ili važne funkcije te za uredno ispunjavanje svojih obveza tijekom trajanja ugovora o izdvajanju poslova računalstva u oblaku. Dodatni čimbenici koje treba razmotriti pri provedbi dubinske analize pružatelja usluga računalstva u oblaku uključuju, među ostalim:

a) upravljanje informacijskom sigurnošću, a posebno zaštitu osobnih, povjerljivih ili drugih osjetljivih podataka;
b) podršku uslugama, uključujući planove podrške i kontaktne podatke, te postupke za upravljanje incidentima;
c) planove kontinuiteta poslovanja i oporavka u slučaju katastrofe.

22. Prema potrebi te kako bi se potkrijepila provedena dubinska analiza, društvo može upotrebljavati i certifikate koji se temelje na međunarodnim standardima te izvješća vanjske ili unutarnje revizije.

23. Ako društvo primijeti bitne nedostatke i/ili promjene u pogledu pružanih usluga ili situacije u kojoj se nalazi pružatelj usluga računalstva u oblaku, trebalo bi što prije preispitati ili, prema potrebi, ponovno provesti analizu ili dubinsku analizu pružatelja usluga računalstva u oblaku koje su provedene prije izdvajanja poslova.

24. Ako društvo sklapa novi ili produljuje postojeći ugovor s pružateljem usluga računalstva u oblaku za kojega je već obavilo procjenu, trebalo bi primjenom pristupa utemeljenog na riziku utvrditi je li potrebna nova dubinska analiza.

Smjernica 3. Ključni elementi ugovora

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

26. Pisanim ugovorom trebalo bi izričito predvidjeti mogućnost društva da ga po potrebi raskine.

27. Ako se izdvajaju ključne ili važne funkcije, pisani ugovor trebao bi uključivati najmanje:

    a) jasan opis izdvojene funkcije;

    b) datum početka i datum prestanka ugovora, ako je primjenjivo, te otkazne rokove za pružatelja usluga računalstva u oblaku i za društvo;

    c) mjerodavno pravo koje se primjenjuje na ugovor i eventualni izbor sudske nadležnosti;

    d) financijske obveze društva i pružatelja usluga računalstva u oblaku;

    e) je li dopušteno podizdvajanje poslova i, ako jest, pod kojim uvjetima, uzimajući u o obzir smjernicu 7.;

    f) lokacije (odnosno regije ili zemlje) na kojima će se obavljati izdvojena funkcija te obrađivati i pohranjivati podatci te uvjete koje je potrebno ispuniti, uključujući zahtjev za obavješćivanje društva u slučaju da pružatelj usluga računalstva u oblaku predloži promjenu lokacije;

    g) odredbe o informacijskoj sigurnosti i zaštiti osobnih podataka, uzimajući u obzir smjernicu 4.;

    h) pravo društva da redovito prati uspješnost rada pružatelja usluga računalstva u oblaku na temelju ugovora o izdvajanju poslova računalstva u oblaku, uzimajući u obzir smjernicu 6.;

    i) dogovorene razine usluge, što bi trebalo uključivati kvantitativne i kvalitativne ciljeve uspješnosti kako bi se omogućilo pravodobno praćenje te time i poduzimanje odgovarajućih korektivnih mjera bez nepotrebnog odgađanja ako se dogovorena razina usluge ne postigne;

j) obveze pružatelja usluga računalstva u oblaku da izvješćuje društvo i, prema potrebi, obveze podnošenja izvješća relevantnih za sigurnosne i ključne funkcije društva, kao što su izvješća koja izrađuje funkcija unutarnje revizije pružatelja usluga računalstva u oblaku;

k) odredbe o načinu na koji pružatelj usluga računalstva u oblaku upravlja incidentima, uključujući njegovu obvezu da bez nepotrebnog odgađanja društvu podnosi izvješća o incidentima koji utječu na pružanje usluge koju društvo izdvaja;

l) treba li pružatelj usluga računalstva u oblaku ugovoriti obvezno osiguranje od određenih rizika te, ako je primjenjivo, razinu pokrića osiguranja koja se traži;

m) zahtjeve za pružatelja usluga računalstva u oblaku da provodi i testira planove kontinuiteta poslovanja i oporavka u slučaju katastrofe;

