III

(Ettevalmistavad aktid)

EUROOPA KESKPANK

EUROOPA KESKPANGA ARVAMUS,

4. juuni 2021,

seoses ettepanekuga Euroopa Parlamendi ja nõukogu määruse kohta, mis käsitleb finantssektori digitaalset tegevuskerksust

(CON/2021/20)

(2021/C 343/01)

Sissejuhatus ja õiguslik alus

Euroopa Keskpank (EKP) sai 22., 23. ja 29. detsembril 2020 vastavalt Euroopa Liidu Nõukogult ja Euroopa Parlamendilt taotlused avaldada arvamust seoses ettepanekuga Euroopa Parlamendi ja nõukogu määruse kohta, mis käsitleb finantssektori digitaalselt tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014 ([1]) (edaspidi „kavandatav määrus“) ning ettepanekuga Euroopa Parlamendi ja nõukogu direktiivi kohta, millega muudetakse direktiive 2006/43/EÜ, 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, 2013/36/EL, 2014/65/EL, (EL) 2015/2366 ja (EL) 2016/2341 ([2]) (edaspidi „kavandatav direktiiv“, koos „kavandatava määrusega“ edaspidi „kavandatavad õigusaktid“).

EKP arvamuse andmise pädevus põhineb Euroopa Liidu toimimise lepingu artikli 127 lõikel 4 ja artikli 282 lõikel 5, kuna kavandatavad õigusaktid sisaldavad EKP pädevusse kuuluvaid sätteid, mis puudutavad eelkõige rahapoliitika määratlemist ja rakendamist, maksesüsteemide tõrgeteta toimimise edendamist, finantsturgude süsteemi stabiilsusega seotud pädevate asutuste poliitika sujuvale elluviimisele kaasaaitamist ning EKP ülesandeid seoses krediidiasutuste usaldatavusnõuete täitmise järelevalvega vastavalt aluslepingu artikli 127 lõike 2 esimesele ja neljandale taandele, artikli 127 lõikele 5 ja artikli 127 lõikele 6. EKP nõukogu on käesoleva arvamuse vastu võtnud kooskõlas Euroopa Keskpanga kodukorra artikli 17.5 esimese lausega.

1. Üldised märkused

1.1 EKP toetab kavandatavat määrust, mille eesmärk on suurendada finantssektori küberturvalisust ja tegevuskerksust. Eelkõige toetab EKP kavandatava määruse eesmärki kõrvaldada finantsteenuste siseturu tõkked ning parandada selle väljakujundamist ja toimimist, ühtlustades info- ja kommunikatsioonitehnoloogia (IKT) riskide juhtimise, teavitamise, testimise ja kolmandast isikust tulenevate IKT-riskide valdkonnas kohaldatavaid nõudeid. Lisaks toetab EKP kavandatava määruse eesmärki ühtlustada ja vähendada finantssektori ettevõtjate suhtes praegu liidu õiguse alusel kohaldatavate regulatiivsete nõuete ja järelevalveootuste kattuvusi.

1.2 EKP arusaama kohaselt soovitakse kavandatavat määrust kohaldada sektoripõhise õigusaktina (*lex specialis*) oluliste teenuste operaatoritena ([3]) määratletud finantssektori ettevõtjate suhtes kooskõlas Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 ([4]) (edaspidi „võrgu- ja infoturbe direktiiv“) artikli 1 lõikes 7 määratletud tähendusega; see tähendab, et kavandatava määruse nõudeid tuleks põhimõtteliselt käsitleda ülimuslikuna võrgu- ja infoturbe direktiivi suhtes. Praktikas hakkaksid oluliste teenuste operaatoritena määratletud finantssektori ettevõtjad ([5]) intsidentidest teatama kavandatava määruse, mitte võrgu- ja infoturbe direktiivi

([1]) COM(2020) 595 final.
([2]) COM (2020) 596 final.
([3]) Vt kavandatava määruse artikli 1 lõige 2.
([4]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148, 6. juuli 2016, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).
([5]) Vt võrgu- ja infoturbe direktiivi artikkel 5.

