30/09/2025
ESMA65-294529287-4737

Suunised

Tegevuse edasiandmine pilveteenuse osutajatele

Sisukord

1 Reguleerimisala....3

2 Viited õigusaktidele, lühendid ja mõisted....4

2.1 Viited õigusaktidele....4

2.2 Lühendid....5

2.3 Mõisted....5

3 Eesmärk....7

4 Järgimis- ja aruandluskohustus....7

4.1 Suuniste staatus....7

4.2 Aruandlusnõuded....7

5 Pilveteenuse osutajatele tegevuse edasiandmise suunised....8

suunis. Juhtimine, järelevalve ja dokumentatsioon....8

2. suunis. Pilveteenuse osutajale tegevuse edasiandmise eelne analüüs ja hoolsuskohustuse audit....10

3. suunis. Lepingu põhielemendid....12

4. suunis. Infoturve....13

5. suunis. Väljumisstrateegiad....14

6. suunis. Juurdepääsu- ja auditeerimisõigused....15

7. suunis. Edasiantud tegevuse edasiandmine....17

8. suunis. Kirjalik teade pädevatele asutustele....18

9. suunis. Pilveteenuse osutajatele tegevuse edasiandmise lepingute järelevalve....19

1 Reguleerimisala

Kellele?

1. Käesolevaid suuniseid kohaldatakse pädevate asutuste ja i) alternatiivsete investeerimisfondide depositooriumide suhtes, millele on osutatud alternatiivsete investeerimisfondide valitsejaid käsitleva direktiivi artikli 21 lõike 3 punktis c ja artikli 21 lõike 3 kolmandas lõigus, kui nad ei ole finantsettevõtjad, kelle suhtes kohaldatakse DORAt, ning ii) eurofondide (UCITS) direktiivi artikli 23 lõike 2 punktis c osutatud eurofondide depositooriumide suhtes, kui nad ei ole finantsettevõtjad, kelle suhtes kohaldatakse DORAt.[1]

Mille alusel?

2. Käesolevaid suuniseid kohaldatakse järgmiste sätete suhtes:

   a) AIFide (alternatiivsete investeerimisfondide) depositooriumide puhul: alternatiivsete investeerimisfondide valitsejaid käsitleva direktiivi artikkel 21; komisjoni delegeeritud määruse (EL) 2013/231 artikkel 98;

   b) Eurofondide depositooriumide puhul: eurofondide direktiivi artiklid 22, 22a ja artikli 23 lõige 2; komisjoni direktiivi 2010/43/EL artikkel 32; Komisjoni delegeeritud määruse (EL) 2016/438 artikli 2 lõike 2 punkt j, artikli 3 lõige 1, artikli 13 lõige 2 ning artiklid 15, 16 ja 22.

Millal?

3. Käesolevaid suuniseid kohaldatakse alates nende avaldamisest ESMA veebisaidil kõigis ELi ametlikes keeltes ja kõigi pilveteenuste allhangete kokkulepete suhtes, mis on sõlmitud, mida on uuendatud või muudetud sellel kuupäeval või pärast seda.

4. Võttes arvesse DORA kohaldamist, lõpetatakse ESMA varasemate suuniste (mis käsitlevad pilveteenuste osutajate allhankeid) kohaldamine nende finantssektori ettevõtjate suhtes, kelle suhtes kohaldatakse sama määruse artiklis 2 osutatud DORAt. Lõikes 1 osutatud AIFide depositooriumide ja eurofondide depositooriumide suhtes kohaldatakse jätkuvalt ESMA varasemaid suuniseid, mis käsitlevad pilveteenuste osutajatega seotud allhankeid, kuni käesolevate suuniste avaldamiseni ESMA veebisaidil kõigis ELi ametlikes keeltes.

[1] Pilveteenuste kasutamise kokkulepete puhul kohaldatakse artikli 2 lõigetes 1 ja 2 määratletud finantsüksustele Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 digitaalset tegevusvastupidavust käsitleva määruse ja määruste (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (DORA määrus) muudatuste suhtes DORA määruses ja komisjoni delegeeritud ning rakendusmäärustes sätestatud erinõudeid.

2 Viited õigusaktidele, lühendid ja mõisted

2.1 Viited õigusaktidele

ESMA määrus	Euroopa Parlamendi ja nõukogu 24. novembri 2010. aasta määrus (EL) nr 1095/2010, millega asutatakse Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve), muudetakse otsust nr 716/2009/EÜ ning tunnistatakse kehtetuks komisjoni otsus 2009/77/EÜ[2]
Alternatiivsete investeerimisfondide valitsejaid käsitlev direktiiv (AIFMD)	Euroopa Parlamendi ja nõukogu 8. juuni 2011. aasta direktiiv 2011/61/EL alternatiivsete investeerimisfondide valitsejate kohta, millega muudetakse direktiive 2003/41/EÜ ja 2009/65/EÜ ning määruseid (EÜ) nr 1060/2009 ja (EL) nr 1095/2010[3]
Komisjoni delegeeritud määrus (EL) nr 2013/231	Komisjoni 19. detsembri 2012. aasta delegeeritud määrus (EL) nr 231/2013, millega täiendatakse Euroopa Parlamendi ja nõukogu direktiivi 2011/61/EL seoses erandite, üldiste tegutsemistingimuste, depositooriumide, finantsvõimenduse, läbipaistvuse ja järelevalvega[4]
Eurofondide direktiiv	Euroopa Parlamendi ja nõukogu 13. juuli 2009. aasta direktiiv 2009/65/EÜ vabalt võõrandatavatesse väärtpaberitesse ühiseks investeeringuks loodud ettevõtjaid (eurofondid) käsitlevate õigus- ja haldusnormide kooskõlastamise kohta[5]
Komisjoni direktiiv 2010/43/EL	Komisjoni 1. juuli 2010. aasta direktiiv 2010/43/EL, millega rakendatakse Euroopa Parlamendi ja nõukogu direktiivi 2009/65/EÜ seoses organisatsiooniliste nõuete, huvide konfliktide, äritegevuse, riskijuhtimise ning depositooriumi ja fondivalitseja vahelise lepingu sisuga[6]
DORA	Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse

