30/09/2025
ESMA65-294529287-4737

Gairės

dėl veiklos funkcijų perdavimo debesijos paslaugų teikėjams

Turinys

1 Taikymo sritis

Kam taikomos šios gairės?

1. Šios gairės taikomos kompetentingoms institucijoms ir i) alternatyvaus investavimo fondų (AIF) depozitoriumams, nurodytiems AIFVD 21 straipsnio 3 dalies c punkte ir 21 straipsnio 3 dalies trečioje pastraipoje, kai jie nėra finansų subjektai, kuriems taikomas DORA, ir ii) KIPVPS depozitoriumams, nurodytiems KIPVPS direktyvos 23 straipsnio 2 dalies c punkte, kai jie nėra finansų subjektai, kuriems taikoma DORA.[1]

Apie ką šios gairės?

2. Šios gairės taikomos šioms nuostatoms:

   a) AIF depozitoriumams: AIFVD 21 straipsnis; Komisijos deleguotojo reglamento (ES) 2013/231 98 straipsnis;
   b) KIPVPS depozitoriumams: KIPVPS direktyvos 22, 22a straipsniai ir 23 straipsnio 2 dalis; Komisijos direktyvos 2010/43/ES 32 straipsnis; Komisijos deleguotojo reglamento (ES) 2016/438 2 straipsnio 2 dalies j punktas, 3 straipsnio 1 dalis, 13 straipsnio 2 dalis, 15, 16 ir 22 straipsniai.

Nuo kada taikomos šios gairės?

3. Šios gairės taikomos nuo jų paskelbimo ESMA interneto svetainėje visomis oficialiosiomis ES kalbomis dienos ir visiems nuo tos dienos arba vėliau sudarytiems, atnaujintiems arba iš dalies pakeistiems užsakomųjų debesijos paslaugų susitarimams.

4. Atsižvelgiant į DORA taikymą, ankstesnės ESMA gairės dėl veiklos funkcijų perdavimo debesijos paslaugų teikėjams nebetaikomos tiems finansų sektoriaus subjektams, kuriems taikoma DORA, kaip nustatyta to paties reglamento 2 straipsnyje. AIF depozitoriumams ir 1 dalyje nurodytiems KIPVPS depozitoriumams ankstesnės ESMA gairės dėl veiklos funkcijų perdavimo debesijos paslaugų teikėjams bus toliau taikomos iki šių gairių paskelbimo ESMA interneto svetainėje visomis oficialiosiomis ES kalbomis dienos.

[1] Dėl debesijos paslaugų teikimo sutarčių finansų įstaigos, apibrėžtos Reglamento 2 straipsnio 1 ir 2 dalyse, pagal Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninio veiklos atsparumo finansų sektoriuje ir kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (DORA reglamentas), yra taikomos specialios taisyklės, nustatytos DORA reglamente ir susijusiuose Komisijos deleguotuosiuose ir įgyvendinimo reglamentuose.

2 Nuorodos į teisės aktus, santrumpos ir sąvokų apibrėžtys

2.1 Nuorodos į teisės aktus

ESMA reglamentas	2010 m. lapkričio 24 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 1095/2010, kuriuo įsteigiama Europos priežiūros institucija (Europos vertybinių popierių ir rinkų institucija) ir iš dalies keičiamas Sprendimas Nr. 716/2009/EB bei panaikinamas Komisijos sprendimas 2009/77/EB[2].
AIFVD	2011 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2011/61/ES dėl alternatyvaus investavimo fondų valdytojų, kuria iš dalies keičiami direktyvos 2003/41/EB ir 2009/65/EB bei reglamentai (EB) Nr. 1060/2009 ir (ES) Nr. 1095/2010[3].
Komisijos deleguotasis reglamentas (ES) 2013/231	2012 m. gruodžio 19 d. Komisijos deleguotasis reglamentas (ES) 2013/231, kuriuo papildomos Europos Parlamento ir Tarybos direktyvos 2011/61/ES nuostatos dėl išimčių, bendrųjų veiklos sąlygų, depozitoriumų, finansinio sverto, skaidrumo ir priežiūros[4].
KIPVPS direktyva	2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/65/EB dėl įstatymų ir kitų teisės aktų, susijusių su kolektyvinio investavimo į perleidžiamus vertybinius popierius subjektais (KIPVPS), derinimo[5].
Komisijos direktyva 2010/43/ES	2010 m. liepos 1 d. Komisijos direktyva 2010/43/ES, kuria įgyvendinamos Europos Parlamento ir Tarybos direktyvos 2009/65/EB nuostatos dėl organizacinių reikalavimų, interesų konfliktų, veiklos vykdymo, rizikos valdymo ir dėl depozitoriumo ir valdymo įmonės susitarimo turinio[6].
DORA	2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami

[2] OL L 331, 2010 12 15, p. 84
[3] OL L 174, 2011 7 1, p. 1.
[4] OL L 83, 2013 3 22, p. 1.
[5] OL L 302, 2009 11 17, p. 32.
[6] OL L 176, 2010 7 10, p. 42.

	reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011[7]
BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB[8].

2.2 Santrumpos

DPT	debesijos paslaugų teikėjas
ES	Europos Sąjunga
ESMA	Europos vertybinių popierių ir rinkų institucija

2.3 Apibrėžtys

funkcija	bet kokie procesai, paslaugos ar veikla;
esminė arba svarbi funkcija	bet kokia funkcija, kurią vykdant netinkamai arba kurios nevykdant, iš esmės nukentėtų: a) taikytinuose teisės aktuose nustatytų įmonės įsipareigojimų vykdymas; b) įmonės finansiniai rodikliai arba c) įmonės pagrindinių paslaugų ir veiklos patikimumas arba tęstinumas;
debesijos paslaugos	debesijos kompiuterijos priemonėmis teikiamos paslaugos;
debesijos kompiuterija ar debesija[9]	paradigma, suteikianti tinklui prieigą prie kintamo masto pritaikomos bendrų fizinių ar virtualių išteklių bazės (pavyzdžiui, serverių, operacinių sistemų, tinklų, programinės įrangos, taikomųjų programų ir saugojimo

[7] *OL L 333, 2022 12 27, p. 1–79.*
[8] OL L 119, 2016 5 4, p. 1–88.
[9] Terminas „debesijos kompiuterija“ dažnai trumpinamas „debesija“. Likusiame dokumente aiškumo sumetimais vartojamas terminas „debesija“.