kohaselt. Kuigi EKP toetab finantssektori ettevõtjate suhtes kohaldatavate nõuete võimalike kattuvuste vähendamist intsidentidest teatamise valdkonnas, tuleks täiendavalt arvesse võtta kavandatava määruse ning võrgu- ja infoturbe direktiivi koostoimet. Näiteks võib kavandatava määruse kohaselt kolmandast isikust IKT-teenuste osutajate ([6]) suhtes kohaldada juhtiva järelevalveasutuse soovitusi ([7]). Samal ajal võib see kolmandast isikust IKT-teenuste osutaja olla võrgu- ja infoturbe direktiivi kohaselt määratletud oluliste teenuste operaatorina, kelle suhtes kohaldatakse pädeva asutuse siduvaid juhiseid ([8]). Sellisel juhul võivad kolmandast isikust IKT-teenuste osutaja suhtes olla vastandlikult kohaldatavad nii kavandatava määruse alusel antud soovitused, kui võrgu- ja infoturbe direktiivi alusel antud siduvad juhised. EKP teeb liidu seadusandlikele organitele ettepaneku täiendavalt kaaluda kavandatava määruse ning võrgu- ja infoturbe direktiivi vahelisi võimalikke vastuolusid, mis võivad takistada finantssektori ettevõtjate suhtes kohaldatavate kattuvate ja vastandlike nõuete ühtlustamist ja vähendamist.

1.3 EKP arusaama kohaselt soovitakse ettepanekuga võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148 ([9]) (edaspidi „kavandatav teine võrgu- ja infoturbe direktiiv“), sätestada „ohuolukordadest“ ([10]) teatamise kohustus ([11]). Kuigi kavandatava teise võrgu- ja infoturbe direktiivi põhjenduses 39 osutatakse mõiste „ohuolukord“ tähendusele, ei ole selge, kas ohuolukordadest teavitamist kavatsetakse nõuda ka kavandatava määruse artiklis 2 loetletud finantssektori ettevõtjatelt. Sellega seoses ning võttes arvesse asjaolu, et ohuolukordi on võimalik sellisena määratleda alles pärast nende tekkimist, sooviks EKP olla õigeaegselt teavitatud olulistest ohuolukordadest, nagu praegu küberintsidentide puhul. EKP teeb ettepaneku tagada parem kooskõla kavandatava määruse ja kavandatava teise võrgu- ja infoturbe direktiivi vahel, et määratleda aruandluse täpne ulatus, mida igalt finantssektori ettevõtjalt võib nende kahe eraldiseisva, kuid omavahel seotud liidu õigusakti alusel nõuda. Samuti tuleks määratleda „ohuolukorrad“ ning töötada välja sätted, milles selgitatakse nende olulisust.

1.4 EKP toetab finantssektori ettevõtjate julgustamist küberohuteadmuse jagamisel küberkerksuse parandamiseks ja tugevdamiseks. EKP ise on toetanud turupõhist algatust küberohuteadmuse jagamiseks (CIISI-EU) ning on avaldanud algatuse edendamise raamistiku ([12]).

1.5 EKP toetab koostööd pädevate asutuste, Euroopa järelevalveasutuste (ESAd) ja küberturbe intsidentide lahendamise üksuste (CSIRT) ([13]) vahel kavandatava määruse kohaldamisel. Liidu tegevuskerksuse tagamiseks on oluline vahetada teavet; ametiasutuste vaheline teabevahetus ja koostöö aitavad ennetada küberrünnideid ja vähendada IKT-ohtude levikut. Edendada tuleks ühist arusaamist IKTga seotud riskidest ning kogu liidus tuleks tagada asjaomaste riskide järjepidev hindamine. On äärmiselt oluline, et pädevad asutused jagaksid teavet ühtse kontaktpunkti ([14]) ja riikliku CSIRTiga ([15]) ainult siis, kui on olemas selgelt määratletud klassifitseerimis- ja teabejagamise mehhanismid koos piisavate kaitsemeetmetega konfidentsiaalsuse tagamiseks.