[2] ELT L 331, 15.12.2010, lk 84.
[3] ELT L 174, 1.7.2011, lk 1.
[4] ELT L 83, 22.3.2013, lk 1.
[5] ELT L 302, 17.11.2009, lk 32.
[6] ELT L 176, 10.7.2010, lk 42.

	määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011[7]
Isikuandmete kaitse üldmäärus	Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta[8]

2.2 Lühendid

CSP	Pilveteenuse osutaja
ESMA	Euroopa Väärtpaberiturujärelevalve
EL	Euroopa Liit (EL)

2.3 Mõisted

funktsioon	Mis tahes protsessid, teenused või tegevused
kriitiline või oluline funktsioon	Iga funktsioon, mille täitmises esinev viga või mille täitmata jätmine kahjustaks oluliselt: a) kohaldatavatest õigusaktidest tulenevate kohustuste täitmist äriühingu poolt; b) äriühingu finantstulemusi või c) äriühingu peamiste teenuste ja tegevuste usaldusväärsust või järjepidevust.
pilveteenused	Teenused, mille osutamisel kasutatakse pilvandmetöötlust.
pilvandmetöötlus või pilv[9]	See on paradigma, mis võimaldab võrgujuurdepääsu jagatavate füüsiliste või virtuaalsete ressursside (nt serverid, operatsioonisüsteemid, võrgud, tarkvara, rakendused ja salvestusseadmed) skaleeritavale ja

[7] *ELT L 333, 27.12.2022, lk 1–79.*
[8] ELT L 119, 4.5.2016, lk 1–88.
[9] Pilvandmetöötlus on sageli lühendatud kujule „pilv“. Viitamise hõlbustamiseks kasutatakse dokumendi ülejäänud osas terminit „pilv“.

	paindlikule kogumile koos iseteeninduse ja tellitava haldusega.
pilveteenuse osutaja	Kolmas isik, kes osutab pilveteenuseid pilveteenuse osutajatele tegevuse edasiandmise lepingu alusel.
pilveteenuse osutajatele tegevuse edasiandmise leping, edasiandmisleping	Mis tahes vormis kokkulepe, sealhulgas delegeerimisleping, mille sõlmivad: (i) äriühing ja pilveteenuse osutaja ning mille alusel pilveteenuse osutaja täidab funktsiooni, mida muul juhul täidaks äriühing ise või (ii) äriühing ja kolmas isik, kes ei ole pilveteenuse osutaja, kuid kes sõltub olulisel määral pilveteenuse osutajast, et täita funktsiooni, mida muidu täidaks äriühing ise. Sellisel juhul tuleks nendes suunistes olevat viidet pilveteenuse osutajale käsitada viitena sellisele kolmandale isikule.
edasiantud tegevuse edasiandmine	Olukord, kus pilveteenuse osutaja annab edasiantud funktsiooni (või osa sellest funktsioonist) alltöövõtulepingu alusel omakorda teisele teenuseosutajale edasi.
pilve kasutuselevõtumudel	Viis, kuidas pilve võib füüsiliste või virtuaalsete vahendite kontrolli ja jagamise alusel korraldada. Pilve kasutuselevõtumudelid hõlmavad kogukonna-[10], hübriid-[11], privaat-[12] ja avalikke[13] pilvi.

[10] Pilve kasutuselevõtumudel, mille puhul pilveteenuste poolt on toetatud ja neid jagab üksnes selliste pilveteenuste tarbijate rühm, kellel on ühised nõuded ja omavaheline suhe ning mille puhul vahendeid kontrollib vähemalt üks selle rühma liige.
[11] Pilve kasutuselevõtumudel, milles kasutatakse vähemalt kahte erinevat pilve kasutuselevõtumudelit.
[12] Pilve kasutuselevõtumudel, mille puhul pilveteenuseid kasutab ainult üks pilveteenuse klient, kes kontrollib ka vahendeid.
[13] Pilve kasutuselevõtumudel, mille puhul pilveteenused võivad olla kättesaadavad ükskõik millisele pilveteenuse kliendile ja vahendeid kontrollib pilveteenuse osutaja.

äriühingud	a) alternatiivsete investeerimisfondide valitsejaid käsitleva direktiivi artikli 21 lõike 3 punktis c ja kolmandas lõigus osutatud depositooriumid (edaspidi „alternatiivsete investeerimisfondide depositooriumid“); b) eurofondide direktiivi artikli 23 lõike 2 punktis c osutatud depositooriumid („eurofondide depositooriumid”).

3 Eesmärk

5. Käesolevad suunised põhinevad ESMA määruse artikli 16 lõikel 1. Suuniste eesmärk on kehtestada Euroopa Finantsjärelevalve Süsteemis ühtsed, tõhusad ja toimivad järelevalvetavad ning tagada jaos 1.1 „Mille alusel?“ viidatud nõuete ühtne, ühetaoline ja järjepidev kohaldamine juhtudel, kui äriühingud tegevusi pilveteenuse osutajatele edasi annavad. Eelkõige on suuniste eesmärk aidata äriühingutel ja pädevatel asutustel kindlaks teha, käsitleda ja jälgida pilveteenuse osutajatele tegevuse edasiandmise lepingutest tulenevaid riske ja probleeme, alates edasiandmise otsuse tegemisest, pilveteenuse osutaja valimisest ning edasiantud tegevuste järelevalvest kuni väljumisstrateegiate koostamiseni.

4 Järgimis- ja aruandluskohustus

4.1 Suuniste staatus

6. Kooskõlas ESMA määruse artikli 16 lõikega 3 peavad pädevad asutused ja äriühingud tegema kõik endast oleneva, et neid suuniseid järgida.

7. Pädevad asutused, kellele suuniseid kohaldatakse, peaksid neid järgima, lisades suunised asjakohasel viisil oma riiklikesse õigus- ja/või järelevalveraamistikesse, sealhulgas kui teatud suunised on suunatud peamiselt äriühingutele. Käesoleval juhul peaksid pädevad asutused järelevalvetegevuse kaudu tagama, et äriühingud järgivad suuniseid.

4.2 Aruandlusnõuded

8. Pädevad asutused, kellele suuniseid kohaldatakse, peavad kahe kuu jooksul alates suuniste avaldamisest kõigis ELi ametlikes keeltes ESMA veebilehel ESMA-le teatama, kas nad i) järgivad suuniseid, ii) ei järgi suuniseid, kuid kavatsevad järgida, või iii) ei järgi suuniseid ega kavatse neid järgida.

