EUROOPA KESKPANK
PANGANDUSJÄRELEVALVE

EKP juhend pilvteenuste edasiandmise kohta pilvteenuste osutajatele

1 Sissejuhatus

Euroopa Keskpank (EKP) möönab, et pilvteenuste kasutamine pakub järelevalve alla kuuluvatele üksustele mitmesuguseid eeliseid. Organisatsioonisisese info- ja kommunikatsioonitehnoloogia (IKT) taristuga võrreldes on pilvteenused kulutõhusad, skaleeritavad ja turvalised, kuna teenuseosutajad kasutavad tipptasemel turvatehnoloogiaid. Ühtlasi on need teenused andmevarundamise lahenduste ja avariitaastevõimaluste tõttu vastupidavad ning annavad järelevalve alla kuuluvatele üksustele juurdepääsu uuenduslikele tehnoloogiatele.

Samal ajal on pilvteenuste turg väga kontsentreeritud ning paljud nende teenuste osutajad tuginevad omandtehnoloogiatele, eelkõige SaaSi (*software as a service*, tarkvara teenusena) ja PaaSi (*platform as a service*, platvorm teenusena) hankemudelite puhul. Seetõttu toob pilvteenuste kasutamine järelevalve alla kuuluvatele üksustele kaasa mitmeid riske, mis on seotud sõltuvusega kolmandast isikust IKT-teenuste osutajatest. Ühtlasi tekitab nende teenuste olemus probleeme seoses pilvtehnoloogiast tulenevate riskide juhtimisega ning pakutavate pilvteenuste jälgimise ja auditeerimisega.

1.1 Eesmärk

EKP juhend pilvteenuste edasiandmise kohta pilvteenuste osutajatele (edaspidi „EKP juhend”) tugineb kolmele põhitegurile.

Esiteks liiguvad järelevalve alla kuuluvad üksused üha enam organisatsioonisisese info- ja kommunikatsioonitehnoloogia (IKT) taristu ja ressursside kasutamiselt pilvteenuse osutajate pakutavate pilvteenuste kasutamisele.[1] Kõnealused järelevalve alla kuuluvad üksused peavad neid tehnoloogiaid mõistma, hindama ja jälgima.

Teiseks on EKP tuvastanud puudusi seoses IKT-teenuste edasiandmisega, mida järelevalve alla kuuluvad üksused peavad kõrvaldama, et parandada oma tegevuskerksust. See on sätestatud EKP pangandusjärelevalve 2024.–2026. aasta järelevalveprioriteetides.

[1] Järelevalve alla kuuluvate üksuste ja pilvteenuse osutajate vaheliste suhete käsitlemisel viidatakse EKP juhendis üksnes hangitud pilvlahenduste portfellile, mitte pilvandmetöötlusega mitteseotud toodetele, mida asjaomased teenuseosutajad võivad pakkuda.

Kolmandaks võttis Euroopa Liit hiljuti vastu digitaalse tegevuskerksuse määruse (DORA)[2] eesmärgiga koondada kokku ja ajakohastada osana operatsiooniriski nõuetest IKT-riskidega seotud nõuded, mis sisaldavad kolmandast isikust tuleneva IKT-riski usaldusväärse juhtimise peamisi põhimõtteid. Digitaalse tegevuskerksuse määruse artikli 5 ja kapitalinõuete direktiivi[3] artikli 74 nõuded tulenevad vajadusest sisse seada IKT-riski tõhus juhtimine (sealhulgas eelkõige kolmandast isikust tuleneva IKT-riski juhtimine) ning IKT-turbe ja küberkerksuse raamistikud. Need peavad võimaldama ennetavalt tegeleda maandamata riskidega, mis võivad põhjustada märkimisväärseid häireid kriitilise tähtsusega või olulistes funktsioonides või teenustes. Asjaomaste nõuete kohaldamisel peaksid järelevalve alla kuuluvad üksused arvesse võtma ärimudelis ja järelevalve alla kuuluva üksuse tegevuses peituvate riskide laadi, ulatust ja keerukust.

Nagu ka teiste EKP juhendite puhul, ei ole käesolevas juhendis sätestatud nõuded õiguslikult siduvad. Ühtlasi ei tohiks seda tõlgendada nii, nagu kehtestataks sellega uusi eeskirju või nõudeid, mis on rangemad praegu digitaalse tegevuskerksuse määruse ja selle rakendusaktidega kehtestatud normidest või nõuetest. Samuti ei asendata sellega liidu või siseriiklikust õigusest tulenevaid asjakohaseid õiguslikke nõudeid.

EKP juhendi eesmärk on selgitada EKP ootusi seoses digitaalse tegevuskerksuse määruses sätestatud nõuetega, edendades seeläbi järelevalvetegevuse järjepidevust ja aidates läbipaistvuse võimaldamise kaudu tagada võrdsed tingimused.

EKP juhendis esitatakse ka näiteid täheldatud heade tavade kohta, tuginedes pideva ja kohapealse järelevalvetegevuse käigus saadud kogemustele ning pangandussektoriga peetavast pidevast dialoogist saadud tagasisidele. Nende heade tavade eesmärk on tuua välja konkreetsed näited tegevustest, mida EKP peab asjakohaseks. EKP möönab, et järelevalve alla kuuluvate üksuste eripära silmas pidades ei kasutata kõiki häid tavasid tingimata kõigis järelevalve alla kuuluvates üksustes ning et võib esineda ka teisi näiteid headest tavadest, mis aitavad samuti kaasa tegevuse edasiandmisega seotud riski tõhusale juhtimisele.

2 Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, 14. detsember 2022, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).

3 Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, 26. juuni 2013, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338).