	įrangos), su apsitarnavimo ir administravimo esant poreikiui funkcija;
debesijos paslaugų teikėjas	trečioji šalis, teikianti debesijos paslaugas pagal debesijos paslaugų perdavimo sutartį;
debesijos paslaugų perdavimo sutartis	bet kokios formos sutartis, įskaitant funkcijų perdavimo sutartis, tarp: (i) įmonės ir DPT, pagal kurią DPT vykdo funkciją, kurią, kitu atveju, vykdytų pati įmonė arba (ii) įmonės ir trečiosios šalies, kuri nėra DPT, bet kuri stipriai priklauso nuo DPT, kad šis vykdytų funkciją, kurią, kitu atveju, vykdytų pati įmonė. Šiuo atveju nuoroda į DPT šiose gairėse laikoma nuoroda į trečiąją šalį.
veiklos funkcijų perdavimas subrangos būdu	situacija, kai DPT perduotą funkciją (ar jos dalį) perduoda vykdyti kitam paslaugų teikėjui pagal veiklos funkcijų perdavimo sutartį;
debesijos diegimo modelis	būdas, kuriuo gali būti organizuojamos debesijos paslaugos, remiantis fizinių ar virtualių išteklių valdymu ir dalijimusi. Debesijos diegimo modelis apima bendruomenės [10], hibridinę [11], privačią [12] ir viešąją [13] debesiją;
įmonės	a) AIFVD 21 straipsnio 3 dalies c punkte ir 21 straipsnio 3 dalies trečioje pastraipoje nurodyti depozitoriumai (toliau – alternatyvaus investavimo fondų (AIF) depozitoriumai); b) KIPVPS direktyvos 23 straipsnio 2 dalies c punkte nurodyti depozitoriumai („KIPVPS depozitoriumai“).

[10] Debesijos diegimo modelis, kai debesijos paslaugas išskirtinai palaiko ir jomis dalijasi konkreti debesijos paslaugų vartotojų grupė, turinti bendrų reikalavimų ir siejama santykių, ir kai išteklius valdo mažiausiai vienas šios grupės narys;
[11] Debesijos diegimo modelis, kuriame naudojami mažiausiai du skirtingi debesijos diegimo modeliai
[12] Debesijos diegimo modelis, kai debesijos paslaugas išskirtinai naudoja ir išteklius valdo vienas debesijos paslaugų vartotojas
[13] Debesijos diegimo modelis, kai debesijos paslaugomis gali naudotis bet kuris debesijos paslaugos vartotojas ir išteklius valdo debesijos paslaugų teikėjas

3 Paskirtis

5. Šių gairių pagrindas – ESMA reglamento 16 straipsnio 1 dalis. Šiomis gairėmis siekiama nustatyti nuoseklią, veiksmingą ir efektyvią Europos finansų priežiūros institucijų sistemos (EFPIS) priežiūros praktiką ir užtikrinti bendrą, vienodą ir nuoseklų 1.1 skirsnio dalyje „Apie ką šios gairės?“ nurodytų reikalavimų, keliamų įmonėms, kurios paslaugas perduoda DPT, taikymą. Visų pirma šiomis gairėmis siekiama padėti įmonėms ir kompetentingoms institucijoms nustatyti, valdyti ir stebėti riziką ir problemas, kylančias iš debesijos paslaugų perdavimo sutarčių, – nuo sprendimo perduoti paslaugas priėmimo, debesijos paslaugų teikėjo pasirinkimo, perduotos veiklos stebėsenos iki pasitraukimo strategijų pateikimo.

4 Pareiga laikytis gairių ir pranešti

4.1 Gairių statusas

6. Pagal ESMA reglamento 16 straipsnio 3 dalį kompetentingos institucijos ir įmonės deda visas pastangas siekdamos laikytis šių gairių.

7. Kompetentingos institucijos, kurioms taikomos šios gairės, turėtų jų laikytis deramai įtraukdamos jas į savo nacionalinės teisės ir (arba) priežiūros sistemas, įskaitant atvejus, kai konkrečios gairės visų pirma skirtos įmonėms. Šiuo atveju vykdydamos priežiūrą kompetentingos institucijos turėtų užtikrinti, kad įmonės laikytųsi gairių.

4.2 Ataskaitų teikimo reikalavimai

8. Per du mėnesius nuo rekomendacijų visomis oficialiosiomis ES kalbomis paskelbimo ESMA svetainėje dienos kompetentingos institucijos, kurioms taikomos šios gairės, privalo pranešti ESMA, ar jos i) laikosi, ii) nesilaiko, bet ketina laikytis, arba iii) nesilaiko ir neketina laikytis gairių.

9. Jei gairių nesilaikoma, kompetentingos institucijos taip pat privalo per du mėnesius nuo gairių paskelbimo ESMA svetainėje visomis ES oficialiosiomis kalbomis dienos pranešti ESMA, dėl kokių priežasčių jos nesilaiko gairių. Pranešimo šabloną galima rasti ESMA svetainėje. Užpildytas šablonas turi būti perduotas ESMA.

10. Įmonės neprivalo pranešti, ar jos laikosi šių gairių.

5 Veiklos funkcijų perdavimo debesijos paslaugų teikėjams gairės

1 gairė. Valdymas, priežiūra ir dokumentavimas

11. Įmonė turėtų turėti apibrėžtą ir atnaujintą debesijos paslaugų perdavimo strategiją, kuri atitinka atitinkamas įmonės strategijas ir vidaus politiką bei procesus, įskaitant su informacinėmis ir ryšių technologijomis, informacijos saugumu ir operacinės rizikos valdymu susijusius procesus.