n) zahtjev za pružatelja usluga računalstva u oblaku da društvu, njegovim nadležnim tijelima i svim drugim osobama koje imenuje društvo ili njegova nadležna tijela dodijeli pravo pristupa („prava pristupa”) i provjere („prava revizije”) relevantnih informacija, prostorija, sustava i uređaja pružatelja usluga računalstva u oblaku u mjeri u kojoj je to potrebo za praćenje uspješnosti njegova izvršenja ugovora o izdvajanju poslova računalstva u oblaku i njegove usklađenosti s primjenjivim regulatornim i ugovornim zahtjevima, uzimajući u obzir smjernicu 6.;

o) odredbe kojima se osigurava da se, prema potrebi, podatcima koje pružatelj usluga računalstva u oblaku obrađuje ili pohranjuje u ime društva može pristupiti, da se oni mogu obnoviti i vratiti društvu, uzimajući u obzir smjernicu 5.

Smjernica 4. Informacijska sigurnost

28. Društvo bi u svojim internim politikama i procedurama te u okviru pisanog ugovora o izdvajanju poslova računalstva u oblaku trebalo utvrditi zahtjeve u pogledu informacijske sigurnosti i kontinuirano pratiti usklađenost s njima, među ostalim radi zaštite povjerljivih, osobnih i drugih osjetljivih podataka. Ti bi zahtjevi trebali biti razmjerni prirodi, opsegu i složenosti funkcije koju društvo izdvaja pružatelju usluga računalstva u oblaku i rizicima svojstvenima toj funkciji.

29. U tu svrhu, ako se izdvajaju ključne ili važne funkcije i ne dovodeći u pitanje primjenjive zahtjeve iz Opće uredbe o zaštiti podataka, društvo bi, primjenjujući pristup utemeljen na riziku, trebalo najmanje:

a) *organizacija informacijske sigurnosti:* osigurati jasnu podjelu uloga i odgovornosti za informacijsku sigurnost između društva i pružatelja usluga računalstva u oblaku, među ostalim u odnosu na otkrivanje opasnosti te upravljanje incidentima i sigurnosnim zakrpama, te voditi računa o tome da pružatelj usluga računalstva u oblaku može učinkovito ispuniti svoje uloge i odgovornosti;

b) *kontrola identiteta i pristupa*: osigurati uspostavu snažnih mehanizama autentifikacije (primjerice višestruku autentifikaciju) i kontrola pristupa kako bi se spriječio neovlašteni pristup podatcima društva i pozadinskim resursima u oblaku;
c) *upravljanje šifriranjem i ključevima:* osigurati, prema potrebi, primjenu relevantnih tehnologija šifriranja podataka u prijenosu, podataka u memoriji, podataka u mirovanju i sigurnosnih kopija podataka u kombinaciji s odgovarajućim rješenjima za upravljanje ključevima kako bi se ograničio rizik neovlaštenog pristupa ključevima za šifriranje; društvo bi pri odabiru rješenja za upravljanje ključevima osobito trebalo uzeti u obzir najnovije tehnologije i postupke;
d) *sigurnost operacija i mreže:* razmotriti primjerene razine raspoloživosti mreže, razdvajanja mreže (primjerice izolacija zakupnika u zajedničkom okruženju oblaka, operativno razdvajanje u pogledu internetske mreže, aplikacijske logike, operacijskog sustava, mreže, sustava upravljanja bazama podataka i slojeva pohrane) i okruženjâ za obradu (primjerice testiranje, testiranje prihvatljivosti za korisnike, razvoj, produkcija);
e) *aplikacijska programska sučelja (API):* razmotriti mehanizme za integraciju usluga računalstva u oblaku u sustave društva kako bi se osigurala sigurnost API-ja (primjerice uspostavom i održavanjem politika i postupaka informacijske sigurnosti za API-je na više sučelja sustava te u više zemalja i poslovnih funkcija radi sprečavanja neovlaštenog otkrivanja, izmjene ili uništavanja podataka);
f) *kontinuitet poslovanja i oporavak u slučaju katastrofe*: osigurati uspostavu djelotvornih kontrola kontinuiteta poslovanja i oporavka u slučaju katastrofe (primjerice utvrđivanjem zahtjeva u pogledu minimalnih kapaciteta, odabirom zemljopisno udaljenih opcija smještaja uz mogućnost prelaska s jedne na drugu ili traženjem i pregledavanjem dokumentacije koja pokazuje put prijenosa podataka društva u sustavima pružatelja usluga računalstva u oblaku, kao i razmatranjem mogućnosti repliciranja strojnih slika na neovisnoj lokaciji pohrane koja je dovoljno izolirana od mreže ili se nalazi izvan mreže);
g) *lokacija podataka*: primijeniti pristup utemeljen na riziku pri odabiru lokacija (regija ili zemalja) za pohranu i obradu podataka;
h) *usklađenost i praćenje*: provjeriti je li pružatelj usluga računalstva u oblaku usklađen s međunarodno priznatim standardima informacijske sigurnosti te je li uveo prikladne kontrole informacijske sigurnosti (primjerice, zahtijevati od pružatelja usluga računalstva u oblaku da dostavi dokaze o provedbi relevantnih pregleda informacijske sigurnosti i obavljati redovite procjene i testiranja mehanizama informacijske sigurnosti pružatelja usluga računalstva u oblaku).