Juhendis kasutatud mõisted	
Pilvteenuse osutaja	Teenuseosutaja, kes vastutab pilvteenuste osutamise eest tegevuse edasiandmise lepingu alusel.
Pilvteenused	Suuniste EBA/GL/2019/02 2. peatüki lõike 12 kohaselt teenused, mida osutatakse pilvtöötluse abil. Selle all peetakse silmas mudelit, mis võimaldab ulatuslikku ja mugavat nõudepõhist juurdepääsu konfigureeritavate andmetöötlusressursside jagatud võrgustikule (nt võrgud, serverid, andmetalletus, rakendused ja teenused), mida on võimalik kiiresti pakkuda ja vabastada minimaalsete halduslike jõupingutuste või minimaalse teenuseosutajate vahelise suhtluse kaudu.
Ühispilv	Suuniste EBA/GL/2019/02 2. peatüki lõike 12 kohaselt pilvetaristu, mida saab kasutada üksnes konkreetne krediidiasutuste või makseasutuste kogukond, sealhulgas ühe grupi mitmed krediidiasutused.
Kriitilise tähtsusega või oluline funktsioon	Digitaalse tegevuskerksuse määruse artikli 3 lõike 22 kohaselt funktsioon, mille katkestus kahjustaks oluliselt finantssektori ettevõtja finantstulemusi või tema teenuste ja tegevuse usaldusväärsust või jätkuvust, või kahjustaks selle funktsiooni häiritud, vigane või ebaõnnestunud täitmine oluliselt finantssektori ettevõtja tegevusloast tulenevate tingimuste ja kohustuste või tema muude, kohaldatava finantsteenuseid käsitleva õiguse kohaste kohustuste jätkuvat täitmist.
Head tavad	Heade tavade all mõistetakse näiteid pangandussektoris kohaldatavatest tavadest, mida ühised järelevalverühmad või kohapealse kontrolli meeskonnad peavad asjakohaseks ja mida EKP soovitab järgida. Siinses juhises on need esitatud näitlikustamise eesmärgil.
Hübriidpilv	Suuniste EBA/GL/2019/02 2. peatüki lõike 12 kohaselt pilvetaristu, mis koosneb kahte või enamat tüüpi pilvetaristust.
Identiteedi- ja juurdepääsuhalduse põhimõtted	Eeskirjad ja protokollid, millega määratakse kindlaks ja kontrollitakse, kuidas antakse üksikisikutele või üksustele juurdepääs organisatsiooni IKT-keskkonna süsteemidele, rakendustele, andmetele ja ressurssidele.
Taristu teenusena (*infrastructure as a service*, IaaS)	Pilvtöötluse mudel, mille puhul müüja tagab kliendile töötlemis-, talletus-, võrgu- ja muud põhilised arvutiressursid ning klient saab ise kasutusele võtta ja käitada enda valitud tarkvara (sh operatsioonisüsteemid ja rakendused). Klient ei halda ega kontrolli pilvetaristut, kuid kontrollib operatsioonisüsteeme, andmetalletust ja rakendusi ning tal võib olla piiratud kontroll valitud võrgukomponentide (nt hostitulemüürid) üle.[4]
IKT-vara	Digitaalse tegevuskerksuse määruse artikli 3 lõike 7 kohaselt järelevalve alla kuuluva üksuse kasutatavates võrgu- ja infosüsteemides sisalduva tark- või riistvara komponent.
IKT kontsentratsioonirisk	Digitaalse tegevuskerksuse määruse artikli 3 lõike 29 kohaselt suhe ühe või mitme seotud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga, mis tekitab nendest teenuseosutajatest teatava sõltuvuse, nii et juhul, kui kõnealused teenuseosutajad ei ole kättesaadavad, muutuvad maksejõuetuks või omavad muid puudusi, võib sattuda ohtu finantsüksuse suutlikkus täita kriitilise tähtsusega või olulisi funktsioone või tulla toime muud liiki negatiivse mõju, sealhulgas suure kahjuga, või võib sattuda ohtu liidu kui terviku finantsstabiilsus.
Sõltuvus IKT-teenuste osutajast	Seotus ühe või mitme seotud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga, mis tekitab nendest teenuseosutajatest teatava sõltuvuse, nii et see seab ohtu krediidiasutuse suutlikkuse tõhusalt loobuda pakutavatest teenustest.
Tegevuse edasiandmine	Suuniste EBA/GL/2019/02 2. peatüki punkti 12 kohaselt mis tahes vormis töökorraldus krediidiasutuse, investeerimisühingu, makse- või e-raha asutuse ja teenuseosutaja vahel, mille käigus teenuseosutaja viib läbi protsessi, teenuse või tegevuse, mida vastasel juhul teostaks finantseerimis-, makse- või e-raha asutus ise.
Platvorm teenusena (PaaS)	Pilvtöötluse mudel, mille puhul klient saab pilvetaristul kasutada enda loodud või omandatud rakendusi, mis on välja töötatud teenuseosutaja toetatavate programmikeelte, teekide (infokandjate kogud), teenuste ja vahendite abil. Klient ei halda ega kontrolli aluseks olevat pilvetaristut (sh võrk, serverid, operatsioonisüsteemid ja andmetalletus), kuid omab kontrolli kasutusele võetud rakenduste üle ja võimalik, et ka rakenduste majutuskeskkonna konfiguratsiooni üle.
Privaatpilv	Suuniste EBA/GL/2019/02 2. peatüki punkti 12 kohaselt pilvetaristu, mis on kättesaadav ainukasutuseks ühele ainsale järelevalve alla kuuluvale üksusele.
Avalik pilv	Suuniste EBA/GL/2019/02 2. peatüki punkti 12 kohaselt pilvetaristu, mis on kättesaadav avalikuks kasutamiseks üldsuse poolt.
Teenuseosutaja	Suuniste EBA/GL/2019/02 2. peatüki punkti 12 kohaselt kolmas isik, kes tegevuse edasiandmise lepingu alusel teostab edasiantud protsessi, teenust või tegevust või selle osa.
Tarkvara teenusena (SaaS)	Ärimudel, mille puhul klient saab kasutada pilvetaristus kättesaadavaid teenuseosutaja rakendusi. Rakendused on eri kliendiseadmetest kättesaadavad kas kõhnklientliidese kaudu (nt veebibrauseri kaudu, nagu veebimeili puhul) või programmiliidese kaudu. Tarbija ei halda ega kontrolli pilvetaristut (sh võrk, serverid, operatsioonisüsteemid ja andmetalletus ning ka konkreetsed rakendusevõimed), välja arvatud mõnel juhul kasutajapõhiste rakenduste piiratud konfiguratsioonid.
Edasiantud tegevuse edasiandmine	Suuniste EBA/GL/2019/02 2. peatüki punkti 12 kohaselt olukord, kui teenuseosutaja vastavalt tegevuse edasiandmise lepingule annab edasiantud tegevuse edasi teisele teenuseosutajale.

[4] Põhineb USA riikliku standardite ja tehnoloogia instituudi kasutataval määratlusel.

Järelevalveootused	EKP seisukoht sellest, kuidas järelevalve alla kuuluvad üksused peaksid kohaldama liidu või riigisisese õiguse kehtivaid sätteid tegevuse edasiandmisega seotud riski tõhusaks juhtimiseks.

1.2 Ulatus ja mõju

EKP juhend käsitleb pilvteenuste edasiandmist pilvteenuste pakkujatele.

EKP juhendis sätestatud järelevalveootused on suunatud EKP pangandusjärelevalve otsese järelevalve alla kuuluvatele krediidiasutustele. Järelevalveootused väljendavad EKP arusaama sellest, kuidas järelevalve alla kuuluvad üksused peaksid kohaldama liidu või riigisisese õiguse kehtivaid sätteid tegevuse edasiandmisega seotud riski tõhusaks juhtimiseks. Need on koostatud viisil, mis on pilvteenuste edasiandmisega seotud küsimuste puhul kooskõlas digitaalse tegevuskerksuse määrusega. Ootusi tuleks mõista kooskõlas digitaalse tegevuskerksuse määruse artiklis 4 sätestatud proportsionaalsuse põhimõttega. EKP juhendis sisalduvaid viiteid liidu direktiividele tuleks käsitada viidetena, mis hõlmavad kõiki õigusakte, millega need direktiivid riigisisesesse õigusesse üle võetakse.

Järelevalve alla kuuluvate üksuste ja pilvteenuse osutajate vaheliste suhete käsitlemisel viidatakse EKP juhendis üksnes pilvlahenduste portfellile, mitte pilvandmetöötlusega mitteseotud toodetele, mida asjaomased teenuseosutajad võivad pakkuda. Kui kolmandast isikust teenuseosutaja, kes ise pilvteenuseid ei paku, tugineb pilvteenustele, mis tulemuslikult toetavad järelevalve alla kuuluva üksuse kriitilise tähtsusega või olulisi funktsioone, kehtivad tema suhtes samad järelevalveootused.

2 Järelevalveootused

2.1 Pilvteenuste juhtimine

EKP soovitab, et järelevalve alla kuuluv üksus pööraks IKT-riski juhtimise raamistiku osana erilist tähelepanu pilvteenuste kasutamisega seotud rollidele ja kohustustele, teeks enne pilvteenuse osutajaga lepingu sõlmimist põhjaliku riskihindamise ning tagaks kooskõla oma pilvestrateegia ja üldise strateegia vahel.

2.1.1 Järelevalve alla kuuluvate üksuste täielik vastutus

Järelevalve alla kuuluvad üksused peaksid tagama, et nad kehtestavad pilvteenuste edasiandmiseks asjakohase juhtimisraamistiku[5] ning seega kontrolli ja järelevalve

[5] Juhtimisraamistik loetakse asjakohaseks, kui see vastab digitaalse tegevuskerksuse määruse artikli 5 ja kapitalinõuete direktiivi artikli 74 nõuetele.

selle üle. See raamistik peaks hõlmama asjaomaste funktsioonide ja organite rollide ja kohustuste määratlusi.

Pilvteenuste edasiandmisega kaasneb nii pilvteenuse osutajale kui ka järelevalve alla kuuluvale üksusele tegevusvastutus ning see muudab kohustuste selge ja üheselt mõistetava jaotuse keerulisemaks. Digitaalse tegevuskerksuse määruse artikli 5 lõike 2 kohaselt vastutab IKT-riski juhtimise eest lõplikult siiski järelevalve alla kuuluva üksuse juhtorgan. Järelevalve alla kuuluv üksus peaks tagama, et pilvteenuste hankimisel oleksid rollid ja vastutusvaldkonnad asutusesiseselt selgelt mõistetavad ja määratletud ning lepingus kokku lepitud.

Digitaalse tegevuskerksuse määruse artikli 28 lõike 1 kohaselt peavad järelevalve alla kuuluvad üksused juhtima kolmandast isikust tulenevat IKT-riski oma IKT-riski juhtimise raamistikus IKT-riski lahutamatu osana. EKP peab heaks tavaks, et IKT-teenuseid edasi andvad järelevalve alla kuuluvad üksused kohaldavad riskijuhtimise tavade, protsesside ja kontrollimeetmete (sh IKT-turbe) suhtes samal tasemel hoolsusmeetmeid kui need üksused, kes otsustavad asjaomased teenused korraldada asutusesiseselt. Seega peetakse järelevalve alla kuuluvate üksuste puhul heaks tavaks tagada, et neile pilvteenuste osutajad on sisse seadnud samaväärsed riskijuhtimistavad, -protsessid ja -kontrollid.