9. Mittejärgimise korral peavad pädevad asutused kahe kuu jooksul pärast seda, kui suunised on avaldatud ESMA veebilehel kõigis ELi ametlikes keeltes, teatama ESMA-le suuniste mittejärgimise põhjused. Teate vorm on ESMA veebilehel. Kui vorm on täidetud, tuleb see edastada ESMA-le.

10. Äriühingud ei pea teatama, kas nad järgivad suuniseid või mitte.

5 Pilveteenuse osutajatele tegevuse edasiandmise suunised

suunis. Juhtimine, järelevalve ja dokumentatsioon

11. Äriühingul peaks olema kindlaksmääratud ja ajakohastatud pilveteenuse osutajatele tegevuse edasiandmise strateegia, mis on kooskõlas äriühingu asjakohaste strateegiate ning sise-eeskirjade ja -menetlustega, sealhulgas seoses info- ja kommunikatsioonitehnoloogia, infoturbe ja tegevusriskide juhtimisega.

12. Äriühing peaks:

    a) määrama selgelt vastutuse pilveteenuse osutajatele tegevuse edasiandmise lepingute dokumenteerimise, haldamise ja kontrolli eest;
    b) eraldama piisavalt vahendeid, et tagada kooskõla nende suuniste ja kõigi õiguslike nõuetega, mida kohaldatakse tema pilveteenuse osutajatele tegevuse edasiandmise lepingute suhtes;
    c) looma pilveteenuse osutajatele tegevuse edasiandmise järelevalvefunktsiooni või määrama kõrgema astme töötajad, kes annavad aru otse juhtorganile ning vastutavad edasiandmislepingutega seotud riskide juhtimise ja järelevalve eest. Seda suunist järgides peaksid äriühingud võtma arvesse oma äritegevuse laadi, ulatust ja keerukust, sealhulgas finantssüsteemile avalduvat riski ja edasiantud funktsioonidega seotud riske, ning tagama, et nende juhtorganil on asjakohased tehnilised oskused, et mõista pilveteenuse osutajatele tegevuse edasiandmise lepingutega kaasnevaid riske. Väikesed ja vähem keerukad äriühingud peaksid tagama pilveteenuse osutajatele tegevuse edasiandmise lepingute haldamisel ja järelevalvel vähemalt ülesannete ja vastutuse selge jaotuse.

13. Äriühing peaks jälgima oma pilveteenuse osutajate tegevust, turvameetmeid ja kokkulepitud teenustaseme järgimist. Järelevalve peaks olema riskipõhine, keskendudes eelkõige kriitilistele või olulistele funktsioonidele, mis on pilveteenuse osutajatele edasi antud.

14. Äriühing peaks perioodiliselt ja alati, kui edasiantud funktsiooni risk, laad või ulatus on oluliselt muutunud, uuesti hindama, kas tema pilveteenuse osutajatele tegevuse edasiandmise lepingud käsitlevad kriitilist või olulist funktsiooni.

15. Äriühing peaks pidama ajakohastatud registrit kõigi pilveteenuse osutajatele tegevuse edasiandmise lepingute teabega, eristades kriitiliste või oluliste funktsioonide edasiandmist muudest edasiandmislepingutest. Kriitiliste või oluliste funktsioonide edasiandmist ja muid edasiandmislepinguid eristades peaks ta esitama lühikokkuvõtte põhjustest, miks pilveteenuse osutajatele edasiantud funktsiooni peetakse või ei peeta kriitiliseks või oluliseks. Samuti peaks äriühing liikmesriigi õigust arvesse võttes säilitama asjakohase ajavahemiku jooksul andmed selliste pilveteenuse osutajatele tegevuse edasiandmise lepingute kohta, mis on lõpetatud.

16. Oluliste või kriitiliste funktsioonidega seotud pilveteenuse osutajatele tegevuse edasiandmise lepingutega seoses peaks register sisaldama iga lepingu kohta vähemalt järgmist teavet:

    a) viitenumber;
    b) lepingu alguskuupäev ja (kui asjakohane) järgmise uuendamise kuupäev, lõppkuupäev ja/või etteteatamistähtajad pilveteenuse osutaja ja äriühingu jaoks;
    c) pilveteenuse osutajatele edasiantud funktsiooni lühikirjeldus, sealhulgas edasiantud andmed ja teave, kas need andmed sisaldavad isikuandmeid (märkides näiteks eraldi andmeväljal „jah“ või „ei“);
    d) äriühingu määratud kategooria, mis näitab pilveteenuse osutajatele edasiantud funktsiooni laadi (nt infotehnoloogia- või kontrollifunktsioon), et oleks lihtsam tuvastada pilveteenuse osutajatele tegevuse edasiandmise lepingute eri liike;
    e) kas edasiantud funktsioon toetab kiireloomulisi äritegevusi;
    f) pilveteenuse osutaja nimi ja kaubamärk (kui olemas), selle registreerimisriik, registreerimisnumber, juriidilise isiku tunnus (kui olemas), registrijärgne aadress, muud asjakohased kontaktandmed ja (kui olemas) emaettevõtte nimi;
    g) pilveteenuse osutajatele tegevuse edasiandmise lepingule kohaldatav õigus ja (kui olemas) kohtualluvuse valik;
    h) pilveteenuste liik ja kasutuselevõtumudelid ning säilitatavate andmete täpsem laad ja asukohad (st piirkonnad või riigid), kus selliseid andmeid võidakse säilitada;
    i) pilveteenuse osutajatele edasiantud funktsiooni kriitilisuse või olulisuse viimase hindamise kuupäev ja järgmise kavandatud hindamise kuupäev;
    j) pilveteenuse osutaja viimase riskihindamise/auditi kuupäev koos peamiste tulemuste lühikokkuvõttega ning järgmise kavandatud riskihindamise/auditi kuupäev;
    k) pilveteenuse osutajatele tegevuse edasiandmise lepingu heakskiitnud üksikisik või otsuseid tegev organ äriühingus;
    l) kui asjakohane, siis alltöövõtjate nimed, kellele kriitiline või oluline funktsioon (või selle olulised osad) edasi anti, sh riigid, kus alltöövõtjad on registreeritud, kus edasiantud teenuseid osutatakse ja asukohad (piirkonnad või riigid), kus andmeid säilitatakse;
    m) pilveteenuse osutajatele tegevuse edasiandmise lepingu hinnanguline eelarvekulu aastas.