1.6 Lõpetuseks toetaks EKP isikuandmete ja andmete säilitamise eeskirjade lisamist kavandatavasse määrusesse. Säilitamisperioodi sätestamisel tuleks arvesse võtta kavandatavast määrusest tulenevate kohustuste ja ülesannete raames pädevate asutuste läbiviidavat uurimist, ülevaatamist, teabenõude esitamist, teabe esitamist, avaldamist, hindamist, kontrollimist, läbivaatamist ja järelevalvekavade koostamist. Selles kontekstis oleks piisav 15-aastane säilitamisperiood. Andmete säilitamise perioodi võib vajadusel lühendada

([6]) Vt kavandatava määruse artikli 3 lõige 15.
([7]) Vt kavandatava määruse artikli 31 lõike 1 punkt d.
([8]) Vt võrgu- ja infoturbe direktiivi artikli 15 lõige 3.
([9]) COM (2020) 823 final.
([10]) Sündmused, mis oleksid võinud põhjustada kahju, kuid mis suudeti edukalt ära hoida; vt teise võrgu- ja infoturbe direktiivi põhjendus 39.
([11]) Vt teise võrgu- ja infoturbe direktiivi artikkel 11.
([12]) Küberohuteadmuse jagamise algatus (Cyber threat Intelligence Information Sharing Initiative, CIISI-EU), avaldatud EKP veebilehel www.ecb.europa.eu.
([13]) Vt kavandatava määruse artikkel 42.
([14]) Vt võrgu- ja infoturbe direktiivi artikli 8 lõige 3.
([15]) Vt ka teise võrgu- ja infoturbe direktiivi artiklid 11, 26 ja 27.

või pikendada. Sellega seoses teeb EKP liidu seadusandlikele organitele ettepaneku võtta isikuandmete ja andmete säilitamise asjakohase sätte sõnastamisel arvesse ka võimalikult väheste andmete kogumise põhimõtet, samuti edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil ([16]).

2. **Konkreetsed märkused järelevaatamise ning väärtpaberite kliiringu ja arvelduse kohta**

2.1 *EKPSi ja eurosüsteemi järelevaatamispädevus*

2.1.1 Aluslepingus ning Euroopa Keskpankade Süsteemi ja Euroopa Keskpanga põhikirjas (edaspidi „EKPSi põhikiri") on sätestatud, et eurosüsteem teostab järelevaatamist arveldus- ja maksesüsteemide üle, mis on tihedalt seotud tema peamiste rahapoliitiliste ülesannetega. Asutamislepingu artikli 127 lõike 2 neljas taane ja EKPSi põhikirja artikkel 3.1 sätestavad, et maksesüsteemide tõrgeteta toimimisele kaasa aitamine on üks Euroopa Keskpankade Süsteemi (EKPS) põhiülesandeid. Selle põhiülesande täitmiseks võivad „EKP ja riikide keskpangad anda vahendeid ja EKP võib kehtestada eeskirju efektiivsete ja usaldatavate arveldus- ja maksesüsteemide tagamiseks liidu piires ja teiste riikidega" ([17]). Järelevaataja rollist tulenevalt on EKP võtnud vastu Euroopa Keskpanga määruse (EL) nr 795/2014 (EKP/2014/28) (edaspidi „süsteemselt oluliste maksesüsteemide määrus") ([18]). Süsteemselt oluliste maksesüsteemide määrusega rakendatakse normatiivselt makse- ja arveldussüsteemide komitee ja Rahvusvahelise Väärtpaberijärelevalve Organisatsiooni poolt 2012. aasta aprillis välja antud finantsturutaristute põhimõtteid ([19]), mis on õiguslikult siduvad ja hõlmavad nii suure väärtusega kui ka süsteemselt olulisi jaemaksesüsteeme, mida haldab kas eurosüsteemi keskpank või eraõiguslik üksus. Eurosüsteemi järelevaatamispoliitika raamistikus ([20]) on maksevahendid määratletud kui „maksesüsteemide lahutamatu osa" ja kuuluvad seega järelevaatamise alla. Maksevahendite järelevaatamisraamistik on praegu läbivaatamisel ([21]). Selle raamistiku kohaselt on maksevahend (nt kaart, kreeditkorraldus, otsekorraldus, e-raha ülekanne ja digitaalne maksetoken ([22])) määratletud kui isikustatud seade (või seadmete kogum) ja/või toimingute kogum, milles makseteenuse kasutaja ja makseteenuse pakkuja on väärtuse ülekandmise algatamiseks kokku leppinud ([23]).