2.1.2 Riskide eelnev hindamine

Digitaalse tegevuskerksuse määruse artikli 28 lõike 4 kohaselt peavad järelevalve alla kuuluvad üksused enne pilvteenuse osutajaga uue lepingu sõlmimist tegema riskianalüüsi ehk eelneva riskihindamise, mis hõlmab teatud konkreetseid elemente. Selleks et nõuetekohaselt kindlaks teha ja hinnata kõiki asjakohaseid pilvteenuste edasiandmisega seotud riske, peaksid järelevalve alla kuuluvad üksused hea tava kohaselt:

- põhjalikult analüüsima tuvastatud asjakohaste riskide jaoks kehtestatud kontrolliprotsesse ning seda, kuidas tõhusalt integreerida järelevalve alla kuuluva üksuse ja talle pilvteenuseid osutava ettevõtte kontrollimehhanismid;
- hindama pilvteenuse osutaja suutlikkust esitada nende kontrollide jaoks vajalikku teavet;
- tagama, et pilvteenuse osutaja ise on asjakohaseid kontrolle nõuetekohaselt rakendanud;
- hindama, kas järelevalve alla kuuluval üksusel on nende kontrollide rakendamiseks ja tegemiseks vajalikud teadmised ja inimressursid;
- kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste puhul hindama riske, mis on seotud tegevuse edasiandmise pikkade ja keerukate alltöövõtuahelatega, pidades silmas digitaalse tegevuskerksuse määruse artikli 29 lõikes 2 sätestatud nõudeid.

Hea tava kohaselt tuleks riskide eelneval hindamisel arvesse võtta järgmisi riske:

- sõltuvust teenuseosutajast ja võimalikke probleeme, mis võivad tekkida alternatiivse teenuseosutaja leidmisel, kui on vaja lepingust väljuda;
- andmetalletus- ja -töötlemisriske, samuti tundlike andmete kaotsimineku, muutmise, hävitamise või ilma loata avalikustamise tõenäosust;
- füüsilisi riske ja piirkondlikke riske (nt riskid, mis on seotud selle riigi poliitilise stabiilsusega, kus teenuseid osutatakse ja/või andmeid talletatakse);
- ohtu, et kvaliteet langeb märkimisväärselt või hind märkimisväärselt tõuseb (mõlemad on väga kontsentreeritud turu puhul tavalised);
- mitme asuriga (st pilvteenuste mitme kasutajaga) keskkonnast tulenevaid riske.

Infokast 1

Kontsentratsiooniriski ja teenuseosutajast sõltuvusse jäämise riski hindamine

Nagu on kirjeldatud punktis 2.1.2, näeb digitaalse tegevuskerksuse määruse artikli 28 lõike 4 punkt c ette, et järelevalve alla kuuluvad üksused peavad tegema eelneva riskihindamise, et tuvastada ja hinnata kõiki lepinguliste tingimustega seotud asjakohaseid riske, sealhulgas artiklis 29 osutatud IKT kontsentratsiooniriski. EKP leiab, et järelevalve alla kuuluvate üksuste jaoks on riskide hindamisel hea tava kaaluda lisaks andmete asukohaga seotud aspektidele ka tüüpilisi pilvteenustega seotud riske (nt suurem sõltuvus ühest teenuseosutajast, raskemini prognoositavad kulud, auditeerimise suurem keerukus, osutatavate funktsioonide kontsentratsioon ja läbipaistmatus seoses allteenuseosutajate kasutamisega). EKP on seisukohal, et eriti kontsentratsiooniriski puhul on hea tava teha sellist riskihindamist korrapäraselt, kuna teenuseosutajate praktikad võivad aja jooksul muutuda, võttes muu hulgas arvesse pilve skaleeritavust (mis võimaldab seda uute funktsioonide lisamiseks järk-järgult laiendada, avaldades võimalikku mõju kontsentratsiooniriskile). Tungivalt soovitatav on korrapäraselt läbi vaadata, mil määral järelevalve alla kuuluv üksus sõltub mõnest konkreetsest teenuseosutajast (sh nende hangitud teenuste puhul, mis on konkreetsetele pilvteenuse osutajatele alltöövõtu korras edasi antud). Kontsentratsiooniriski võib süvendada teadmiste puudumine teiste pilvteenuse osutajate omandtehnoloogia kohta, mis raskendab ümberlülitumist või lepingutest väljumist ning suurendab nendega seotud kulusid (nn sõltuvusse jäämise risk). Ideaaljuhul tuleb sellist kontsentratsiooniriski arvesse võtta ka kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise põhimõtetes.[6]

[6] See on sätestatud ka kolmandast isikust IKT-teenuste osutajaid käsitlevate regulatiivsete tehniliste standardite artikli 1 punktis h. Vt komisjoni delegeeritud määrus (EL) 2024/1773, 13. märts 2024, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, et täpsustada põhimõtete üksikasjalikku sisu seoses lepingutega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist (ELT L, 2024/1773, 25.6.2024).

2.1.3 Järelevalve alla kuuluva üksuse pilvestrateegia ja üldise strateegia vaheline kooskõla

Digitaalse tegevuskerksuse määruse artikli 6 lõike 3 kohaselt peavad järelevalve alla kuuluvad üksused minimeerima IKT-riski mõju, võttes kasutusele asjakohased strateegiad, põhimõtted, menetlused, IKT-protokollid ja -vahendid. Sama määruse artikli 28 lõike 2 kohaselt peab järelevalve alla kuuluval üksusel olema strateegia, mis hõlmab kolmandast isikust tulenevat IKT-riski, sealhulgas pilvteenuse osutajale tegevuse edasiandmisest tulenevat riski. Määruses nõutud strateegia võidakse lisada järelevalve alla kuuluva üksuse digitaalse tegevuskerksuse strateegiasse või üldisesse tegevuse edasiandmise strateegiasse, milles käsitletakse pilvteenuste küsimusi. Digitaalse tegevuskerksuse määruse põhjenduses 45 märgitakse, et mis tahes kolmandast isikust tuleneva IKT-riski strateegia peaks olema kooskõlas järelevalve alla kuuluva üksuse üldstrateegiaga. Samal ajal peetakse heaks tavaks, et kolmandast isikust tuleneva IKT-riski strateegia on kooskõlas järelevalve alla kuuluva üksuse digitaalse tegevuskerksuse strateegiaga ning selle sise-eeskirjade ja protsessidega, sealhulgas tema IKT-riski valmidusega.

2.2 Pilvteenuste kättesaadavus ja kerksus

Selleks et järelevalve alla kuuluv üksus saaks tõsiste häirete korral järjepidevalt tegutseda, tuleks üldiste talitluspidevuse põhimõtete raames kindlaks määrata asjakohased IKT talitluspidevuse meetmed. EKP peab heaks tavaks, et järelevalve alla kuuluvatel üksustel on terviklik vaade pilvlahenduste talitluspidevuse meetmetele. Ühtlasi esitab EKP siinses juhendis head tavad kriitilise tähtsusega või olulisi funktsioone toetavate pilvteenustega seotud kerksusmeetmete rakendamiseks, eelkõige pilvteenuse osutaja avariitaastekavade hindamiseks.

Tulenevalt pilvteenuste ülesehituse erilisest viisist on pilvteenuse osutajal tehniline suutlikkus lõpetada mis tahes kliendi mis tahes teenus/juurdepääs mis tahes ajahetkel nii, et mõni teine pilvteenuse osutaja või järelevalve alla kuuluv üksus ise ei saa teenuse osutamist jätkata. EKP peab heaks tavaks, et järelevalve alla kuuluvad üksused koostavad asjakohased talitluspidevuse põhimõtted, et tagada enda suutlikkus sellise stsenaariumiga toime tulla ja omada juurdepääsu asjaomase teenuse osutamiseks vajalikele andmetele.

2.2.1 Terviklik vaade pilvlahenduste talitluspidevuse meetmetele

Nagu on osutatud kapitalinõuete direktiivi artikli 85 lõikes 2, peavad järelevalve alla kuuluval üksusel olema situatsiooni- ja talitluspidevuse kavad, mis tagavad tema võime tegutseda järjepidevalt ja piirata kahju majandustegevuse tõsiste häirete korral. Digitaalse tegevuskerksuse määruse artikli 11 lõike 1 kohaselt peavad järelevalve alla kuuluvad üksused kehtestama laiahaardelised IKT talitluspidevuse põhimõtted. Pilvteenuseid valides – eelkõige kriitilise tähtsusega või oluliste funktsioonide jaoks – peaks järelevalve alla kuuluv üksus tagama talitluspidevus-, kerksus- ja avariitaastevõimekuse.