Smjernica 5. Izlazne strategije

30. U slučaju izdvajanja ključnih ili važnih funkcija društvo bi trebalo osigurati mogućnost raskida ugovora o izdvajanju poslova računalstva u oblaku bez nepotrebnog narušavanja poslovnih aktivnosti i usluga koje pruža klijentima i bez ugrožavanja

usklađenosti s obvezama iz primjenjivog zakonodavstva te povjerljivosti, integriteta i dostupnosti podataka. Društvo bi u tu svrhu trebalo:

a) izraditi izlazne planove koji su sveobuhvatni, dokumentirani i dovoljno testirani. Planove bi trebalo prema potrebi ažurirati, među ostalim u slučaju promjena izdvojene funkcije;
b) utvrditi alternativna rješenja i izraditi prijelazne planove kako bi pružatelju usluga računalstva u oblaku i, ako je primjenjivo, bilo kojem podizvođaču oduzeli izdvojenu funkciju i podatke te ih prenijeli drugom pružatelju usluga računalstva u oblaku kojeg odredi društvo ili izravno natrag društvu. Ta bi rješenja trebalo definirati uzimajući u obzir probleme do kojih može doći zbog lokacije podataka, uz poduzimanje potrebnih mjera za osiguravanje kontinuiteta poslovanja tijekom prijelazne faze;
c) osigurati da pisani ugovor o izdvajanju poslova računalstva u oblaku uključuje obvezu pružatelja usluga računalstva u oblaku da pruži podršku pri pravilnom prijenosu izdvojene funkcije i povezanoj obradi podataka od pružatelja usluga računalstva u oblaku i bilo kojeg podizvođača drugom pružatelju usluga računalstva u oblaku kojeg odredi društvo ili izravno društvu ako ono aktivira izlaznu strategiju. Obveza pružanja podrške pri pravilnom prijenosu izdvojene funkcije i povezanom postupanju s podatcima trebala bi, prema potrebi, uključivati sigurno brisanje podataka iz sustavâ pružatelja usluga računalstva u oblaku i svih podizvođača.

31. Društvo bi pri izradi izlaznih planova i rješenja iz prethodnih točaka (a) i (b) („izlazna strategija”) trebalo:

a) definirati ciljeve izlazne strategije;
b) definirati događaje koji bi mogli dovesti do aktiviranja izlazne strategije. Oni uključuju najmanje raskid ugovora o izdvajanju poslova računalstva u oblaku na inicijativu društva ili pružatelja usluga računalstva u oblaku te kvar ili drugi ozbiljan prestanak poslovnih aktivnosti pružatelja usluga računalstva u oblaku;
c) provesti analizu učinka na poslovanje razmjernu izdvojenoj funkciji kako bi se utvrdilo koji bi ljudski i drugi resursi bili potrebni za provedbu izlazne strategije;
d) dodijeliti uloge i odgovornosti za upravljanje izlaznom strategijom;
e) testirati primjerenost izlazne strategije služeći se pristupom utemeljenim na riziku (primjerice, izraditi analize potencijalnih troškova, učinaka, resursa i vremenskih aspekata prijenosa izdvojene usluge drugom pružatelju usluga);
f) definirati kriterije uspješnosti prijelaza.