2.1.2 Eeltoodut arvesse võttes toetab EKP Euroopa Parlamendi ja nõukogu direktiivi 98/26/EÜ ([24]) artikli 2 punktis p määratletud süsteemi operaatorite, maksesüsteemide (sealhulgas keskpankade hallatavate süsteemide), makseskeemide ja maksekorra väljajätmist kavandatava määruse kohaldamisalast, arvestades eeltoodud

([16]) Vt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725, 23. oktoober 2018, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39) artikli 4 punkt b ja artikkel 13.

([17]) Vt EKPSi põhikirja artikkel 22.

([18]) Euroopa Keskpanga määrus (EL) nr 795/2014, 3. juuli 2014, süsteemselt oluliste maksesüsteemide järelevaatamise kohta (EKP/2014/28) (ELT L 217, 23.7.2014, lk 16).

([19]) Avaldatud Rahvusvaheliste Arvelduste Panga veebilehel www.bis.org.

([20]) Eurosüsteemi järelevaatamispoliitika raamistik, läbivaadatud redaktsioon (juuli 2016), avaldatud EKP veebilehel www.ecb.europa.eu.

([21]) Vt eurosüsteemi läbivaadatud ja konsolideeritud järelevaatamisraamistik elektrooniliste maksevahendite, -skeemide ja -korra kohta (PISA raamistik, oktoober 2020), mis on avaldatud EKP veebilehelwww.ecb.europa.eu.

([22]) Digitaalne maksetoken on mujal registreeritud nõuete või varadega tagatud väärtuse digitaalne esitus, mis võimaldab väärtuse ülekandmist lõppkasutajate vahel. Olenevalt oma alusstruktuurist võivad digitaalsed maksetokenid ette näha väärtuse ülekandmise ilma tingimata keskset kolmandat osapoolt kaasamata ja/või maksekontot kasutamata.

([23]) „Väärtuse ülekandmine" - „Maksja poolt või maksja nimel või makse saaja algatatud rahaliste vahendite või digitaalsete maksetokenite ülekandmine või raha sissemakse kasutajakontole või väljavõtmine kasutajakontolt, mis ei olene makse aluseks olevatest mis tahes kohustustest maksja ja makse saaja vahel. Ülekanne võib hõlmata üht või mitut makseteenuse pakkujat." Mõiste „väärtuse ülekandmine" PISA raamistikus erineb mõistest „rahaliste vahendite ülekandmine" Euroopa Parlamendi ja nõukogu 25. novembri 2015. aasta direktiivis (EL) 2015/2366 makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35). „Väärtuse ülekandmine" selles direktiivis määratletud „maksevahendi" kontekstis saab tähendada ainult „rahaliste vahendite" ülekandmist. Direktiivi kohaselt ei hõlma „rahalised vahendid" digitaalseid maksetokeneid, välja arvatud juhul, kui neid saab liigitada e-rahaks (või hüpoteetilisemalt kontorahaks).

([24]) Euroopa Parlamendi ja nõukogu direktiiv 98/26/EÜ, 19. mai 1998, arvelduse lõplikkuse kohta makse- ja väärtpaberiarveldussüsteemides (EÜT L 166, 11.6.1998, lk 45).

järelevaatamisraamistike kohaldamist. Nimetatud põhjustel tuleks kavandatava määruse põhjendustes selgelt välja tuua asutamislepingust tulenev EKPSi pädevus ja süsteemselt oluliste maksesüsteemide määrusest tulenev eurosüsteemi pädevus.