Digitaalse tegevuskerksuse määruse artikli 12 kontekstis peab EKP heaks tavaks, et järelevalve alla kuuluvate üksuste pilvteenustega seotud reageerimis- ja taastekavad hõlmavad varunduspõhimõtteid ja -menetlusi ning ennistamis- ja taastamismenetlusi ning -meetodeid, et leevendada olukorda, kus pilvteenuse osutaja teenused katkevad või pilvteenuse osutaja satub tervikuna raskustesse. Varundamisele kuuluvate andmete ulatus ja varundamise minimaalne sagedus peaks põhinema teabe olulisusel või andmete konfidentsiaalsustasemel. EKP peab heaks tavaks, et andmete ja süsteemide säilitamiseks ja taastamiseks vajalike lahenduste valimisel võetakse arvesse riskihinnangut. Ühtlasi soovitab EKP järelevalve alla kuuluvatel üksustel arvestada oma riskihinnangus asjaoluga, et varuandmed ja -süsteemid salvestatakse IKT-süsteemides füüsiliselt ja on loogiliselt eraldatud andmete allikaks olevatest IKT-süsteemidest. Sõltuvalt riskihindamise tulemusest võidakse varundamismeetodites kasutada sama pilvteenuse osutaja, mõne teise pilvteenuse osutaja, pilvteenuseid mitteosutava teenusepakkuja või kohapealseid vahendeid. Kooskõlas digitaalse tegevuskerksuse määruse artikli 12 lõikega 2 tuleb varundusmenetlusi ning ennistamis- ja taastamismenetlusi ja meetodeid perioodiliselt testida. On hea tava, et testide käigus kontrollitakse ennistamis- ja taastamismenetluste ning meetodite täpsust, täielikkust ja praktilisust.

Digitaalse tegevuskerksuse määruse artikli 12 lõike 6 täiendamiseks peab EKP heaks tavaks, et talitluspidevuse juhtimise meetmed käsitlevad halvimat võimalikku stsenaariumit, mille puhul mõned või kõik asjaomased pilvteenused (mida osutab üks või mitu pilvteenuse osutajat) ei ole kättesaadavad.

2.2.2 Proportsionaalsed nõuded kriitilise tähtsusega või olulistele funktsioonidele

Kapitalinõuete direktiivi artikli 85 lõikes 2 ja digitaalse tegevuskerksuse määruse artikli 6 lõikes 8 sätestatud nõuete kohaselt peab järelevalve alla kuuluv üksus hindama edasiantud pilvteenuste ja hallatavate andmete kerksusnõudeid ning lähtudes riskipõhisest lähenemisviisist ja kooskõlas proportsionaalsuse põhimõttega, kehtestama pilvteenustele asjakohased kerksusmeetmed. Allpool on loetletud võimalikud meetmed, mida peetakse heaks tavaks praegu kättesaadavate tavapäraste talitluspidevusmudelite puhul. Loetelu ei ole ammendav ega hõlma kõiki stsenaariumeid:

- Mitu aktiivset andmekeskust eri geograafilistes asukohtades, millel on sõltumatud toiteallikad ja võrguühendused, mis võimaldavad ümber lülitada muus füüsilises asukohas asuvale andmekeskusele, kui asjaomane andmekeskus ei ole enam kättesaadav. Kriitilise tähtsusega või oluliste funktsioonide puhul ei pruugi piisata kahest reaalajas sünkroonitavast andmekeskusest ühes ja samas füüsilises asukohas.
- Hübriidpilvearhitektuuri kasutamine.

- Mitu pilvteenuse või varundusteenuse osutajat, tingimusel et nende andmekeskused ja füüsilised asukohad ei kattu, kui nad jagavad samu andmekeskusi.

Kooskõlas digitaalse tegevuskerksuse määruse artikliga 12 peab EKP heaks tavaks, et järelevalve alla kuuluv üksus tagab, et kriitilise tähtsusega või oluliste funktsioonide puhul ei põhjusta pilvteenuse osutajale edasiantud pilvteenuste järsk lõpetamine äritegevuse häireid, mis ületavad järelevalve alla kuuluva üksuse IKT talitluspidevuse kavas kindlaksmääratud maksimaalset lubatud seisuaega või andmekadu.

2.2.3 Pilvteenuse osutaja avariitaastestrateegia kavandamise, kehtestamise, testimise ja rakendamise järelevalve

Digitaalse tegevuskerksuse määruse artikli 11 lõike 6 kohaselt peavad järelevalve alla kuuluvate üksuste testimiskavad sisaldama muu hulgas stsenaariumeid, mis käsitlevad küberründe id ning esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust. EKP peab heaks tavaks, et järelevalve alla kuuluv üksus hindab oma pilvteenuse osutaja avariitaastekavasid ja -teste ning ei tugine üksnes asjaomastele avariitaastesertifikaatidele. Pilvteenuse osutaja avariitaastetesti hindamisel soovitatakse järelevalve alla kuuluval üksusel hinnata teenuseosutaja valmisolekut tegelikuks avariijuhtumiks. On soovitatav, et testimiskava hõlmab mitmesuguseid avariitaastestsenaariumeid (sealhulgas komponentide tõrked, töötluskoha täielik kadu, piirkonna kadu ja osalised tõrked). Digitaalse tegevuskerksuse määruse artikli 11 lõike 6 punkti a kohaselt tuleb neid stsenaariumeid katsetada vähemalt kord aastas vastavalt järelevalve alla kuuluva üksuse strateegiale ning kooskõlas tema talitluspidevuse põhimõtete ja nõuetega.

EKP hinnangul on hea tava, kui järelevalve alla kuuluva üksuse ja pilvteenuse osutaja avariitaastemenetluses osalevatel töötajatel on kindlaksmääratud rollid ja väljaõpe, et tagada nende asjakohased oskused ja teadlikkus oma kohustustest. Pilvteenuse osutaja avariitaastetestide hindamisel peaks järelevalve alla kuuluv üksus tagama, et pilvteenuse osutaja läbiviidavad testid hõlmaksid kõiki tema vastutusalas olevaid komponente.

Samuti tuleks hea tava kohaselt dokumenteerida ja analüüsida testimise käigus tuvastatud puudusi, et määrata kindlaks parandusmeetmed. See hõlmab asjakohaseid juhtorganeid, kes koostavad paranduskava (mis sisaldab üksikasju vajalike rollide ja vastutusvaldkondade kohta) ja jälgivad selle täitmist.

2.3 IKT- ja andmeturve, konfidentsiaalsus ja terviklikkus

Kui järelevalve alla kuuluvad üksused ühendavad oma sisesüsteemid pilvepõhiste rakendustega, kaasavad nad oma turvaaladesse ka pilvplatvormi. Sel juhul on oluline riske hoolikalt hinnata ja teha nende riskide juhtimise kohta teadlikke otsuseid. Selles protsessis tuleks arvesse võtta ka digitaalse tegevuskerksuse

määruse artiklis 9 ja artikli 28 lõikes 5 ning seda määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1774 artiklis 11 sätestatud nõudeid[7]. Sellest tulenevalt peavad järelevalve alla kuuluvad üksused kaitsma oma andmeid (sealhulgas asjaomaseid varukoopiaid) loata juurdepääsu eest, kasutades selleks näiteks andmete tõhusat krüpteerimist ja kohandades oma kaitsemeetmeid pidevalt vastavalt küberohtudele. Digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1774 artikli 6 kohaselt hõlmab see andmete krüptimist edastamise, jõudeoleku või vajaduse korral kasutamise ajal, asjakohaste krüptimismeetodite kasutamist kooskõlas järelevalve alla kuuluva üksuse andmete tundlikkustasemete liigitamise põhimõtetega ning riskipõhise lähenemisviisi järgimist.

Edastamisel ja jõudeolekus olevate andmete turvalisuse ja täpsuse tagamine on põhinõuded, mida tuleb pilvteenuste, sealhulgas pilvetaristu kasutamisel järgida. Nende nõuete täitmata jätmisel võib tekkida tõsine mainekahju ja sellel võib olla märkimisväärne finantsmõju.

Järelevalve alla kuuluvatel üksustel, kes pilvteenuseid edasi annavad, säilib vastutus oma andmete eest. Nii nagu nähakse ette isikuandmete kaitse üldmääruses[8] ja isikuandmeid käsitlevates Euroopa Andmekaitsenõukogu suunistes[9] sätestatud nõuetes, leiab ka EKP, et järelevalve alla kuuluvatel üksustel on hea tava piirata kohti, kus pilvteenuse osutajad saavad oma andmeid säilitada, ning kohaldada asjakohaseid mehhanisme nende piirangute täitmise kontrollimiseks, tagades samal ajal vajaduse korral juurdepääsu andmetele.