12. Įmonė turėtų:

    a) aiškiai priskirti debesijos paslaugų perdavimo sutarčių dokumentavimo, valdymo ir kontrolės pareigas organizacijoje;
    b) skirti pakankamus išteklius atitikčiai šioms gairėms ir visiems teisiniams reikalavimams, taikytiniems debesijos paslaugų perdavimo sutartims, užtikrinti;
    c) nustatyti debesijos paslaugų perdavimo priežiūros funkciją ar paskirti vyresniuosius darbuotojus, kurie bus tiesiogiai atskaitingi valdymo organui ir atsako už rizikos, susijusios su debesijos paslaugų perdavimo sutartimis, valdymą ir priežiūrą; Vykdydamos šių gairių reikalavimus, įmonės turėtų atsižvelgti į savo verslo pobūdį, mastą ir sudėtingumą, įskaitant su finansų sistema susijusią riziką ir perduotoms funkcijoms būdingą riziką, ir užtikrinti, kad jų valdymo organas turėtų atitinkamų techninių įgūdžių, leidžiančių suprasti su debesijos paslaugų perdavimo sutartimis susijusią riziką. Mažos ir ne tokios sudėtingos struktūros įmonės turėtų bent jau aiškiai atskirti su debesijos paslaugų perdavimo sutartimis susijusias valdymo ir priežiūros užduotis ir pareigas.

13. Įmonė turėtų stebėti veiklos vykdymą, apsaugos priemones ir tai, kaip DPT laikosi sutartų paslaugos teikimo lygių. Ši stebėsena turėtų būti grindžiama rizika daugiausia dėmesio skiriant perduotoms esminėms ar svarbioms funkcijoms.

14. Įmonė turėtų reguliariai ir visada, kai iš esmės pasikeičia perduotos funkcijos rizika, pobūdis ar mastas, iš naujo įvertinti, ar jos debesijos paslaugų perdavimo sutartys susijusios su esmine ar svarbia funkcija.

15. Įmonė turėtų turėti nuolat atnaujinamą informacijos apie visas debesijos paslaugų perdavimo sutartis registrą ir esminių ar svarbių funkcijų perdavimo sutartis atskirti nuo kitų veiklos funkcijų sutarčių. Esminių ar svarbių funkcijų perdavimo sutartis atskirdama nuo kitų veiklos funkcijų sutarčių, ji turėtų trumpai apibendrinti priežastis, dėl kurių perduodama funkcija yra arba nėra laikoma esmine ar svarbia. Atsižvelgdama į

nacionalinės teisės nuostatas, įmonė taip pat turėtų atitinkamą laikotarpį turėti nutrauktų debesijos paslaugų perdavimo sutarčių sąrašą.

16. Registre turėtų būti bent ši informacija apie kiekvieną esminių ar svarbių funkcijų debesijos paslaugų perdavimo sutartį:

    a) registracijos numeris;
    b) įsigaliojimo data ir, kai tinkama, sutarties galiojimo pratęsimo data, galiojimo pabaigos data ir (arba) DPT ir įmonei taikomi pranešimo laikotarpiai;
    c) trumpas perduotos funkcijos aprašymas, įskaitant perduotus duomenis ir tai, ar jie apima asmens duomenis (pavyzdžiui, atskirame duomenų lauke pažymint „taip“ arba „ne“);
    d) įmonės priskirta perduotos funkcijos (pavyzdžiui, informacinių technologijų, kontrolės funkcijos) pobūdį atspindinti kategorija, padedanti identifikuoti įvairių rūšių debesijos paslaugų perdavimo sutartis;
    e) ar perduota funkcija skirta veiklai, kurią svarbu vykdyti laiku;
    f) DPT pavadinimas ir prekių ženklas (jei yra), registracijos šalis, įmonės registracijos numeris, juridinio subjekto identifikacinis numeris (jei yra), registruotas adresas, svarbūs kontaktiniai duomenys ir patronuojančiosios įmonės pavadinimas (jei yra);
    g) debesijos paslaugų perdavimo sutartį reglamentuojantis įstatymas ir, jei yra, pasirinkta jurisdikcija;
    h) debesijos paslaugų rūšis ir diegimo modeliai bei konkretus saugotinų duomenų pobūdis ir vietos (t. y. regionai ar šalys), kuriose galima tokius duomenis saugoti;
    i) paskutinio perduotos funkcijos esmingumo ar svarbos vertinimo data ir kito planuojamo vertinimo data;
    j) paskutinio DPT vertinimo ir (arba) audito data ir trumpa pagrindinių rezultatų santrauka bei kito planuojamo rizikos vertinimo ir (arba) audito data;
    k) įmonės asmuo ar sprendimą priimantis organas, kuris patvirtino debesijos paslaugų perdavimo sutartį;
    l) jei taikytina, visų subrangovų, kuriems subrangos pagrindu perduota esminė ar svarbi funkcija (ar jos esminės dalys), pavadinimai, įskaitant šalis, kuriose subrangovai yra registruoti, šalis, kuriose bus teikiama subrangos būdu perduota paslauga, ir vietas (t. y. regionus ar šalis), kuriose bus saugomi duomenys;
    m) debesijos paslaugų perdavimo sutarties metinio biudžeto sąmata.

17. Neesminių ar nesvarbių funkcijų debesijos paslaugų perdavimo sutarčių atveju įmonė turėtų nustatyti į registrą įrašytiną informaciją pagal perduotai funkcijai būdingos rizikos pobūdį, mastą ir sudėtingumą.

2 gairė. Išankstinė veiklos funkcijų perdavimo analizė ir išsamus patikrinimas

18. Prieš sudarydama bet kokią debesijos paslaugų perdavimo sutartį, įmonė turėtų:

    a) įvertinti, ar debesijos paslaugų perdavimo sutartis taikoma esminei ar svarbiai funkcijai;
    b) nustatyti ir įvertinti visą su debesijos paslaugų perdavimo sutartimi susijusią riziką;
    c) atlikti tinkamą galimo DPT išsamų patikrinimą;
    d) nustatyti ir įvertinti bet kokį interesų konfliktą, kurį gali sukelti paslaugų perdavimas.