17. Mittekriitilisi või väheolulisi funktsioone käsitlevate edasiandmislepingute puhul peaks äriühing määrama kindlaks registrisse kantava teabe, lähtudes edasiantud funktsiooniga seotud riskide laadist, ulatusest ja keerukusest.

2. suunis. Pilveteenuse osutajale tegevuse edasiandmise eelne analüüs ja hoolsuskohustuse audit

18. Enne pilveteenuse osutajatele tegevuse edasiandmise lepingu sõlmimist peaks äriühing:

    a) hindama, kas edasiandmisleping puudutab kriitilist või olulist funktsiooni;
    b) tuvastama kõik pilveteenuse osutajatele tegevuse edasiandmise lepinguga seotud riskid ja neid hindama;
    c) tegema tulevase pilveteenuse osutaja suhtes asjakohase hoolsuskohustuse auditi;
    d) tegema kindlaks ja hindama mis tahes huvide konflikti, mida pilveteenuse osutajatele tegevuse edasiandmine võib põhjustada.

19. Pilveteenuse osutajatele tegevuse edasiandmise eelne analüüs ja tulevase pilveteenuse osutaja hoolsuskohustuse audit peaksid olema proportsionaalsed edasiantava funktsiooni laadi, ulatuse ja keerukusega ning selle funktsiooniga seotud riskidega. See peaks sisaldama vähemalt hinnangut pilveteenuse osutajatele tegevuse edasiandmise lepingu võimaliku mõju kohta äriühingu tegevus-, õigus-, vastavus- ja maineriskidele.

20. Kui pilveteenuse osutajatele tegevuse edasiandmise leping hõlmab kriitilisi või olulisi funktsioone, peaks äriühing samuti:

    a) hindama kõiki asjakohaseid riske, mis võivad tuleneda pilveteenuse osutajatele tegevuse edasiandmise lepingust, sh info- ja kommunikatsioonitehnoloogia, infoturbe ja talitluspidevusega seotud riske, õigus- ja vastavusriske, maineriske, tegevusriske ja võimalike järelevalvepiirangutega seotud riske, mis tulenevad järgmisest:
        i. valitud pilveteenus ja kavandatud kasutuselevõtumudelid;
        ii. andmete migratsioon ja/või rakendusprotsess;
        iii. edasiantava funktsiooni ja sellega seotud andmete tundlikkus ning vajalikud turvameetmed;
        iv. äriühingu ja pilveteenuse osutaja süsteemide ja rakenduste koostalitlusvõime, täpsemalt nende suutlikkus teavet vahetada ja vahetatud teavet vastastikku kasutada;
        v. äriühingu andmete ülekantavus, eelkõige suutlikkus edastada äriühingu andmeid hõlpsalt ühelt pilveteenuse osutajalt teisele ja tagasi äriühingule;
        vi. poliitiline stabiilsus, julgeolekuolukord ja õigussüsteem (sealhulgas kehtivad õiguskaitsesätted, pilveteenuse osutaja pankroti korral kohaldatavad maksejõuetusõiguse sätted, kehtivad andmekaitseseadused ja see, kas

isikuandmete kolmandale riigile edastamise tingimused on isikuandmete kaitse üldmääruse alusel täidetud) riikides (ELis või väljaspool), kus pilveteenuse osutajale edasiantud funktsioone osutatakse ja edasiantud andmeid säilitatakse; edasiantud tegevuse edasiandmise korral lisariskid, mis võivad tekkida, kui alltöövõtja asub kolmandas riigis või pilveteenuse osutajast erinevas riigis, ning edasiantud tegevuse edasiandmise ahela korral mis tahes tekkida võiv lisarisk, sealhulgas seoses otselepingu puudumisega äriühingu ja edasiantud funktsiooni täitva alltöövõtja vahel;

vii. võimalik kontsentreerumine äriühingus (sealhulgas kontserni tasandil, kui see on kohaldatav), mida põhjustavad mitu pilveteenuse osutajale tegevuse edasiandmise lepingut sama pilveteenuse osutajaga, samuti võimalik kontsentreerumine ELi finantssektoris, mida põhjustavad mitu äriühingut, kes kasutavad sama pilveteenuse osutajat või väikest pilveteenuse osutajate rühma. Äriühing peaks kontsentratsiooniriski hindamisel võtma arvesse kõiki asjaomase pilveteenuse osutajaga sõlmitud edasiandmislepinguid (ja oma kontserni tasandil sõlmitud edasiandmislepinguid, kui see on kohaldatav);

b) võtma arvesse pilveteenuse osutajatele tegevuse edasiandmise lepinguga kaasnevat oodatavat kasu ja kulu, võrreldes sealhulgas kõiki olulisi riske, mida võidakse vähendada või paremini juhtida, kõigi oluliste riskidega, mis võivad edasiandmislepingu tulemusena tekkida.

21. Kriitiliste või oluliste funktsioonide edasiandmise korral peaks hoolsuskohustuse audit hõlmama pilveteenuse osutaja sobivuse hindamist. Äriühing peaks pilveteenuse osutaja sobivust hinnates veenduma, et teenuseosutajal oleks maine, oskused, ressursid (inimesed, IT ja raha), organisatsiooniline struktuur ja (vajadusel) asjakohased tegevusload või registreeringud, mida on vaja kriitilise või olulise funktsiooni usaldusväärseks ja professionaalseks täitmiseks ning muude kohustuste täitmiseks pilveteenuse osutajatele tegevuse edasiandmise lepingu kehtivusperioodil. Lisategurid, millega tuleks pilveteenuse osutaja hoolsuskohustuse auditis arvestada, on muu hulgas järgmised:

    a) infoturbe haldamine, eelkõige isikuandmete, konfidentsiaalsete või muul viisil tundlike andmete kaitse;
    b) teenusetugi, sealhulgas tugikavad ja kontaktid ning intsidentide haldamise protsessid;
    c) talitluspidevus- ja avariitaasteplaanid.