2.3.1 Asjakohaste andmeturbemeetmete sisseseadmine

Digitaalse tegevuskerksuse määruse artikli 9 lõike 4 punkti d kohaselt peavad järelevalve alla kuuluvad üksused rakendama krüptovõtmete kaitsmise meetmeid, mille puhul andmed krüptitakse heakskiidetud andmete liigituse ja IKT-riski hindamise protsesside põhjal. Seda nõuet on täpsustatud digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1774 artiklites 6 ja 7. Nende sätete täiendamiseks võib allpool loetletud meetmeid pidada headeks tavadeks asjakohaste krüptimis- ja krüptovõtmete haldamise protsesside sisseseadmise tagamisel.

- Kehtestatud on üksikasjalikud põhimõtted ja menetlused, mis reguleerivad andmete krüptimise ja krüptokontrollide kogu elutsüklit, sealhulgas võtmele juurdepääsutaotluste põhjendamise protsessi, mida iseloomustavad digitaalse tegevuskerksuse määruse artikli 9 lõikes 3 kindlaks määratud omadused.

[7] Komisjoni delegeeritud määrus (EL) 2024/1774, 13. märts 2024, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 seoses regulatiivsete tehniliste standarditega, millega määratakse kindlaks IKT-riski juhtimise vahendid, meetodid, protsessid ja põhimõtted ning lihtsustatud IKT-riski juhtimise raamistik (ELT L, 2024/1774).

[8] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus; ELT L 119, 4.5.2016, lk 1).

[9] Näiteks suunised 10/2020 isikuandmete kaitse üldmääruse artikli 23 kohaste piirangute kohta või suunised 05/2021 isikuandmete kaitse üldmääruse artikli 3 ja rahvusvahelist andmeedastust käsitlevate sätete kohaldamise koostoime kohta vastavalt üldmääruse V peatükile.

- Krüptimisalgoritmide, vastavate võtmepikkuste, andmevoogude ja töötlemisloogika üksikasjad vastavad kaasaegsetele standarditele ning neid vaatavad korrapäraselt ja vajadust mööda läbi valdkonnaeksperdid, et tuvastada võimalikud nõrgad ja riskidele avatud kohad. Krüptimiseks kasutatakse ainult mittevananenud krüptimismeetodeid ja piisava pikkusega võtmeid.
- Krüptovõtmeid kontrollitakse, et tagada nende turvaline genereerimine ja haldamine, ning need vaadatakse korrapäraselt läbi vastavalt valdkonna parimatele tavadele.
- Järelevalve alla kuuluva üksuse andmete krüptimiseks kasutatavad krüptovõtmed on kordumatud ja neid ei jagata pilvteenuse teiste kasutajatega.

Lisaks krüptimistehnoloogiale võivad järelevalve alla kuuluvad üksused rakendada ka i) mitme pilve tehnoloogiaid, mis tõhustavad nende andmeturvet, ii) võrkude asjakohast segmentimist või iii) muid andmekao vältimise meetmeid.

2.3.2 Andmete asukohast ja töötlemisest tulenevad riskid

Vastavalt digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1774 artikli 26 lõike 2 punktile h tuleb järelevalve alla kuuluvate üksuste IKT reageerimis- ja taastekavades arvesse võtta poliitilise ja sotsiaalse ebastabiilsuse stsenaariumit, sealhulgas asjakohasel juhul kolmandast isikust IKT-teenuste osutaja jurisdiktsioonis ning andmete säilitamise ja töötlemise kohas. Kuna mõni pilvteenuse osutaja võib olla tugevalt mõjutatud kolmandate riikide seadusandlusest, leiab EKP ühtlasi, et hea tava kohaselt tuleb neid riske selgelt arvesse võtta. Seetõttu soovitatakse järelevalve alla kuuluvatel üksustel koostada nimekiri riikidest[10], mis on neile vastuvõetavad nende andmete talletamiseks ja töötlemiseks[11] olenevalt konkreetsete andmete laadist. Ideaaljuhul tuleks sellise hindamise käigus arvesse võtta tegevuse edasiandmisega seotud õiguslikke ja poliitilisi riske (nt kohtuvaidluste või sanktsioonide risk).

On hea tava, et andmete töötlemise ja talletamise nõuded, protsessid ja kontrollimeetmed on kõigis kokkulepitud asukohtades või tsoonides ühtsed. Seda tuleks eri tsoonide ja asukohtade puhul korrapäraselt hinnata. Juhuks, kui (isiku)andmeid otsitakse, teisendatakse või liigitatakse järelevalve alla kuuluva üksuse nimel või pilvteenuse osutaja nimel (alltöötlemine), tuleks sisse seada andmetöötluskontrollid.

[10] Euroopa Komisjon on koostanud nimekirja ELi-välistest riikidest, kus andmekaitse taset peetakse isikuandmete kaitse üldmääruse artikli 45 kohaselt piisavaks. EKP soovitab järelevalve alla kuuluvatel üksustel laiendada selle nimekirja kohaldamisala isikuandmete kõrval kõigile andmetele, mida hallatakse pilvteenuse osutajaga sõlmitud pilvteenuste edasiandmise lepingu alusel.

[11] Kui need on hõlmatud järelevalve alla kuuluva üksuse ja kolmandast isikust IKT-teenuste osutaja vahelise lepingulise kokkuleppega vastavalt digitaalse tegevuskerksuse määruse artikli 30 lõike 2 punktile b.

Peale selle leiab EKP, et hea tava kohaselt peaksid järelevalve alla kuuluvad üksused hindama ka täiendavaid riske juhul, kui pilvteenustega seotud alltöövõtja asub muus riigis kui pilvteenuse osutaja. Samal ajal peaksid nad võtma arvesse riske, mis on seotud tegevuse edasiandmise keerukate ahelatega, nagu on kirjeldatud EBA tegevuse edasiandmise suuniste punkti 67 alapunktis b.[12]

2.3.3 Edasiantud varade järjepidev lisamine järelevalve alla kuuluva üksuse IKT-varade loendisse

Digitaalse tegevuskerksuse määruse artikli 8 lõike 1 kohaselt peavad järelevalve alla kuuluvad üksused kindlaks tegema, liigitama ja asjakohaselt dokumenteerima kõik IKT-põhised ärifunktsioonid, rollid ja vastutusvaldkonnad, neid funktsioone toetavad teabevarad ja IKT-varad ning nende rollid ja sõltuvuse seoses IKT-riskiga. Seepärast leiab EKP, et hea tava kohaselt peaksid järelevalve alla kuuluvad üksused kehtestama kõigi IKT-varade, sealhulgas pilvteenuse osutajatele edasiantud varade liigitamise selged põhimõtted. Järelevalve alla kuuluv üksus peaks neid põhimõtteid kohaldama igal juhul ning need peaksid toetama tema suutlikkust hinnata ja kindlaks määrata kontrollimeetmeid, mis on vajalikud andmete konfidentsiaalsuse, tervikluse ja kättesaadavuse tagamiseks olenemata sellest, kus andmeid talletatakse ja töödeldakse.

Selle tegevuse osana soovitatakse järelevalve alla kuuluval üksusel pidada ajakohast loendit kõigist IKT-varadest, mille eest ta nimetatud põhimõtete raames vastutab, tagamaks, et kõik tegevusprotsessid (jälgimine, paikamine, intsidendihaldus, muudatuste juhtimine jne) laienevad ka pilvevaradele.

2.3.4 Identiteedi- ja juurdepääsuhalduse põhimõtted pilvteenuste edasiandmise lepingutes

Nagu järelevalvetegevuses võib sageli täheldada, lähtuvad operatsioonirisk ja pilvteenuste häired peamiselt ebaselgetest rollidest ja kohustustest juurdepääsu- ja konfiguratsiooniõiguste ning krüptovõtmete haldamisel. Seetõttu peaks pilvekeskkonna konfiguratsioon olema selgelt määratletud ja poolte vahel kokku lepitud ning ülesanded üksteisest selgelt eraldatud.

Järelevalve alla kuuluva üksuse identiteedi- ja juurdepääsuhalduse põhimõtteid tuleks laiendada pilvevaradele ning need peaksid hõlmama nii tehnilisi kui ka ärikasutajaid.