19. Išankstinė veiklos funkcijų perdavimo analizė ir išsamus galimo DPT patikrinimas turėtų būti proporcingas funkcijos, kurią įmonė ketina perduoti, pobūdžiui, mastui ir sudėtingumui ir šiai funkcijai būdingai rizikai. Tai turėtų apimti bent galimą debesijos paslaugų perdavimo sutarties poveikio įmonės veiklos, teisinei, atitikties ir reputacijos rizikai vertinimą.

20. Jei debesijos paslaugų perdavimo sutartis susijusi su esmine ar svarbia funkcija, įmonė taip pat turėtų:

    a) įvertinti visą riziką, kuri gali kilti dėl debesijos paslaugų perdavimo sutarties, įskaitant su informacinėmis ir ryšių technologijomis, informacijos saugumu, veiklos tęstinumu susijusią riziką, teisinę ir atitikties, reputacijos riziką, veiklos riziką ir galimus įmonei taikomus priežiūros apribojimus, kylančius dėl:
        i. pasirinktos debesijos paslaugos ir pasiūlytų diegimo modelių;
        ii. perėjimo ir (arba) įgyvendinimo procesų;
        iii. funkcijos ir susijusių duomenų, kuriuos numatoma perduoti, slaptumo ir apsaugos priemonių, kurių reikėtų imtis;
        iv. įmonės ir DPT sistemų ir taikomųjų programų suderinamumo, t. y. jų gebėjimo keistis informacija ir bendrai naudotis apsikeista informacija;
        v. įmonės duomenų perkeliamumo, t. y. galėjimo įmonės duomenis lengvai perkelti iš vieno DPT į kitą ar grąžinti įmonei;
        vi. šalių (ES ar ES nepriklausančių šalių), kuriose būtų vykdomos perduotos funkcijos ir būtų saugomi perduoti duomenys, politinio stabilumo, saugumo padėties ir teisės sistemos (įskaitant galiojančias teisėsaugos nuostatas, bankroto teisės nuostatas, kurios būtų taikomos DPT bankrutavus, galiojančius duomenų apsaugos įstatymus ir tai, ar laikomasi asmens duomenų perdavimo trečiajai šaliai pagal BDAR sąlygų); jei perduotos paslaugos perduodamos subrangos būdu, papildomos rizikos, kuri gali kilti, jei subrangovas yra trečiojoje šalyje ar kitoje šalyje nei DPT, ir perduotų veiklos funkcijų perdavimo subrangos būdu atveju, bet kokios papildomos rizikos, kuri gali kilti, įskaitant riziką, kuri kyla, kai nėra tiesioginės sutarties tarp įmonės ir subrangovo, vykdančio perduotą funkciją;

vii. galimos koncentracijos įmonėje (įskaitant, jei taikoma, jos grupės lygmeniu esančią koncentraciją), susidariusios dėl kelių su tuo pačiu DPT sudarytų debesijos paslaugų perdavimo sutarčių, ir galimos koncentracijos ES finansų sektoriuje, susidariusios dėl to, kad kelios įmonės naudojasi to paties DPT ar mažos DPT grupės paslaugomis. Vertindama koncentracijos riziką, įmonė turėtų atsižvelgti į visas su tuo DPT sudarytas debesijos paslaugų perdavimo sutartis (ir, jei taikoma, jos grupės lygmeniu sudarytas debesijos paslaugų perdavimo sutartis);

b) atsižvelgti į tikėtiną debesijos paslaugų perdavimo sutarties naudą ir sąnaudas, be kita ko, palygindama bet kokią reikšmingą riziką, kuri gali būti sumažinta arba geriau valdoma, su bet kokia reikšminga rizika, kuri gali kilti dėl debesijos paslaugų perdavimo sutarties;

21. Perduodant esmines ar svarbias funkcijas, atliekamas išsamus patikrinimas turi apimti DPT tinkamumo vertinimą. Vertindama DPT tinkamumą, įmonė turėtų užtikrinti, kad DPT turėtų gerą reputaciją taip pat gebėjimus, išteklius (įskaitant žmogiškuosius, IT, finansinius), organizacinę struktūrą ir, jei taikytina, reikiamą (-us) leidimą (-us) arba registraciją (-as), kad galėtų patikimai ir profesionaliai vykdyti esminę ar svarbią funkciją ir prisiimtus įsipareigojimus visą debesijos paslaugų perdavimo sutarties galiojimo laikotarpį. Kiti veiksniai, į kuriuos reikia atsižvelgti atliekant išsamų DPT patikrinimą, gali būti šie (bet ne tik):

a) informacijos saugumo valdymas ir visų pirma asmens, konfidencialių ir kitaip neskelbtinų duomenų apsauga;
b) paslaugos palaikymas, įskaitant palaikymo planus ir kontaktinius asmenis, ir incidentų valdymo procesai;
c) veiklos tęstinumo ir atkūrimo po ekstremalių įvykių planai.

22. Jei taikoma ir siekdama prisidėti prie atlikto išsamaus patikrinimo, įmonė taip pat gali naudoti tarptautiniais standartais pagrįstus sertifikatus ir išorės ar vidaus audito ataskaitas.

23. Jeigu įmonė sužino apie didelius suteiktų paslaugų arba DPT padėties trūkumus ir (arba) reikšmingus pokyčius, reikėtų nedelsiant peržiūrėti išankstinę perdavimo analizę ir išsamų DPT patikrinimą arba prireikus atlikti jį iš naujo.

24. Jeigu įmonė su jau įvertintu DPT sudaro naują sutartį arba atnaujina jau sudarytą sutartį, ji, laikydamasi rizika pagrįsto metodo, turėtų nustatyti, ar reikia atlikti naują išsamų patikrinimą.

3 gairė. Pagrindiniai sutartiniai elementai

25. Įmonės ir DPT atitinkamos teisės ir įsipareigojimai turėtų būti aiškiai išdėstyti rašytinėje sutartyje.