22. Äriühing võib tehtud hoolsuskohustuse auditi toetamiseks ja juhul, kui see on asjakohane, kasutada ka rahvusvahelistel standarditel ja välis- või siseauditi aruannetel põhinevaid sertifikaate.

23. Kui äriühing saab teada olulistest puudustest ja/või olulistest muutustest osutatavates teenustes või pilveteenuse osutaja olukorras, tuleks pilveteenuse osutajale tegevuse

edasiandmise eelne analüüs ja pilveteenuse osutaja hoolsuskohustuse audit viivitamata läbi vaadata või neid korrata.

24. Kui äriühing sõlmib hindamise juba läbinud pilveteenuse osutajaga uue lepingu või uuendab olemasolevat lepingut, tuleks riskipõhise lähenemisviisi alusel määrata, kas on vaja teha uus hoolsuskohustuse audit.

3. suunis. Lepingu põhielemendid

25. Äriühingu ja talle teenust osutava pilveteenuse osutaja õigused ja kohustused peaksid olema kirjalikus lepingus selgelt vormistatud.

26. Äriühingul peaks kirjalikus lepingus olema sõnaselgelt ette nähtud võimalus vajadusel leping lõpetada.

27. Kriitiliste või oluliste funktsioonide edasiandmise korral peaks kirjalik leping sisaldama vähemalt järgmist:

    a) edasiantud funktsiooni selge kirjeldus;

    b) lepingu algus- ja (kui asjakohane) lõppkuupäev ning etteteatamistähtajad pilveteenuse osutaja ja äriühingu jaoks;

    c) lepingule kohaldatav õigus ja (kui olemas) kohtualluvuse valik;

    d) äriühingu ja pilveteenuse osutaja finantskohustused;

    e) kas edasiantud tegevuse edasiandmine on lubatud ja kui on, siis mis tingimustel, võttes arvesse 7. suunist;

    f) koht (kohad) (st piirkonnad või riigid), kus edasiantud funktsioone osutatakse ning andmeid töödeldakse ja säilitatakse ning nõutavad tingimused, sealhulgas nõue äriühingut teavitada, kui pilveteenuse osutaja kavatseb asukohta (asukohti) muuta;

    g) infoturbe ja isikuandmete kaitse sätted, võttes arvesse 4. suunist;

    h) äriühingu õigus jälgida pilveteenuse osutajatele tegevuse edasiandmise lepingu alusel korrapäraselt pilveteenuse osutaja tegevust, võttes arvesse 6. suunist;

    i) kokkulepitud teenustasemed, sealhulgas kvantitatiivsed ja kvalitatiivsed toimivusnõuded, mille alusel saab teha õigeaegset seiret ja rakendada ilma põhjendamatu viivituseta asjakohaseid parandusmeetmeid, kui teenustase ei vasta kokkulepitule;

    j) pilveteenuse osutaja aruandluskohustus äriühingu ees ja vajadusel kohustus esitada äriühingu turbefunktsiooni ja põhifunktsioonide jaoks olulisi aruandeid, näiteks pilveteenuse osutaja siseauditi funktsiooni koostatud aruandeid;

k) sätted, mis käsitlevad intsidentide haldamist pilveteenuse osutaja poolt, sealhulgas pilveteenuse osutaja kohustus teavitada äriühingut põhjendamatu viivituseta intsidentidest, mis mõjutavad äriühingu lepingulise teenuse toimimist;

l) kas pilveteenuse osutaja peaks olema kohustatud sõlmima kindlustuslepingu teatud riskide vastu ja (kui asjakohane) nõutava kindlustuskaitse tase;

m) nõuded pilveteenuse osutajale talitluspidevus- ja avariitaasteplaanide rakendamiseks ja testimiseks;

n) nõue, et pilveteenuse osutaja annaks äriühingule, selle pädevatele asutustele ja äriühingu või pädevate asutuste määratud mis tahes muule isikule õiguse pääseda juurde („juurdepääsuõigused“) ja kontrollida („auditeerimisõigused“) pilveteenuse osutaja asjaomast teavet, ruume, süsteeme ja seadmeid ulatuses, mis on vajalik pilveteenuse osutaja tegevuse jälgimiseks tegevuse edasiandmise lepingu alusel, ning selle tegevuse vastavust kohaldatavatele regulatiivsetele ja lepingulistele nõuetele, võttes arvesse 6. suunist;

o) sätted, millega tagatakse, et andmed, mida pilveteenuse osutaja äriühingu nimel töötleb või säilitab, on vastavalt vajadusele juurdepääsetavad, taaskasutatavad ja äriühingule tagastatavad, võttes arvesse 5. suunist.

4. suunis. Infoturve

28. Äriühing peaks kehtestama infoturbenõuded oma sise-eeskirjades ja -menetlustes ning pilveteenuse osutajatele tegevuse edasiandmise kirjalikus lepingus ning jälgima pidevalt nende nõuete täitmist, sealhulgas selleks, et kaitsta konfidentsiaalseid, isikuandmeid või muul viisil tundlikke andmeid. Need nõuded peaksid olema proportsionaalsed pilveteenuse osutajatele edasiantava funktsiooni laadi, ulatuse ja keerukuse ning selle funktsiooniga seotud riskidega.

29. Seetõttu peaks äriühing kriitiliste või oluliste funktsioonide pilveteenuste osutajatele edasiandmisel (ilma et see piiraks isikuandmete kaitse üldmääruse alusel kohaldatavaid nõudeid) tegema riskipõhist lähenemisviisi kohaldades vähemalt järgmist:

a) *infoturbe korraldus:* tagama, et infoturbega seotud ülesanded ja vastutus on äriühingu ja pilveteenuse osutaja vahel selgelt jaotatud (sealhulgas seoses ohtude avastamise, intsidentide haldamise ja turvaaukude paikamise haldamisega), ning tagama, et pilveteenuse osutaja on võimeline oma ülesandeid ja kohustusi tõhusalt täitma;
b) *tuvastus- ja juurdepääsuhaldus*: tagama, et on kehtestatud tugevad autentimismehhanismid (nt kaksikautentimine) ja juurdepääsukontrollid, et vältida loata juurdepääsu äriühingu andmetele ja pilvandmetöötluse põhiressurssidele;
c) *krüpteerimine ja võtmehaldus:* tagama, et edastatavate, mälus säilitatavate, puhke- ja varundusandmete jaoks kasutatakse vajadusel asjakohaseid