32. Društvo bi u svoje kontinuirano praćenje i nadzor usluga koje obavlja pružatelj usluga računalstva u oblaku na temelju ugovora o izdvajanju poslova računalstva u oblaku trebalo uključiti i pokazatelje događaja uslijed kojih se aktivira izlazna strategija.

Smjernica 6. Pravo pristupa i revizije

33. Društvo bi trebalo osigurati da se pisanim ugovorom o izdvajanju poslova računalstva u oblaku ne ograničava ostvarivanje prava društva i nadležnog tijela na pristup i reviziju te njihove mogućnosti nadzora nad pružateljem usluga računalstva u oblaku.

34. Društvo bi trebalo osigurati da se u okviru ostvarivanja prava pristupa i revizije (primjerice, u pogledu učestalosti revizija te područja i usluga koji će se revidirati) uzme u obzir pitanje odnosi li se izdvajanje na ključnu ili važnu funkciju, vrstu i opseg rizikâ te učinak koji ugovor o izdvajanju poslova računalstva u oblaku ima na društvo.

35. Ako ostvarivanje prava pristupa ili revizije ili primjena određenih revizijskih tehnika čine rizik za okruženje pružatelja usluga računalstva u oblaku i/ili drugog klijenta tog pružatelja (primjerice, ako utječu na razine usluge te na povjerljivost, integritet i dostupnost podataka), pružatelj usluga računalstva u oblaku trebao bi društvu dostaviti jasno obrazloženje o tome zašto bi to predstavljalo rizik te bi se trebao dogovoriti s društvom o alternativnim načinima postizanja sličnog rezultata (primjerice, uključivanjem posebnih kontrola koje će se testirati u okviru posebnog izvješća/certifikata pružatelja usluga računalstva u oblaku).

36. Ne dovodeći u pitanje njihovu krajnju odgovornost za ugovore o izdvajanju poslova računalstva u oblaku te kako bi se učinkovitije koristila resursima revizije i smanjila organizacijski teret koji snose pružatelj usluga računalstva u oblaku i njegovi klijenti, društva mogu upotrebljavati:

    a) certifikate trećih strana i izvješća vanjske i unutarnje revizije koje je pružatelj usluga računalstva u oblaku stavio na raspolaganje;
    b) skupne revizije koje provode zajedno s drugim klijentima istog pružatelja usluga računalstva u oblaku ili skupne revizije koje provodi vanjski revizor kojeg je imenovalo više klijenata istog pružatelja usluga računalstva u oblaku.

37. Ako se izdvajaju ključne ili vanjske funkcije, društvo bi trebalo procijeniti jesu li certifikati trećih strana i izvješća vanjske ili unutarnje revizije iz stavka 37. točke (a) primjereni i dovoljni za ispunjavanje obveza iz primjenjivog zakonodavstva te se dugoročno ne bi trebalo oslanjati samo na te certifikate i izvješća.

38. U slučaju izdvajanja ključnih ili važnih funkcija društvo bi se trebalo služiti certifikatima trećih strana i izvješćima vanjske ili unutarnje revizije iz stavka 37. točke (a) samo:

    a) ako se uvjerilo da su opsegom certifikata ili revizorskih izvješća obuhvaćeni ključni sustavi pružatelja usluga računalstva u oblaku (primjerice postupci, aplikacije, infrastruktura, podatkovni centri), ključne kontrole koje je društvo utvrdilo i usklađenost s relevantnim primjenjivim zakonodavstvom;
    b) ako detaljno i redovito ocjenjuje sadržaj certifikata ili revizorskih izvješća te provjerava jesu li zastarjeli;