26. Rašytinėje sutartyje turėtų būti aiškiai numatyta, kad įmonė prireikus sutartį gali nutraukti.

27. Perduodant esmines ar svarbias funkcijas, rašytinėje sutartyje turėtų būti nurodyta bent ši informacija:

    a) aiškus perduodamos veiklos funkcijos aprašymas;
    b) sutarties įsigaliojimo ir galiojimo pabaigos data, jei taikytina, ir DPT bei įmonei taikomi pranešimo laikotarpiai;
    c) sutartį reglamentuojantis įstatymas ir, jei yra, pasirinkta jurisdikcija;
    d) įmonės ir DPT finansiniai įsipareigojimai;
    e) ar leidžiamas veiklos funkcijų perdavimas subrangos būdu ir, jei taip, kokiomis sąlygomis, atsižvelgiant į 7 gairę;
    f) vieta (-os) (t. y. regionai arba šalys), kurioje (-iose) bus vykdoma perduota veiklos funkcija ir bus tvarkomi ir saugomi duomenys, ir sąlygos, kurių reikia laikytis, įskaitant reikalavimą pranešti įmonei, jeigu DPT pasiūlo pakeisti vietą (-as);
    g) informacijos saugumo ir asmens duomenų apsaugos nuostatos, atsižvelgiant į 4 gairę;
    h) įmonės teisė reguliariai stebėti DPT veiklą pagal debesijos paslaugų perdavimo sutartį, atsižvelgiant į 6 gairę;
    i) sutarti paslaugų lygiai, kurie turėtų apimti kiekybinius ir kokybinius veiklos rezultatus, siekiant sudaryti sąlygas laiku atlikti stebėseną, kad būtų galima nepagrįstai nedelsiant imtis atitinkamų taisomųjų veiksmų, jeigu neužtikrinamas sutartas paslaugų lygis;
    j) DPT pareiga pranešti įmonei, taip pat, kai tinkama, pareiga teikti ataskaitas, susijusias su įmonės saugumo funkcija ir pagrindinėmis funkcijomis, pvz., DPT vidaus audito funkcijos ataskaitomis;
    k) DTP incidentų valdymo nuostatos, įskaitant DPT pareigą pranešti įmonei nepagrįstai nedelsiant apie incidentus, kurie turėjo įtakos įmonės perduotos paslaugos vykdymui;
    l) nuostata, ar DPT turėtų turėti privalomą tam tikrų rūšių rizikos draudimą, ir, jei taikytina, prašomos draudimo apsaugos lygis;
    m) DPT keliami reikalavimai įgyvendinti ir tikrinti veiklos tęstinumą ir veiklos atkūrimo po ekstremaliųjų įvykių planus;
    n) DPT keliami reikalavimai suteikti įmonei, jos kompetentingai institucijai ir bet kokiam kitam įmonės ar kompetentingų institucijų paskirtam asmeniui prieigos prie atitinkamos informacijos, DPT patalpų, sistemų ir prietaisų teisę (prieigos teisę) ir teisę juos tikrinti (audito teisę) tiek, kiek tai būtina stebėti DPT darbą pagal

debesijos paslaugų perdavimo sutartį ir jo atitiktį taikytiniems normatyviniams ir sutartiniams reikalavimams, atsižvelgiant į 6 gairę;

o) nuostatos, užtikrinančios, kad galima pasiekti, atkurti ir prireikus grąžinti įmonei DPT tvarkomus ir įmonės vardu saugomus duomenis, atsižvelgiant į 5 gairę.

4 gairė. Informacijos saugumas

28. Įmonė turėtų nustatyti informacijos saugumo reikalavimus savo vidaus politikoje, procedūrose ir rašytiniame debesijos paslaugų perdavimo sutartyje ir reguliariai stebėti atitiktį šiems reikalavimams, įskaitant konfidencialių, asmens ir kitaip neskelbtinų duomenų apsaugą. Šie reikalavimai turėtų būti proporcingi funkcijos, kurią įmonė perduoda DPT, pobūdžiui, apimčiai ir sudėtingumui ir šiai funkcijai būdingai rizikai.

29. Dėl to, perduodama esmines ar svarbias veiklos funkcijas ir nepažeisdama pagal BDAR taikytinų reikalavimų, įmonė, taikydama rizika pagrįstą metodą, turėtų bent jau:

a) *informacijos saugumo organizavimas:* užtikrinti, kad būtų aiškiai atskirtos įmonės ir DPT informacijos saugumo funkcijos ir pareigos, įskaitant su grėsmių nustatymu, incidentų valdymu ir pataisų valdymu susijusias funkcijas ir pareigas, ir užtikrinti, kad DPT sugebėtų įvykdyti savo funkcijas ir pareigas;

b) *tapatybės ir prieigos valdymas*: užtikrinti, kad būtų įdiegti stiprūs tapatumo nustatymo (pavyzdžiui, daugiaveiksnio tapatumo nustatymo) mechanizmai ir prieigos kontrolės priemonės, siekiant užkirsti kelią neteisėtai prieigai prie įmonės duomenų ir vidinių debesijos išteklių;

c) *šifravimas ir kriptografinių raktų administravimas:* užtikrinti, kad prireikus būtų naudojamos atitinkamos perduodamų duomenų, duomenų atminties laikmenose, duomenų saugojimo vietose ir duomenų atsarginių kopijų šifravimo technologijos kartu su atitinkamais kriptografinių raktų administravimo sprendimais, siekiant apriboti neteisėtos prieigos prie kriptografinių raktų riziką; pasirinkdama savo kriptografinių raktų administravimo sprendimą įmonė visų pirma turėtų atkreipti dėmesį į pažangiausią technologiją ir procesus;

d) *operacijų ir tinklo saugumas:* apsvarstyti tinkamus tinklo prieinamumo lygius, tinklo atskyrimą (pavyzdžiui, nuomininko izoliavimą bendroje debesijos aplinkoje, operacinį atskyrimą žiniatinklio, taikomosios programos logiką, operacinę sistemą, tinklą, duomenų bazių valdymo sistemą (DBVS) ir saugyklos lygmenis) ir apdorojimo aplinką (pavyzdžiui, testavimą, priimtinumo vartotojui bandymus, plėtrą, gamybą)