krüpteerimistehnoloogiaid koos sobivate võtmehalduslahendustega, et piirata krüpteerimisvõtmetele loata juurdepääsu riski; eelkõige peaks äriühing oma võtmehalduslahenduse valimisel kaaluma tipptasemel tehnoloogia ja protsesside kasutamist;

d) *tegevuse ja võrgu turve:* kaaluma võrgu kättesaadavuse, võrgu eraldamise (näiteks rentniku isoleerimine pilve jagatud keskkonnas, tegevuste eraldamine seoses veebi, rakendusloogika, operatsioonisüsteemi, võrgu, andmebaasihaldussüsteemi ja salvestuskihtidega) ja töötlemiskeskkondade (näiteks testimine, kasutajapoolse omaksvõtu testimine, arendamine, tootmine) asjakohaseid tasemeid;
e) *rakendusliidesed:* kaaluma mehhanisme pilveteenuste integreerimiseks äriühingu süsteemidega, et tagada rakendusliideste turvalisus (näiteks kehtestades ja säilitades rakendusliideste infoturvapoliitika ja menetluskorra eri süsteemiliideste, jurisdiktsioonide ja ärifunktsioonide lõikes, et hoida ära andmete loata avalikustamine, muutmine või hävitamine);
f) *talitluspidevus ja avariitaaste*: tagama, et on kehtestatud tõhusad talitluspidevuse ja avariitaastekontrollid (näiteks kehtestades minimaalse suutlikkuse nõuded, valides geograafiliselt hajutatud majutusvõimalused võimalusega ühelt teenusepakkujalt teisele üle minna, või nõudes ja vaadates läbi dokumente, mis näitavad äriühingu andmete transporditeed pilveteenuse osutaja süsteemides, samuti kaaludes võimalust kopeerida masinkujutisi sõltumatusse salvestuskohta, mis on võrgust piisavalt eraldatud või võrgust eemaldatud);
g) *andmete asukoht*: võtma seoses andmete salvestuse ja töötlemise asukohtadega (st piirkondade või riikidega) kasutusele riskipõhise lähenemisviisi;
h) *nõuete järgimine ja järelevalve*: kontrollima, et pilveteenuse osutaja järgib rahvusvaheliselt tunnustatud infoturbestandardeid ja on rakendanud asjakohased infoturbekontrollid (näiteks paludes pilveteenuse osutajal esitada asjakohaste infoturbe läbivaatamiste tõendid ning viies läbi pilveteenuse osutaja infoturbekorra korrapäraseid hindamisi ja testimisi).

5. suunis. Väljumisstrateegiad

30. Kriitiliste või oluliste funktsioonide edasiandmise korral peaks äriühing tagama, et tal on võimalik pilveteenuse osutajatele tegevuse edasiandmise leping lõpetada, ilma et see häiriks põhjendamatult tema äritegevust ja teenuseid klientide jaoks või kahjustaks tema kohaldatavatest õigusaktidest tulenevate kohustuste täitmist ning tema andmete konfidentsiaalsust, terviklust ja kättesaadavust. Selleks peaks äriühing:

a) töötama välja väljumiskavad, mis on terviklikud, dokumenteeritud ja piisavalt testitud. Neid kavasid tuleks vastavalt vajadusele ajakohastada, sealhulgas edasiantud funktsiooni muutumisel;
b) tegema kindlaks alternatiivsed lahendused ja töötama välja üleminekukavad edasiantud funktsiooni ja andmete eemaldamiseks pilveteenuse osutajalt (ja

vajadusel ükskõik milliselt alltöövõtjalt) ning nende edastamiseks äriühingu määratud alternatiivsele pilveteenuse osutajale või otse tagasi äriühingule. Need lahendused tuleks kindlaks määrata, arvestades probleeme, mis võivad tekkida andmete asukoha tõttu, ja rakendades vajalikke meetmeid talitluspidevuse tagamiseks üleminekuetapis;

c) tagama, et pilveteenuse osutajatele tegevuse edasiandmise kirjalik leping sisaldab pilveteenuse osutaja kohustust toetada edasiantud funktsiooni nõuetekohast üleandmist ja sellega seotud andmete töötlemist pilveteenuse osutajalt ja ükskõik milliselt alltöövõtjalt teisele äriühingu määratud pilveteenuse osutajale või otse äriühingule, kui äriühing käivitab väljumisstrateegia. Kohustus toetada edasiantud funktsiooni nõuetekohast üleandmist ja sellega seotud andmete töötlemist peaks vajaduse korral hõlmama andmete turvalist kustutamist pilveteenuse osutaja ja alltöövõtjate süsteemidest.

31. Eeltoodud punktides a ja b viidatud väljumiskavade ja -lahenduste („väljumisstrateegia“) väljatöötamisel peaks äriühing võtma arvesse järgmist:

a) määrama kindlaks väljumisstrateegia eesmärgid;
b) määrama kindlaks käivitavad sündmused, mis võiksid väljumisstrateegia aktiveerida. Nende hulgas peaks olema vähemalt pilveteenuse osutajatele tegevuse edasiandmise lepingu lõpetamine äriühingu või pilveteenuse osutaja algatusel ning pilveteenuse osutaja maksejõuetus või muu tema äritegevuse oluline katkemine;
c) tegema edasiantava funktsiooni mõjuanalüüsi, et välja selgitada, milliseid inim- ja muid ressursse on väljumisstrateegia rakendamiseks vaja;
d) määrama väljumisstrateegia haldamiseks ülesanded ja vastutusalad;
e) testima väljumisstrateegia asjakohasust, kasutades riskipõhist lähenemist (nt edasiantud teenuse teisele teenuseosutajale üleandmisega seotud kulude, mõju, ressursside ja ajastusmõjude analüüs);
f) määratlema ülemineku edukuse kriteeriumid.

32. Äriühing peaks lisama väljumisstrateegiat käivitavate sündmuste näitajad oma pidevasse seiresse ja järelevalvesse, mida tehakse pilveteenuste osutaja poolt edasiandmislepingu alusel osutatavate teenuste üle.