c) ako osigura da su ključni sustavi i kontrole pružatelja usluga računalstva u oblaku obuhvaćeni budućim verzijama certifikata ili revizorskih izvješća;
d) ako je zadovoljno subjektom koji izdaje certifikat ili obavlja reviziju (primjerice, u pogledu kvalifikacija, stručnosti, ponovnog izvođenja / provjere dokaza u osnovnoj dokumentaciji revizije, kao i rotacije društva koje izdaje certifikat ili obavlja reviziju);
e) ako se uvjerilo da se certifikati izdaju i da se revizije provode u skladu s odgovarajućim standardima te da uključuju testiranje učinkovitosti postojećih ključnih kontrola;
f) ako ima ugovorno pravo zatražiti proširenje opsega certifikata ili revizorskih izvješća na druge relevantne sustave i kontrole pružatelja usluga računalstva u oblaku; broj i učestalost zahtjeva za proširenje opsega trebali bi biti razumni i opravdani sa stajališta upravljanja rizicima;
g) ako zadrži ugovorno pravo provođenja, prema vlastitoj odluci, pojedinačnih neposrednih revizija izdvojene funkcije.

39. Prije neposrednog posjeta, među ostalim i ako ga obavlja treća strana koju je imenovalo društvo (primjerice revizor), društvo bi trebalo osigurati da se pružatelju usluga računalstva u oblaku u razumnom roku dostavi prethodna obavijest osim ako takva obavijest nije moguća zbog izvanrednog ili kriznog stanja ili bi nastala situacija u kojoj revizija više ne bi bila učinkovita. Takva bi obavijest trebala sadržavati informacije o lokaciji, svrsi posjeta i osoblju koje će sudjelovati u posjetu.

40. Budući da usluge računalstva u oblaku podrazumijevaju visoku razinu tehničke složenosti i posebne izazove u pogledu nadležnosti, osoblje koje obavlja reviziju, neovisno o tome je li riječ o unutarnjim revizorima društva ili revizorima koji djeluju u njegovo ime, trebalo bi imati odgovarajuće vještine i znanje za pravilnu ocjenu relevantnih usluga računalstva u oblaku te za provedbu učinkovite i relevantne revizije. To se odnosi i na osoblje društva koje preispituje certifikate ili revizorska izvješća pružatelja usluga računalstva u oblaku.

Smjernica 7. Podizdvajanje

41. Ako je podizdvajanje ključnih ili važnih funkcija (ili njihovih bitnih dijelova) dopušteno, u ugovoru o izdvajanju poslova računalstva u oblaku između društva i pružatelja usluga računalstva u oblaku trebalo bi:

a) utvrditi sve dijelove ili aspekte izdvojene funkcije koji su isključeni iz eventualnog podizdvajanja;
b) navesti uvjete koje je potrebno ispuniti u slučaju podizdvajanja;
c) navesti da je pružatelj usluga računalstva u oblaku odgovoran i obvezan nadzirati usluge koje je podizdvojio kako bi se osiguralo kontinuirano ispunjavanje svih ugovornih obveza pružatelja usluga računalstva u oblaku i društva;
d) uključiti obvezu pružatelja usluga računalstva u oblaku da obavijesti društvo o namjeri podizdvajanja ili bitnim promjenama izdvajanja, osobito ako bi to moglo

utjecati na njegovu sposobnost ispunjavanja obveza iz ugovora o izdvajanju poslova računalstva u oblaku koji je sklopio s društvom. Rokom za obavješćivanje utvrđenim u pisanom ugovoru trebalo bi omogućiti dovoljno vremena društvu da barem provede procjenu rizika predloženog podizdvajanja ili bitnih promjena izdvajanja te da podnese prigovor na njih ili ih izričito odobri, kako je navedeno u točki (e) u nastavku;

e) osigurati da društvo ima pravo podnijeti prigovor na planirano podizdvajanje ili bitne promjene izdvajanja ili da je potrebno izričito odobrenje prije no što predloženo podizdvajanje ili bitne promjene izdvajanja stupe na snagu;

f) osigurati da društvo ima ugovorno pravo raskinuti ugovor o izdvajanju poslova računalstva u oblaku s pružateljem usluga računalstva u oblaku u slučaju podnošenja prigovora na predloženo podizdvajanje ili bitne promjene izdvajanja i u slučaju nepravilnog podizdvajanja (primjerice, ako pružatelj usluga računalstva u oblaku nastavi s podizdvajanjem, a da nije obavijestio društvo ili ako ozbiljno krši uvjete podizdvajanja utvrđene u ugovoru o izdvajanju).