Digitaalse tegevuskerksuse määruse artikli 30 täiendamiseks peab EKP heaks tavaks, et järelevalve alla kuuluvad üksused kaaluvad pilvteenuse osutajaga tegevuse edasiandmise lepingu sõlmimise korral lepingusse üksikute klauslite lisamist, mille kohaselt viimane peab järgima järelevalve alla kuuluva üksuse IT- ning

[12] Lõpparuanne: EBA suunised tegevuse edasiandmise kohta (EBA/GL/2019/02).

identiteedi- ja juurdepääsuhalduse põhimõtteid. Kui see ei ole võimalik, peaks järelevalve alla kuuluv üksus ülesannete tõhusaks eraldamiseks analüüsima, kuidas pilvteenuse osutaja poolt pilvteenuste osutamisel pakutav identiteedi- ja juurdepääsuhalduse struktuur sobitub järelevalve alla kuuluva üksuse rollide ja vastutusvaldkondadega. Seejärel saab analüüsida mis tahes kõrvalekaldeid ülesannete tõhusast eraldamisest ja võtta nende kõrvaldamiseks riskimaandusmeetmeid.

Infokast 2

Juurdepääsuhaldus, kaugjuurdepääs ja kasutajate autentimine

Digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1774 artiklite 20 ja 21 järgimise kõrval soovitab EKP järelevalve alla kuuluvatel üksustel kaaluda järgmisi häid tavasid:

- Järelevalve alla kuuluvatest üksustest kasutajad, eriti need, kellel on süsteemile eelisjuurdepääs, on selgelt identifitseeritud ja autenditud tugeva autentimislahenduse abil (st mitmikautentimine), võttes arvesse sellise lahenduse kohaldatavust kriitilise tähtsusega või olulisi funktsioone toetavate pilvesüsteemidega ühendamisel. Juurdepääsuõigused tuleks korrapäraselt läbi vaadata. Juurdepääsuõiguste kontrollimisel tuleks kasutada uuesti sertifitseerimise ja juurdepääsu äravõtmise protsesse, et kasutajatel ei oleks ülemääraseid eelisõigusi. Nende protsesside läbiviimise sagedus peaks olema vastavuses asjaomase funktsiooni olulisusega.
- Eeliskasutajate juurdepääsu tuleks selgelt reaalajas jälgida ja see aruannetes dokumenteerida. Kui juurdepääsu- või selle muutmise taotlused puudutavad juurdepääsu järelevalve alla kuuluva üksuse andmetele, tuleb nende heakskiitmiseks rakendada kokkulepitud menetlusi. Juurdepääsuõiguste läbivaatamist tuleks teha laiemas kontekstis, pidades seejuures silmas ka asutusesiseseid süsteeme.
- Teenuste äriomanikud tuleks üheselt kindlaks määrata, et igal konkreetsel rollil oleks vastutaja ja omanik.
- Kasutusele tuleks võtta juurdepääsu turvameetmed (nt kaksikautentimine ja virtuaalse privaatvõrgu (VPN) krüptimine).
- Selleks et nõuetekohaselt dokumenteerida ja jälgida pilvteenuste osutaja juurdepääsu järelevalve alla kuuluva üksuse süsteemidele või andmetele, kasutatakse asjakohaseid seire- ja logimisvahendeid. Sellised vahendid vaadatakse korrapäraselt läbi.

2.4 Väljumisstrateegiad ja lõpetamisõigus

Digitaalse tegevuskerksuse määruse artikli 28 lõike 8 kohaselt peavad järelevalve alla kuuluvad üksused kehtestama kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste jaoks väljumisstrateegiad. Kui järelevalve alla kuuluv üksus otsustab lõpetada pilvteenuse osutajaga lepingu, ilma et ta oleks eelnevalt

koostanud kriitilise tähtsusega või olulisi funktsioone toetava tegevuse edasiandmise üldisele strateegiale tuginevat põhjalikku väljumiskava, võib tekkida olulisi probleeme ja riske. Enne süsteemide kasutuselevõttu tuleks koostada selgelt määratletud rollide ja vastutusvaldkondadega väljumisstrateegiad ning hinnangulised kulud kõigi edasiantavate pilvteenuste kohta, mis toetavad kriitilise tähtsusega või olulisi funktsioone. Väljumiseks kuluv aeg peaks kajastama asjaomases lepingus sätestatud üleminekuperioodi.

2.4.1 Lõpetamisõigus

IKT-teenuste kasutamist käsitlevad lepingud peavad võimaldama järelevalve alla kuuluval üksusel lepingu lõpetada digitaalse tegevuskerksuse määruse artikli 28 lõikes 7 nimetatud mis tahes asjaolu ilmnemisel. EKP tõlgenduse kohaselt kuuluvad lepingu lõpetamise põhjuste (mis tuleks selgelt loetleda pilvteenuse osutajaga sõlmitud pilvteenuste edasiandmise lepingus) hulka i) lepingu pidev mittenõuetekohane täitmine või ii) lepingutingimuste või kohaldatavate õigusaktide tõsine rikkumine.

Ühtlasi peab EKP digitaalse tegevuskerksuse määruse artikli 28 lõike 7 kohaldamisel heaks tavaks, et järelevalve alla kuuluvad üksused peavad tegevuse lõpetamise põhjenduseks äriüksuste või andmekeskuste ümberasumist. Lisaks sellele sättele soovitab EKP järelevalve alla kuuluvatel üksustel silmas pidada, et lepingu lõpetamist võivad õigustada ka järgmised muudatused: i) ühinemine või müük, ii) pilvteenuse osutaja peakontori üleviimine teise jurisdiktsiooni, iii) majutava andmekeskuse üleviimine teise riiki, iv) tegevuse edasiandmise kokkulepet mõjutavate siseriiklike õigusaktide muutmine, v) andmete asukoha ja andmetöötluse suhtes kohaldatavate eeskirjade muutmine, kui pilvteenuse osutaja ei saa enda osutatavaid teenuseid õigusaktide muudatustega kooskõlastamiseks muuta või otsustab seda mitte teha, vi) alltöövõtja küberturvalisuse riski taseme olulised muudatused ning vii) püsiv suutmatus saavutada kokkulepitud teenusetaset või teenuse oluline kadu.

Hea tavana peaksid kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise lepingud sisaldama lepingu lõpetamise korral üleminekuperioodi. Selle eesmärk on vähendada häirete riski ning võimaldada ümberlülitumist teisele teenuseosutajale või teenuse ületoomist asutusse või selle kasutamise lõpetamist. EKP mõistab, et sellise ülemineku võimaldamiseks on järelevalve alla kuuluval üksusel soovitatav tagada, et kokkulepitud üleminekutingimused kajastavad tema väljumiskava.

Kui tegevuse edasiandmise leping hõlmab mitut teenust, mida saab hallata üksteisest sõltumatult, peaks juhul, kui see on teostatav ja kasulik, olema võimalik teenuseid eraldi lõpetada.

Digitaalse tegevuskerksuse määruse artikli 30 lõike 2 punktis a sisalduva peamisi lepingusätteid käsitleva nõude kohaselt leiab EKP, et järelevalve alla kuuluvatel üksustel on hea tava tagada, et kriitilise tähtsusega või olulisi funktsioone toetava pilvteenuste osutaja alltöövõtjad täidavad samu lepingulisi kohustusi, mis kehtivad

järelevalve alla kuuluva üksuse ja pilvteenuse osutaja vahel. See hõlmab andmete konfidentsiaalsuse, tervikluse, kättesaadavuse, säilitamise ja hävitamise ning konfiguratsioonide ja varundamisega seotud kohustusi.

Hea tavana peaks järelevalve alla kuuluv üksus tagama, et pilvteenuse osutaja lõpetamisõigused oleksid kooskõlas järelevalve alla kuuluva üksuse väljumisstrateegiaga. Eelkõige peaks pilvteenuse osutajaga sõlmitud lepingus sätestatud etteteatamistähtaeg olema piisav, et võimaldada järelevalve alla kuuluval üksusel (või tema palgatud kolmandast isikust teenuseosutajal, kes kasutab oma alltöövõtuahelas pilvteenuseid) asjaomased teenused vastavalt väljumiskavas kindlaksmääratud ajakavale teisele teenuseosutajale üle kanda või asutusse üle tuua.