6. suunis. Juurdepääsu- ja auditeerimisõigused

33. Äriühing peaks tagama, et pilveteenuse osutajatele tegevuse edasiandmise kirjalik leping ei piiraks äriühingu ega pädeva asutuse võimalusi kasutada pilveteenuse osutaja suhtes juurdepääsu- ja auditeerimisõigusi ning teha järelevalvet.

34. Äriühing peaks tagama, et juurdepääsu- ja auditeerimisõiguste kasutamisel (näiteks seoses auditi sageduse ning auditeeritavate valdkondade ja teenustega) võetakse arvesse seda, kas pilveteenuse osutajatele tegevuse edasiandmine on seotud kriitilise

või olulise funktsiooniga, samuti pilveteenuse osutajatele tegevuse edasiandmise lepingust äriühingule tulenevate riskide ja mõju laadi ning ulatust.

35. Kui juurdepääsu- või auditeerimisõiguste või teatavate auditeerimistehnikate kasutamine tekitab ohtu pilveteenuse osutaja ja/või mõne teise pilveteenuse osutaja kliendikeskkonnale (näiteks mõjutades teenuse taset, andmete konfidentsiaalsust, terviklust ja kättesaadavust), peaks pilveteenuse osutaja esitama äriühingule selge põhjenduse vastava riski tekkimise põhjuse kohta ja leppima äriühinguga kokku alternatiivsed viisid sarnase tulemuse saavutamiseks (näiteks teatud kontrollimehhanismide lisamine, mida pilveteenuse osutaja peab teatud aruande/sertifikaadi loomisel testima).

36. Ilma et see piiraks äriühingute lõplikku vastutust pilveteenuse osutajatele tegevuse edasiandmise lepingute eest, võivad nad kasutada auditeerimisressursside tõhusamaks rakendamiseks ning pilveteenuse osutaja ja tema klientide organisatsioonilise koormuse vähendamiseks järgmist:

    a) pilveteenuse osutaja esitatud kolmanda isiku väljastatud sertifikaadid ja välis- või siseauditi aruanded;
    b) sama pilveteenuse osutaja teiste klientidega ühiselt tehtud auditid või sama pilveteenuse osutaja mitme kliendi määratud kolmandast isikust audiitori poolt tehtud ühisauditid.

37. Kriitiliste või oluliste funktsioonide edasiandmise korral peaks äriühing hindama, kas punkti 37 alapunktis a viidatud kolmandate isikute sertifikaadid ja välis- või siseauditi aruanded on asjakohased ja piisavad, võimaldamaks äriühingul täita kohaldatavatest õigusaktidest tulenevaid kohustusi, ning võtta eesmärgiks tugineda edaspidi ka muule kui üksnes neile sertifikaatidele ja aruannetele.

38. Kriitiliste või oluliste funktsioonide edasiandmise korral peaks äriühing kasutama punkti 37 alapunktis a viidatud kolmanda isiku sertifikaate ja välis- või siseauditi aruandeid üksnes juhul, kui ta:

    a) on kindel, et sertifikaadid või auditiaruanded hõlmavad pilveteenuse osutaja olulisi süsteeme (nt protsessid, rakendused, taristu, andmekeskused), äriühingu määratletud olulisi kontrollimehhanisme ning vastavust kohaldatavatele õigusaktidele;
    b) hindab korrapäraselt ja põhjalikult sertifikaatide ja auditiaruannete sisu ning jälgib, et sertifikaadid ja aruanded ei oleks aegunud;
    c) tagab, et tulevastes sertifikaatides või auditiaruannetes oleks käsitletud pilveteenuse pakkuja olulisi süsteeme ja kontrollimehhanisme;
    d) on rahul sertifitseeriva või auditeeriva isikuga (näiteks tema kvalifikatsiooni, asjatundlikkuse, aluseks olevas audititoimikus olevate tõendite ülekontrollimise/kinnitamise ning sertifitseerimis- või auditeerimisettevõtte rotatsiooniga);

e) on veendunud, et sertifikaate väljastatakse ja auditeid tehakse asjakohaste standardite alusel ning need sisaldavad kehtestatud oluliste kontrollimehhanismide tulemuslikkuse kontrolli;
f) on sätestanud lepingus enda õiguse nõuda sertifikaatide ja auditiaruannete ulatuse laiendamist pilveteenuse osutaja muudele asjaomastele süsteemidele ja kontrollimehhanismidele (ulatuse muutmise taotluste arv ja esitamise sagedus peaks olema mõistlik ja riskijuhtimise seisukohast põhjendatud);
g) säilitab lepingulise õiguse teha edasiantud funktsiooni täitmise kohapealseid üksikauditeid omal äranägemisel.

39. Äriühing peaks tagama, et enne kohapealset kontrollkäiku, sealhulgas äriühingu määratud kolmanda isiku (näiteks audiitori) poolt, antakse pilveteenuse osutajale sellest mõistliku aja jooksul ette teada, välja arvatud juhul, kui etteteavitamine ei ole võimalik häda- või kriisiolukorra tõttu või tooks kaasa olukorra, kus audit ei oleks enam tulemuslik. Sellises teates tuleks täpsustada kontrollkäigu toimumiskoht, eesmärk ning osalevad töötajad.

40. Kuna pilveteenused on tehniliselt väga keerukad ja tekitavad jurisdiktsiooniga seotud spetsiifilisi probleeme, peaks auditit tegevatel töötajatel (äriühingu siseaudiitoritel või tema nimel tegutsevatel audiitoritel) olema asjakohased oskused ja teadmised, mis võimaldavad asjaomaseid pilveteenuseid nõuetekohaselt hinnata ning teha tulemuslikke ja asjakohaseid auditeid. See peaks kehtima ka äriühingu töötajate suhtes, kes vaatavad läbi pilveteenuse osutaja esitatud sertifikaate või auditiaruandeid.