42. Društvo bi trebalo osigurati da pružatelj usluga računalstva u oblaku primjereno nadzire svojeg podizvođača.

Smjernica 8. Obavješćivanje nadležnih tijela u pisanom obliku

43. Društvo bi trebalo pravodobno i u pisanom obliku obavijestiti svoje nadležno tijelo o planiranim ugovorima o izdvajanju poslova računalstva u oblaku koji se odnose na ključnu ili važnu funkciju. Društvo bi trebalo pravodobno i u pisanom obliku obavijestiti svoje nadležno tijelo i o ugovorima o izdvajanju poslova računalstva u oblaku koji se odnose na funkciju koja je, iako prethodno nije bila klasificirana kao takva, u međuvremenu postala ključna ili važna.

44. Uzimajući u obzir načelo proporcionalnosti, pisana obavijest društva trebala bi uključivati najmanje sljedeće informacije:

a) datum početka ugovora o izdvajanju poslova računalstva u oblaku i, prema potrebi, datum sljedećeg produljenja ugovora, datum prestanka ugovora i/ili otkazne rokove za pružatelja usluga računalstva u oblaku i za društvo;

b) kratak opis izdvojene funkcije;

c) kratak sažetak razloga zbog kojih se izdvojena funkcija smatra ključnom ili važnom;

d) naziv i trgovačko ime (ako postoji) pružatelja usluga računalstva u oblaku, zemlju registracije, broj iz registra poslovnih subjekata, identifikacijsku oznaku pravne osobe (ako je dostupna), adresu sjedišta i druge relevantne podatke za kontakt te naziv matičnog društva (ako postoji);

e) mjerodavno pravo koje se primjenjuje na ugovor o izdvajanju poslova računalstva u oblaku i eventualni izbor sudske nadležnosti;

f) modele uporabe oblaka, konkretnu prirodu podataka koje čuva pružatelj usluga računalstva u oblaku i lokacije (regije ili zemlje) na kojima će se ti podatci pohranjivati;
g) datum posljednje procjene ključnosti ili važnosti izdvojene funkcije;
h) datum posljednje procjene rizika ili revizije pružatelja usluga računalstva u oblaku i kratak sažetak najvažnijih rezultata te datum sljedeće planirane procjene rizika ili revizije;
i) osobu u društvu koja je odobrila ugovor o izdvajanju poslova računalstva u oblaku ili tijelo nadležno za odlučivanje koje je odobrilo takav ugovor;
j) ako je primjenjivo, imena svih podizvođača kojima se podizdvajaju značajni dijelovi ključne ili važne funkcije, uključujući zemlju ili regiju u kojoj su registrirani podizvođači, u kojoj će se pružati podizdvojena usluga i u kojoj će se podatci pohranjivati;

Smjernica 9. Nadzor ugovora o izdvajanju poslova računalstva u oblaku

45. Nadležna bi tijela u okviru svojih postupaka nadzora društava trebala procijeniti rizike koji proizlaze iz njihovih ugovorâ o izdvajanju poslova računalstva u oblaku. U procjeni bi naglasak ponajprije trebao biti na ugovorima koji se odnose na izdvajanje ključnih ili važnih funkcija.

46. Nadležna tijela trebala bi se uvjeriti da mogu uspješno provoditi nadzor, posebno kad društva svoje ključne ili važne funkcije izdvajaju izvan EU-a.

47. Nadležna tijela trebala bi, primjenjujući pristup utemeljen na riziku, procijeniti:

a) jesu li društva uspostavila odgovarajuće postupke upravljanja, resurse i operativne postupke za primjereno i učinkovito sklapanje, provedbu i nadzor ugovorâ o izdvajanju poslova računalstva u oblaku;
b) jesu li društva utvrdila sve relevantne rizike povezane s izdvajanjem poslova računalstva u oblaku i upravljaju li tim rizicima.

48. Ako se utvrde rizici koncentracije, nadležna tijela trebala bi pratiti kretanje tih rizika i procijeniti njihov potencijalni utjecaj na druga društva koja nadziru te na stabilnost financijskog tržišta.