e) *programų sąsajos (API):* apsvarstyti debesijos paslaugų integravimą į įmonės sistemas, siekiant užtikrinti API saugumą (pavyzdžiui, nustatyti ir tvarkyti informacijos saugumo politiką ir API procedūras įvairiose sistemų sąsajose, jurisdikcijas ir veiklos funkcijas, siekiant užkirsti kelią neteisėtam duomenų atskleidimui, keitimui ar sunaikinimui);

f) *veiklos tęstinumas ir atkūrimas po ekstremalių įvykių*: užtikrinti, kad būtų įdiegtos veiksmingos veiklos tęstinumo ir atkūrimo po ekstremalių įvykių kontrolės

priemonės (pavyzdžiui, nustatant minimalius pajėgumo reikalavimus, pasirenkant geografiškai pasiskirsčiusios prieglobos parinktis sudarant galimybę vieną pakeisti kita arba teikiant užklausas dėl dokumentų ir peržiūrint dokumentus, kuriuose parodytas įmonės duomenų maršrutas DPT sistemose, taip pat apsvarstant galimybę kopijuoti aparatinius atvaizdus į atskirą saugyklą, kuri yra pakankamai izoliuota nuo tinklo ar veikia atjungties režimu);

g) *duomenų saugojimo vieta*: laikytis rizika pagrįsto duomenų saugojimo ir duomenų apdorojimo vietos (-ų) (t. y. regionų ar šalių) parinkimo metodo;
h) *atitiktis ir stebėsena*: patikrinti, ar DPT laikosi tarptautiniu mastu pripažintų informacijos saugumo standartų ir įdiegė tinkamas informacijos saugumo kontrolės priemones (pavyzdžiui, reikalaujant, kad DPT pateiktų įrodymų, patvirtinančių, kad jis atlieka atitinkamą informacijos saugumo peržiūrą, ir atliekant reguliarius DPT informacijos saugumo susitarimų vertinimus ir tikrinimus).

5 gairė. Pasitraukimo strategijos

30. Perduodama esmines ar svarbias funkcijas, įmonė turėtų užtikrinti, kad ji galės pasitraukti iš debesijos paslaugų perdavimo sutarties nepagrįstai nesutrikdydama savo veiklos ir klientams teikiamų paslaugų ir nedarydama neigiamo poveikio savo įsipareigojimų pagal taikytinus teisės aktus vykdymui bei savo duomenų konfidencialumui, vientisumui ir prieinamumui. Dėl to įmonė turėtų:

a) parengti pasitraukimo planus, kurie turėtų būti išsamūs, pagrįsti dokumentais ir pakankamai išbandyti. Šie planai turėtų būti prireikus naujinami, įskaitant tuos atvejus, kai pasikeičia perduota funkcija;
b) nustatyti alternatyvius sprendimus ir sukurti perėjimo planus perduotai veiklos funkcijai ir duomenims iš DPT ir, jei taikytina, iš bet kokio subrangovo perkelti ir perduoti juos alternatyviam įmonės nurodytam DPT ar grąžinti įmonei. Šie sprendimai turėtų būti apibrėžti atsižvelgiant į problemas, kurios gali kilti dėl duomenų vietos, imantis būtinų priemonių veiklos tęstinumui pereinamuoju laikotarpiu užtikrinti;
c) užtikrinti, kad rašytinėje debesijos paslaugų perdavimo sutartyje būtų numatytas DPT įsipareigojimas palaikyti tinkamą veiklos funkcijų perdavimą ir susijusį duomenų apdorojimą iš DPT ir bet kokio subrangovo kitam įmonės nurodytam DPT ar pačiai įmonei, jei įmonė pradėtų taikyti pasitraukimo strategiją. Įsipareigojimas palaikyti tinkamą perduotos funkcijos perdavimą ir su tuo susijusį duomenų tvarkymą turėtų apimti, jei taikoma, saugų duomenų šalinimą iš DPT ir bet kokio subrangovo sistemų.

31. Rengdama a ir b punktuose nurodytus pasitraukimo planus ir sprendimus (pasitraukimo strategiją), įmonė turėtų apsvarstyti šiuos aspektus:

a) nustatyti pasitraukimo strategijos tikslus;

b) nustatyti kritinius įvykius, kurie leistų taikyti pasitraukimo strategiją. Jie turėtų apimti bent debesijos paslaugų perdavimo sutarties nutraukimą įmonės ar DPT iniciatyva, taip pat DPT nesugebėjimą vykdyti veiklą ar kitokį veiklos nutraukimą;
c) atlikti poveikio verslui analizę, atitinkančią perduotą veiklos funkciją, kad būtų galima nustatyti, kokių žmogiškųjų ir kitų išteklių reikėtų pasitraukimo strategijai įgyvendinti;
d) paskirstyti funkcijas ir pareigas pasitraukimo strategijai valdyti;
e) išbandyti pasitraukimo strategijos tinkamumą naudojant rizika pagrįstą metodą (pavyzdžiui, atliekant galimų sąnaudų, poveikio, išteklių ir laiko aspektų, susijusių su perduotos paslaugos perdavimu alternatyviam paslaugų teikėjui, analizę);
f) apibrėžti perėjimo sėkmės kriterijus.

32. Įmonė turėtų į savo vykdomą stebėseną ir pagal debesijos paslaugų perdavimo sutartį DPT teikiamų paslaugų priežiūrą įtraukti pasitraukimo strategijos kritinių įvykių rodiklius.

6 gairė. Prieigos ir audito teisės

33. Įmonė turėtų veiksmingai užtikrinti, kad debesijos paslaugų perdavimo rašytinė sutartis neribotų įmonės ir kompetentingos institucijos prieigos ir audito teisės ir DPT priežiūros galimybės.