7. suunis. Edasiantud tegevuse edasiandmine

41. Kui edasiantud kriitiliste või oluliste funktsioonide (või nende oluliste osade) edasiandmine on lubatud, tuleks äriühingu ja pilveteenuse osutaja vahelise pilveteenuse osutajatele tegevuse edasiandmise kirjaliku lepinguga:

a) täpsustada edasiantud funktsiooni mis tahes osa või aspekt, mis ei kuulu võimaliku alltöövõtjale edasiandmise hulka;
b) määrata tingimused, mida tuleb edasiantud tegevuse edasiandmisel täita;
c) täpsustada, et pilveteenuse osutaja jääb alltöövõtjale edasiantud teenuste eest endiselt vastutavaks ja peab tegema nende üle järelevalvet, et tagada kõigi pilveteenuse osutaja ja äriühingu vahelises lepingus sätestatud kohustuste pidev täitmine;
d) lisada pilveteenuse osutajale kohustus teavitada äriühingut mis tahes talle edasiantud tegevuse kavandatud edasiandmisest või selle olulistest muudatustest, eelkõige juhul, kui see võib mõjutada pilveteenuse osutaja suutlikkust täita äriühinguga sõlmitud edasiandmislepingust tulenevaid kohustusi. Kirjalikus lepingus sätestatud teatamistähtaeg peaks jätma äriühingule piisavalt aega vähemalt edasiantud tegevuse kavandatud edasiandmise või selle oluliste

muudatuste riskihindamiseks ning edasiandmise või muudatuste vaidlustamiseks või sõnaselgeks heakskiitmiseks, nagu on osutatud allpool alapunktis e;

e) tagada, et äriühingul on õigus edasiantud tegevuse kavandatud edasiandmise või selle oluliste muudatuste suhtes vastuväiteid esitada või et enne kavandatud edasiandmise või oluliste muudatuste jõustumist on nõutav tema selgesõnaline heakskiit;

f) tagada, et äriühingul on lepinguline õigus lõpetada pilveteenuse osutajaga edasiandmisleping, kui ta on vastu edasiantud tegevuse kavandatud edasiandmisele või selle olulistele muudatustele ning kui selline edasiandmine alltöövõtjale on sobimatu (näiteks kui pilveteenuse osutaja kasutab tegevuse edasiandmist alltöövõtjale ilma äriühingut teavitamata või rikub oluliselt pilveteenuse osutajatele tegevuse edasiandmise lepingus sätestatud edasiantud tegevuse edasiandmise tingimusi).

42. Äriühing peaks tagama, et pilveteenuse osutaja teeb alltöövõtja üle asjakohast järelevalvet.

8. suunis. Kirjalik teade pädevatele asutustele

43. Äriühing peaks pädevat asutust õigeaegselt ja kirjalikult teavitama pilveteenuse osutajatele tegevuse edasiandmise kavandatud lepingutest, mis puudutavad kriitilist või olulist funktsiooni. Samuti peaks äriühing pädevale asutusele õigeaegselt ja kirjalikult teatama nendest pilveteenuse osutajatele tegevuse edasiandmise lepingutest, mis puudutavad funktsiooni, mis varem liigitati mittekriitiliseks või väheoluliseks ja mis seejärel muutus kriitiliseks või oluliseks.

44. Äriühingu kirjalik teade peaks proportsionaalsuse põhimõtet arvestades sisaldama vähemalt järgmist teavet:

a) pilveteenuse osutajatele tegevuse edasiandmise lepingu alguskuupäev ja (kui asjakohane) järgmise uuendamise kuupäev, lõppkuupäev ja/või etteteatamistähtajad pilveteenuse osutaja ja äriühingu jaoks;

b) edasiantud funktsiooni lühikirjeldus;

c) lühikokkuvõte põhjustest, miks edasiantud funktsiooni peetakse kriitiliseks või oluliseks;

d) pilveteenuse osutaja nimi ja kaubamärk (kui olemas), selle registreerimisriik, registreerimisnumber, juriidilise isiku tunnus (kui olemas), registrijärgne aadress, muud asjakohased kontaktandmed ja emaettevõtte nimi (kui olemas);

e) pilveteenuse osutajatele tegevuse edasiandmise lepingule kohaldatav õigus ja (kui olemas) kohtualluvuse valik;

f) pilveteenuste kasutuselevõtumudelid ning pilveteenuse osutaja poolt säilitatavate andmete täpsem laad ja asukohad (st piirkonnad või riigid), kus neid andmeid säilitatakse;

g) edasiantud funktsiooni kriitilisuse või olulisuse viimase hindamise kuupäev;

h) pilveteenuse osutaja viimase riskihindamise või auditi kuupäev koos peamiste tulemuste lühikokkuvõttega ja järgmise kavandatud riskihindamise või auditi kuupäev;
i) pilveteenuse osutajatele tegevuse edasiandmise lepingu heakskiitnud üksikisik või otsuseid tegev organ äriühingus;
j) kui asjakohane, siis alltöövõtja nimi, kellele edasiantud kriitilise või olulise funktsiooni olulised osad on omakorda edasi antud (sh riik või piirkond, kus alltöövõtja on registreeritud, kus alltöövõtjale edasiantud teenust osutatakse ja kus andmeid säilitatakse).

9. suunis. Pilveteenuse osutajatele tegevuse edasiandmise lepingute järelevalve

45. Pädevad asutused peaksid äriühingute pilveteenuse osutajatele tegevuse edasiandmise lepingutest tulenevaid riske hindama oma järelevalvemenetluse raames. Eelkõige tuleks hindamisel keskenduda lepingutele, mis on seotud kriitiliste või oluliste funktsioonide edasiandmisega.

46. Pädevad asutused peaksid veenduma, et nad saavad teha tulemuslikku järelevalvet, eriti juhul, kui äriühingud annavad edasi olulisi või kriitilisi funktsioone, mida hakatakse täitma väljaspool ELi.

47. Pädevad asutused peaksid riskipõhise lähenemisviisi alusel hindama, kas äriühingud:

a) omavad asjakohaseid juhtimistavasid, ressursse ja tegevusprotsesse, et pilveteenuse osutajatele tegevuse edasiandmise lepinguid nõuetekohaselt ja tõhusalt sõlmida ja rakendada ning nende üle järelevalvet teha;
b) suudavad tuvastada ja hallata kõiki pilveteenuse osutajatele tegevuse edasiandmisega seotud asjakohaseid riske.

48. Kontsentratsiooniriski tuvastamise korral peaksid pädevad asutused jälgima selliste riskide arengut ja hindama nii nende võimalikku mõju teistele äriühingutele, kelle üle nad järelevalvet teevad, kui ka finantsturu stabiilsust.