2.4.2 Väljumisstrateegia osad ja kooskõla väljumiskavaga

Seoses digitaalse tegevuskerksuse määruse artikli 28 lõikega 8 peab EKP heaks tavaks, et järelevalve alla kuuluvad üksused kehtestavad üldise väljumisstrateegia, et tagada tegevuskerksus ja maandada asjakohaseid riske. Selline strateegia peaks sisaldama üksikasjalikke tehnilisi väljumiskavasid iga konkreetse pilvteenuste edasiandmise lepingu jaoks, mis toetab kriitilisi või olulisi funktsioone. Vastavalt digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1773 artiklile 10 peab väljumiskava olema realistlik ja teostatav, põhinema usutavatel stsenaariumitel ja mõistlikel eeldustel ning sellel peab olema rakendamise ajakava, mis on kooskõlas lepingus sätestatud väljumis- ja lõpetamistingimustega. Seejuures mõistab EKP, et järelevalve alla kuuluvate üksuste väljumiskavades peaks olema ette nähtud piisav aeg kõigi meetmete lõpuleviimiseks, mida on vaja võtta plaanipärase või järsu väljumise korral. See hõlmab alternatiivsete lahenduste leidmist, nagu teenuste asutusse ületoomine või uue teenuseosutaja leidmine. Kui talitluspidevuse juhtimise meetmed peaksid tagama teenuste jätkumise lühikese aja jooksul, siis väljumiskavad peaksid selle tagama pikas perspektiivis.

Peale selle on digitaalse tegevuskerksuse määruse artikli 28 lõikes 8 sätestatud, et järelevalve alla kuuluvad üksused peavad välja töötama üleminekukavad, mis võimaldavad neil võtta ära lepingupõhised IKT-teenused ja asjaomased andmed kolmandast isikust IKT-teenuste osutajalt ning kanda need turvaliselt ja terviklikult üle alternatiivsetele teenuseosutajatele või inkorporeerida need uuesti ettevõttesiseselt. EKP mõistab, et järelevalve alla kuuluvad üksused peaksid säilitama suutlikkuse tuua andmed ja rakendused tagasi asutuse süsteemidesse või kanda need üle alternatiivsetele teenuseosutajatele. Sel otstarbel võivad järelevalve alla kuuluvad üksused kaaluda selliste lahenduste kasutamist, mis suurendavad andmete ja IKT-süsteemide porditavust, hõlbustades tõhusat migratsiooni. IaaSi porditavate tehnoloogiate näiteks on virtuaalmasina- ja konteinerpõhised rakendused, samal ajal kui PaaSi ja SaaSi porditavuse aspektid sõltuvad konkreetsetest lahendustest.

Kui väljumisstrateegia keskmes on IKT-teenuste ülekandmine teisele teenuseosutajale, soovitab EKP järelevalve alla kuuluval üksusel koostada

kvalifitseeritud alternatiivsete teenuseosutajate nimekiri. Seda nimekirja tuleks korrapäraselt läbi vaadata ja turuülevaadetele tuginedes ajakohastada, analüüsides näiteks erinevate teenuseosutajate eeliseid ja puudusi. Kui väljumisstrateegia hõlmab teenuste ületoomist asutusse või nende migreerimist teisele pilvteenuse osutajale, peaksid järelevalve alla kuuluvad üksused läbi viima tehnilised analüüsid ja hindama selliseks üleminekuks vajaminevat aega. See peaks olema kooskõlas lepingus sätestatud lõpetamiskuupäevade ja -tähtaegadega.

2.4.3 Väljumiskavade detailsus

Digitaalse tegevuskerksuse määruse artikli 28 lõike 8 kontekstis peab EKP heaks tavaks, et spetsiaalne väljumiskava sisaldab sätteid, millega tagatakse järelevalve alla kuuluva üksuse suutlikkus pilvteenuse osutaja pakutava teenuse kvaliteedi halvenemise korral kiiresti reageerida. Hea tava kohaselt peaksid väljumiskavad sisaldama vähemalt kriitilise tähtsusega vahe-eesmärke, väljumiseks vajalike ülesannete ja oskuste kirjeldust ning ligikaudset hinnangut väljumiseks vajamineva aja ja sellega seotud kulude kohta. Väljumiskavasid tuleks korrapäraselt läbi vaadata ja testida, pidades silmas digitaalse tegevuskerksuse määruse artikli 28 lõike 1 punktis b kirjeldatud proportsionaalsuse põhimõtet. Lisaks leiab EKP, et hea tavana peaksid järelevalve alla kuuluvad üksused oma väljumiskavad vähemalt dokumendipõhiselt põhjalikult läbi vaatama, tagades, et seda teevad töötajad, kellel on piisavad teadmised pilvtehnoloogiast. Samuti peaksid järelevalve alla kuuluvad üksused analüüsima migreerimist vajavate andmete mahtu ja rakenduste keerukust, pidades seejuures silmas andmete võimalikku ülekandmismeetodit, et teha vajamineva aja kohta mõistlik hinnang. Järelevalve alla kuuluvad üksused peaksid proportsionaalsuse põhimõtet silmas pidades kontrollima, kas neil on väljumiskavade jaoks vajalikud töötajad, olgu need asutusesisesed või -välised. Et olemasolevad töötajad oleksid võimelised täitma väljumiskavas kirjeldatud ülesandeid, tuleks need koos töötajatega samm-sammult läbi käia.

Selleks et kontrollida töötajate suutlikkust oma rolliga seotud ülesandeid täita, tuleks hea tavana migratsiooniprotsessi kõige olulisemaid etappe korrapäraselt testida. Järelevalve alla kuuluvad üksused peaksid korrapäraselt kontrollima, kas nende töötajatel on väljumiskavas kindlaks määratud ülesannete täitmiseks vajalikud oskused või kas pilvteenuste edasiandmise lepingust väljumiseks oleks aja kaasata väliskonsultante. Hea tava kohaselt kontrollib iga väljumiskava teostatavust sõltumatu isik, st isik, kes ei vastuta kõnealuse kava koostamise eest.

2.5 Järelevalve, jälgimine ja siseaudit

Järelevalve alla kuuluvad üksused peavad sisse seadma usaldusväärse IKT-riskide juhtimise raamistiku, sealhulgas kolmandast isikust tuleneva IKT-riski usaldusväärse jälgimise korra, mille suhtes kohaldatakse korrapäraseid siseauditeid. Peale selle moodustavad intsidentidest teatamist käsitlevad lepingusätted olulise osa järelevalve alla kuuluva üksuste poolt tehtavast jälgimisest seoses kolmandast isikust tuleneva

IKT-riskiga. Digitaalse tegevuskerksuse määruse artikli 6 lõike 4 kohaselt peavad järelevalve alla kuuluvad üksused tagama, et IKT-riski juhtimise funktsioonid, kontrollifunktsioonid ja siseauditifunktsioonid on sobivalt eraldatud ja sõltumatud vastavalt kolme kaitseliiniga mudelile.

2.5.1 Pilvteenuse osutajate sõltumatu jälgimine

Digitaalse tegevuskerksuse määruse artikli 6 lõike 10 kohaselt võivad järelevalve alla kuuluvad üksused kooskõlas liidu ja liikmesriigi valdkondliku õigusega anda IKT-riski juhtimise nõuete täitmise kontrollimise ülesanded edasi kontsernisisestele või -välistele ettevõtjatele. Sel juhul jääb järelevalve alla kuuluv üksus IKT-riski juhtimise nõuete täitmise kontrollimise eest täielikult vastutavaks. EKP tõlgenduse kohaselt tähendab see seda, et vastutust ennast edasiantud funktsiooni poolt IKT-riski juhtimise nõuete täitmise kontrollimise eest ei saa omakorda tegevusena edasi anda. See kehtib ka juhul, kui pilvteenuseid osutatakse hallatud teenustena, mille puhul pilvteenuse osutaja vastutab tegevuse käigushoidmise ja turvastandardite järgimise eest. Piisava kvaliteeditaseme tagamiseks peaks järelevalve alla kuuluv üksus jälgima pilvteenuse osutaja poolt osutatavaid pilvteenuseid. Üksnes pilvteenuse osutaja antud jälgimisvahendite kasutamine tulemuslikkuse hindamisel ei pruugi olla piisav, kui edasi on antud kriitilise tähtsusega või olulised funktsioonid. Sellisel juhul tuleks lisaks pilvteenuse osutaja pakutavatele jälgimisvahenditele kasutada ka sõltumatuid vahendeid, et tõhustada kriitilise tähtsusega või oluliste funktsioonide jälgimist. Järelevalve alla kuuluvad üksused peaksid tagama asutusesiseselt vajalikud eksperditeadmised, et pilveteenuse osutajate tegevust asjakohaselt jälgida. Kasutatavad jälgimis- ja järelevalvenäitajad peaksid andma asjaomasele meeskonnale kõikehõlmava ülevaate ning neile peaks tuginema järelevalve alla kuuluva üksuse tegevuse edasiandmist käsitlev aruandlus, mis esitatakse juhtorganile.