34. Įmonė turėtų užtikrinti, kad naudojantis prieigos ir audito teisėmis (pavyzdžiui, audito periodiškumas ir tikrintinos sritys bei paslaugos) būtų atsižvelgta į tai, ar perduotos paslaugos yra susijusios su esmine ar svarbia veiklos funkcija, ir į rizikos bei poveikio, kylančių iš debesijos paslaugų perdavimo sutarties įmonės atžvilgiu, pobūdį ir mastą.

35. Jeigu naudojamasi prieigos ar audito teisėmis ar naudojantis tam tikrais audito metodais kyla rizika DPT aplinkai ir (arba) kitam DPT klientui (pavyzdžiui, darant poveikį paslaugos lygiams, duomenų konfidencialumui, vientisumui ir prieinamumui), DPT turėtų įmonei pateikti aiškią priežastį, kodėl tai keltų riziką, ir DPT turėtų susitarti su įmone dėl alternatyvių būdų panašiam rezultatui pasiekti (pavyzdžiui, įtraukti konkrečias kontrolės priemones, kurios būtų tikrinamos DPT pateiktoje konkrečioje ataskaitoje ir (arba) sertifikate).

36. Nedarydamos poveikio galutinei atsakomybei už debesijos paslaugų perdavimo sutartis, įmonės, siekdamos veiksmingiau naudoti audito išteklius ir sumažinti DPT ir jo klientams tenkančią organizacinę naštą, gali naudoti:

a) DPT pateiktus trečiosios šalies teikiamus sertifikatus ir išorės arba vidaus audito ataskaitas;
b) jungtinius auditus, atliekamus kartu su kitais to paties DPT klientais, ar jungtinius auditus, kuriuos atlieka to paties DPT kelių klientų trečiosios šalies auditorius.

37. Perduodama esmines ar svarbias funkcijas, įmonė turėtų įvertinti, ar 37 punkto a papunktyje nurodyti trečiosios šalies sertifikatai ir išorės ar vidaus audito ataskaitos yra tinkami ir juose pateikta pakankamai informacijos, kad jie atitiktų taikytinuose teisės aktuose nurodytus įsipareigojimus, ir turėtų siekti, kad ilgainiui nebūtų vadovaujamasi vien šiais sertifikatais ir ataskaitomis.

38. Perduodama esmines ar svarbias funkcijas, įmonė turėtų naudotis 37 punkto a papunktyje nurodytais trečiosios šalies sertifikatais ir išorės ar vidaus audito ataskaitomis tik tuo atveju, jeigu:

    a) užtikrinama, kad sertifikatai ar audito ataskaitos apimtų pagrindines DPT sistemas (pvz., procesus, taikomąsias programas, infrastruktūrą, duomenų centrus), įmonės nustatytas pagrindines kontrolės priemones ir atitinkamų taikytinų teisės aktų reikalavimų laikymąsi;
    b) nuolat išsamiai vertinamas sertifikatų ar audito ataskaitų turinys ir tikrinama, ar sertifikatai ar ataskaitos nėra pasenę;
    c) užtikrinama, kad pagrindinės DPT sistemos ir kontrolės priemonės būtų įtraukiamos į kitas sertifikatų ar audito ataskaitų redakcijas;
    d) įmonę tenkina sertifikavimo ar auditą atliekančios šalies teikiamos paslaugos (pavyzdžiui, atsižvelgiant į jos kvalifikaciją, patirtį, pakartotinį darbą ir (arba) įrodymų esamoje audito byloje tikrinimą bei sertifikavimo ar audito įmonės rotaciją);
    e) įmonė yra įsitikinusi, kad sertifikatai išduodami ir auditas atliekamas laikantis tinkamų standartų, įskaitant įdiegtų pagrindinių kontrolės priemonių veiksmingumo patikrinimą;
    f) turi sutartyje įtvirtintą teisę prašyti išplėsti sertifikatų ar audito ataskaitų taikymo sritį, kad būtų įtrauktos kitos svarbios DPT sistemos ir kontrolės priemonės; tokių prašymų pakeisti taikymo sritį skaičius ir dažnumas turėtų būti pagrįstas ir rizikos valdymo požiūriu teisėtas;
    g) išlaiko sutartyje įtvirtintą teisę savo nuožiūra atlikti pavienius auditus vietoje, susijusius su perduota funkcija.

39. Įmonė turėtų užtikrinti, kad prieš apsilankymą vietoje, įskaitant įmonės paskirtą trečiąją šalį (pavyzdžiui, auditorių), DPT apie tai iš anksto pranešama per pagrįstą laikotarpį, nebent iš anksto pranešti neįmanoma dėl ekstremaliosios situacijos ar krizės arba tai lemtų tokią situaciją, kai auditas nebebūtų veiksmingas. Tokiame pranešime reikėtų nurodyti apsilankymo vietą ir tikslą bei jame dalyvausiančius darbuotojus.

40. Atsižvelgdami į tai, kad debesijos paslaugos yra aukšto techninio sudėtingumo lygio ir kelia konkrečių sunkumų dėl jurisdikcijos, auditą atliekantys darbuotojai, kurie yra įmonės vidaus auditoriai ar jos vardu veikiantys auditoriai, turėtų turėti tinkamų įgūdžių ir žinių, kad tinkamai įvertintų atitinkamas debesijos paslaugas ir atliktų veiksmingą ir

aktualų auditą. Tai turėtų būti taikoma ir tiems įmonės darbuotojams, kurie peržiūri DPT pateiktus sertifikatus ar audito ataskaitas.

7 gairė. Veiklos funkcijų perdavimas subrangos būdu

41. Jei esmines ar svarbias funkcijas (arba esmines jų dalis) leidžiama perduoti subrangovams, įmonės ir DPT rašytinėje debesijos paslaugų perdavimo sutartyje reikėtų:

    a) nurodyti visas perduodamos funkcijos dalis ar aspektus, kurių negalima perduoti subrangos būdu;
    b) nustatyti sąlygas, kurių reikia laikytis perduotas paslaugas perduodant subrangos būdu;
    c) nurodyti, kad DPT išlieka atskaitingas ir privalo vykdyti tokių subrangos būdu perduotų paslaugų priežiūrą ir užtikrinti, kad visi DPT ir įmonės sutartiniai įsipareigojimai būtų nuolat įvykdomi;
    d) įtraukti DPT pareigą pranešti įmonei apie bet kokį planuojamą veiklos funkcijų perdavimą subrangos būdu ar esminius jo pakeitimus visų pirma tada, kai tai gali daryti poveikį DPT gebėjimui vykdyti pagal debesijos paslaugų perdavimo sutartį, sudarytą su įmone, prisiimtus įsipareigojimus. Rašytinėje sutartyje nustatytu pranešimo laikotarpiu įmonei turėtų būti suteikta pakankamai laiko bent siūlomo veiklos funkcijų perdavimo subrangos būdu ar jo esminių pakeitimų rizikos vertinimui atlikti ir jiems paprieštarauti ar atskirai juos patvirtinti, kaip nurodyta e punkte;
    e) užtikrinti, kad įmonė turėtų teisę nesutikti su planuojamu veiklos funkcijų perdavimu subrangos būdu ar jo esminiais pakeitimais arba reikalauti atskiro patvirtinimo prieš įsigaliojant veiklos funkcijų perdavimui subrangos būdu ar jo esminiams pakeitimams;
    f) užtikrinti, kad įmonė turėtų sutartinę teisę nutraukti su DPT sudarytą debesijos paslaugų perdavimo sutartį, jei ji prieštarautų siūlomam veiklos funkcijų perdavimui subrangos būdu ar esminiams jo pakeitimams, ir netinkamo veiklos funkcijų perdavimo subrangos būdu atveju (pavyzdžiui, kai DPT tęsia veiklos funkcijų perdavimą subrangos būdu nepranešdamas apie tai įmonei arba jis šiurkščiai pažeidžia veiklos funkcijų sutartyje nurodytas veiklos funkcijų perdavimo subrangos būdu sąlygas).

42. Įmonė turėtų užtikrinti, kad DPT tinkamai prižiūrėtų subrangovo veiklą.

8 gairė. Rašytiniai pranešimai kompetentingoms institucijoms

43. Įmonė turėtų laiku kompetentingai institucijai raštu pranešti apie planuojamas debesijos paslaugų perdavimo sutartis dėl esminės ar svarbios funkcijos. Įmonė taip pat turėtų laiku savo kompetentingai institucijai raštu pranešti apie debesijos paslaugų perdavimo

sutartis dėl funkcijos, kuri anksčiau buvo kvalifikuojama kaip neesminė ar nesvarbi, o vėliau tapo esminė arba svarbi.

44. Atsižvelgiant į proporcingumo principą įmonės rašytiniuose pranešimuose reikėtų nurodyti bent šią informaciją:

    a) debesijos paslaugų perdavimo sutarties įsigaliojimo datą ir, kai tinkama, sutarties galiojimo pratęsimo datą, galiojimo pabaigos datą ir (arba) DPT ir įmonei taikomus pranešimo laikotarpius;
    b) trumpą perduodamos veiklos funkcijos aprašymą;
    c) trumpą priežasčių, dėl kurių perduodama veiklos funkcija laikoma esmine arba svarbia, santrauką;
    d) DPT pavadinimą ir prekės ženklą (jei yra), registracijos šalį, įmonės registracijos numerį, juridinio subjekto identifikacinį numerį (jei yra), registruotą adresą, svarbius kontaktinius duomenis ir patronuojančiosios įmonės pavadinimą (jei yra);
    e) debesijos paslaugų perdavimo sutartį reglamentuojantį įstatymą ir, jei yra, pasirinktą jurisdikciją;
    f) debesijos diegimo modelius bei konkretų DPT saugotinų duomenų pobūdį ir vietas (t. y. regionus ar šalis), kuriose tokie duomenys bus saugomi;
    g) paskutinio perduotos veiklos funkcijos esmingumo ar svarbumo vertinimo datą;
    h) paskutinio DPT vertinimo ar audito datą ir trumpą pagrindinių rezultatų santrauką bei kito planuojamo rizikos vertinimo ar audito datą;
    i) įmonės asmenį ar sprendimą priimantį organą, kuris patvirtino debesijos paslaugų perdavimo sutartį;
    j) jei taikytina, visų subrangovų, kuriems subrangos būdu perduotos esminės ar svarbios funkcijos esminės dalys, pavadinimus, įskaitant šalį ar regioną, kuriame subrangovai yra įregistruoti, šalį ar regioną, kuriame bus teikiama perduota paslauga, ir šalį ar regioną, kuriame bus saugomi duomenys.

9 gairė. Debesijos paslaugų perdavimo sutarties priežiūra

45. Kompetentingos institucijos, vykdydamos savo priežiūros procesą, turėtų įvertinti riziką, kylančią iš įmonių debesijos paslaugų perdavimo sutarčių. Visų pirma vertintinos esminių ar svarbių funkcijų perdavimo sutartys.

46. Kompetentingos institucijos turėtų būti tikros, kad gali veiksmingai vykdyti priežiūrą, ypač tais atvejais, kai įmonės perduoda esminių ar svarbių veiklos funkcijų paslaugas, vykdomas už ES ribų.

47. Vadovaudamosi rizika pagrįstu metodu, kompetentingos institucijos turėtų įvertinti, ar įmonės:

    a) turi įdiegtus atitinkamus valdymo, išteklių ir veiklos procesus, kad tinkamai ir veiksmingai sudarytų, įgyvendintų ir prižiūrėtų debesijos paslaugų perdavimo sutartis;

b) nustato ir valdo visą su perduotomis debesijos paslaugomis susijusią riziką.

48. Nustačiusios koncentracijos riziką, kompetentingos institucijos turėtų stebėti tokios rizikos raidą ir įvertinti tiek jos galimą poveikį kitoms įmonėms, kurias jos prižiūri, tiek finansų rinkos stabilumui.