Järelevalve alla kuuluv üksus peaks tagama, et kõigis tegevuse edasiandmise (sealhulgas grupisisese tegevuse edasiandmise) lepingutes võetakse arvesse jälgimise eesmärgil nõutavat aruandlust, eelkõige kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamisel, nagu on sätestatud digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1773 artiklis 9.[13]

2.5.2 Intsidendiaruanded ja lepingute üksikasjad

Digitaalse tegevuskerksuse määruse artikli 19 lõike 5 kohaselt jäävad järelevalve alla kuuluvad üksused, kes otsustavad oma teavitamiskohustuse edasi anda

[13] Komisjoni delegeeritud määrus (EL) 2024/1773, 13. märts 2024, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 regulatiivsete tehniliste standarditega, et täpsustada põhimõtete üksikasjalikku sisu seoses lepingutega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist (ELT L, 2024/1773, 25.6.2024).

kolmandast isikust teenuseosutajale, siiski täielikult vastutavaks intsidentidest teavitamise nõuete täitmise eest. Järelevalve alla kuuluva üksuse järelevaatamisfunktsioonil peaks olema võimalik uurida üksikasjalikult kõiki pilvteenust osutavas ettevõttes aset leidnud intsidente, mis võivad mõjutada järelevalve alla kuuluvat üksust. Intsidentide haldamiseks peavad olema selgelt määratletud menetlused, rollid ja kohustused. Aruanded peaksid sisaldama üksikasju, mis võimaldavad kindlaks teha intsidendist mõjutatud teenused. Aruanded peaksid võimaldama järelevalve alla kuuluval üksusel hinnata võimalikku mõju tema äritegevusele. Intsidendihaldusprotsessi kõik etapid peaksid olema dokumenteeritud, et oleks võimalik teha järeldusi ja neist õppida. Järelevalve alla kuuluvatel üksustel soovitatakse tagada, et lepingutingimustes sisaldub asjakohaste intsidendi- ja jälgimisaruannete koostamine, mis võimaldab edasiantud funktsioonide pidevat hindamist.

Infokast 3
Lepingutingimused

Digitaalse tegevuskerksuse määruse artikli 30 lõike 4 kohaselt peavad järelevalve alla kuuluvad üksused ja kolmandast isikust IKT-teenuste osutajad lepingute üle läbi rääkides kaaluma, kas kasutada konkreetsete teenuste jaoks avaliku sektori asutuste välja töötatud lepingu tüüptingimusi. Allpool esitatud konkreetseid soovitusi võib selles vallas käsitleda parimate tavade suunistena.

- Lepingutingimused võimaldavad järelevalve alla kuuluvatel üksustel võtta teenuste ebatõhusa osutamise korral järelmeetmeid ja nõuda parandusmeetmete rakendamist.
- Lepingutingimused võimaldavad järelevalve alla kuuluvatel üksustel jälgida teenuste kvaliteedi halvenemist ja nõuda parandusmeetmete rakendamist.
- Lepingud sisaldavad üksikasjalikke andmeid kohapealsete auditite läbiviimise kulude arvestamise kohta.
- Nii järelevalve alla kuuluv üksus kui ka teenuseosutaja peaksid säilitama lepingu sõlmimise ajal originaallepingu koopia. Lepingutingimuste võimalikest hilisematest muudatustest tuleks teatada kõigile lepinguosalistele ja neis tuleks nendega kokku leppida, kusjuures kõik pooled saavad endale lepingu koopia.

2.5.3 Siseaudit

Digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1773 artikli 8 lõike 3 kohaselt ei tohi järelevalve alla kuuluv üksus aja jooksul tugineda üksnes teenuseosutaja poolt kättesaadavaks tehtud kolmanda isiku koostatud auditiaruannetele. Kui järelevalve alla kuuluv üksus teeb kompromisse seoses auditeerimisõiguste korraga, ei pruugi järelevalve alla kuuluva üksuse auditifunktsioon olla enam suuteline tegevuse edasiandmise lepingut sõltumatult läbi vaatama. Kui pilvteenuse osutaja ei esita piisavalt üksikasju oma taristuga seotud protsesside ja sisekontrollisüsteemide kohta, võivad järelevalve alla kuuluval

üksustel puududa üksikasjalikud vahetud teadmised pilvteenuse osutaja tööruumide, infosüsteemide, omandtehnoloogia, alltöövõtjate ja hädaolukorrakavade kohta, kuna enamik üksusi tugineb ainult pilvteenuse osutaja avaldustele ja kolmandate isikute väljastatud sertifikaatidele. Seetõttu ei ole piisav, kui tugineda üksnes pilvteenuse osutaja avaldustele ja kolmandate isikute väljastatud sertifikaatidele.

Seoses digitaalse tegevuskerksuse määruse artikli 6 lõikega 6 eeldab EKP, et järelevalve alla kuuluvate üksuste siseauditi funktsioonid vaatavad korrapäraselt läbi pilvteenuse osutaja osutatavate pilvteenuste kasutamisest tulenevad riskid. EKP soovitab, et läbivaatamine peaks muu hulgas hõlmama sisesuuniste kohaldamise asjakohasust, riskihindamise nõuetekohasust ja teenuseosutaja riskijuhtimise kvaliteedi piisavust. Järgides häid tavasid, mis tagavad, et edasiantud pilvteenuseid saab tõhusalt kontrollida ja juhtida, soovitab EKP järelevalve alla kuuluvatel üksustel pilvteenuse osutajaga sõlmitud lepingus selgelt sätestada, et järelevalve alla kuuluval üksusel, selle siseauditi funktsioonil ning pädevatel asutustel ja kriisilahendusasutustel on õigus pilvteenuse osutajale juurde pääseda ning teda kontrollida ja auditeerida. See on sarnane sellega, mis on digitaalse tegevuskerksuse määruse artikli 30 lõike 3 punkti e alapunkti i kohaselt nõutav kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise lepingute puhul.

Seoses pilvetaristu ja pilvteenuste üha keerukamaks muutumisega on vaja rohkem koondada eksperditeadmisi ja ressursse, arvestades auditite läbiviimiseks vajalikke oskusi ja ressursse ning nendega seotud kulusid. Hea tavana peaksid järelevalve alla kuuluvad üksused kontrollima, kas auditit läbi viivatel audiitoritel on heakskiidetud kutsetunnistus. Samuti tuleb seonduvaid teadmisi kiirete tehnoloogiliste muutuste tõttu sageli värskendada. Järelevalve alla kuuluva üksuse siseauditi funktsioonil soovitatakse tagada, et teise kaitseliini tehtavad riskihindamised ei põhineks üksnes pilvteenuse osutaja esitatud selgitustel ja sertifikaatidel, ilma et võetaks arvesse sõltumatuid hindamisi/läbivaatamisi ning kolmandate isikute (nt turvaanalüütikud) esitatud andmeid. Pilvteenuse osutaja auditi tegemiseks võib järelevalve alla kuuluv üksus kasutada oma siseauditi funktsiooni või määratud kolmandat isikut, nagu on sätestatud digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1773 artikli 8 lõike 2 punktis a.

EKP peab heaks tavaks, et järelevalve alla kuuluvad üksused teevad pilvteenuse osutaja auditeerimisel digitaalse tegevuskerksuse määrust täiendava komisjoni delegeeritud määruse (EL) 2024/1773 artikli 8 lõike 2 punkti b kohaselt koostööd, moodustades ühise kontrollirühma, kuhu kuulub igast järelevalve alla kuuluvast üksusest vähemalt üks tehniline ekspert. Kontrollikavas võiksid asjaomased järelevalve alla kuuluvad üksused kokku leppida konsensuse alusel. Kui sellise ühisauditi käigus tekib konkreetseid küsimusi, mis puudutavad ainult üht järelevalve alla kuuluvat üksust, peaks järelevalve alla kuuluvatel üksustel olema võimalik suhelda pilvteenuse osutajaga järelmeetmete võtmiseks kahepoolselt. Et vältida auditi läbiviimisel pimealasid, soovitab EKP regulaarselt valida kontrollirühmale asjaomaste järelevalve alla kuuluvate üksuste seast rotatsiooni põhimõttel uus juht.

Lisa: lühendid

Lühend	
CRD	kapitalinõuete direktiiv
CSP	pilvteenuse osutaja
DORA	digitaalse tegevuskerksuse määrus
EBA	Euroopa Pangandusjärelevalve
EKP	Euroopa Keskpank
IAM	identiteedi- ja juurdepääsuhaldus
IaaS	taristu teenusena
IKT	info- ja kommunikatsioonitehnoloogia
PaaS	platvorm teenusena
SaaS	tarkvara teenusena

Postiaadress 60640 Frankfurt am Main, Germany
Telefon +49 69 1344 0
Veebileht www.bankingsupervision.europa.eu

PDF ISBN 978-92-899-7155-3, doi 10.2866/0599539, QB-01-25-041-ET-N