2.1.3 Samuti toetab EKP kavandatavas määruses sätestatud järelevaatamisraamistiku kohaldamisalast selliste kolmandast isikust IKT-teenuste osutajate väljajätmist, kelle suhtes kohaldatakse järelevaatamisraamistikke, mis on kehtestatud aluslepingu artikli 127 lõikes 2 osutatud ülesannete toetamiseks ([25]). Sellega seoses soovib EKP rõhutada, et EKPSi keskpangad, kui nad tegutsevad rahandusasutusena ([26]), ning eurosüsteem, kui ta osutab teenuseid TARGET2, TARGET2-Securites (Tel 2S) ([27]) ja TARGETi välkmaksete arveldamise teenuse (TIPS) ([28]) kaudu, ei kuulu kavandatava määruse kohaldamisalasse, samuti ei saa neid käsitada kolmandast isikust IKT-teenuste osutajatena ning seega potentsiaalselt ka kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatena kavandatava määruse tähenduses. Eurosüsteem teostab Tel 2Si üle järelevaatamist tulenevalt oma ülesandest tagada tõhusad ja usaldusväärsed arveldus- ja maksesüsteemid. Lisaks on ESMA selgitanud, et Tel 2S ei ole kriitilise tähtsusega teenuseosutaja ([29]) Euroopa Parlamendi ja nõukogu määruse (EL) nr 909/2014 ([30]) (edaspidi „väärtpaberite keskdepositooriumide määrus“) tähenduses. Seetõttu tagatakse Tel 2Si korralduse ja tegevuse ohutus, tõhusus ja vastupanuvõime kohaldatava Tel 2Si õigusliku, regulatiivse ja korraldusliku raamistiku ning kokkulepitud juhtimiskorra, mitte väärtpaberite keskdepositooriumide määruse kaudu.

2.1.4 Lisaks hõlmab eurosüsteemi järelevaatamispoliitika raamistik ([31]) kriitilise tähtsusega teenuseosutajaid, nagu ülemaailmse pankadevahelise finantstelekommunikatsiooni ühing (SWIFT). SWIFT on Belgias asutatud piiratud vastutusega ühistu, mis osutab turvalist sõnumivahetuse teenust rahvusvahelisel tasandil. Nationale Bank van België/Banque Nationale de Belgique on SWIFTi juhtiv järelevaataja ning teostab SWIFTi üle järelevaatamist koostöös teiste G10 keskpankadega, sealhulgas EKPga, tuginedes koostööl põhinevale järelevaatamiskorrale. G10 järelevaatajad tunnistavad, et järelevaatamisel keskendutakse peamiselt SWIFTi operatsiooniriskile, kuna seda peetakse peamiseks riskikategooriaks, mille kaudu SWIFT võib kujutada endast süsteemset riski liidu finantssüsteemile. Seetõttu on SWIFTi järelevaatamise koostöörühm välja töötanud SWIFTi suhtes kohaldatavad konkreetsed põhimõtted ja kõrgetasemelised ootused, näiteks riskide tuvastamise ja juhtimise, infoturbe, usaldusväärsuse ja vastupidavuse, tehnoloogia planeerimise ja kasutajatega teabevahetuse valdkonnas. G10 järelevaatajate ootuste kohaselt peab SWIFT järgima maksete ja turuinfrastruktuuri komitee (CPMI) ja Rahvusvahelise Väärtpaberijärelevalve Organisatsiooni (IOSCO) küberkerksuse suuniseid ([32]) ning muid rahvusvahelisi IKT-turbe standardeid, mis üheskoos ületavad kavandatavas määruses sätestatud nõudeid.

2.1.5 Ei saa välistada võimalust, et SWIFTile ning potentsiaalselt ka teistele teenuseosutajatele, kelle suhtes kohaldatakse eurosüsteemi järelevaatamispoliitika raamistikku, hakatakse kavandatavat määrust kohaldama kui kolmandast isikust IKT-teenuste osutajatele, kui nad osutavad teenuseid, mis ei ole hõlmatud aluslepingu artikli 127 lõikega 2. Seetõttu EKP tugevalt toetab teenuseosutajate, kelle suhtes juba kohaldatakse eurosüsteemi järelevaatamispoliitika raamistikku (sealhulgas, kuid mitte ainult SWIFTi), välja jätmist kavandatavas määruses sätestatud järelevaatamisraamistiku kohaldamisalast.

([25]) Vt kavandatava määruse artikli 28 lõige 5.

([26]) Vt Euroopa Keskpanga arvamuse, 19. veebruar 2021, ettepaneku kohta võtta vastu määrus, mis käsitleb krüptovaraturge ja millega muudetakse direktiivi (EL) 2019/1937 (CON/2021/4), punkt 1.3. Kõik EKP arvamused on avaldatud EUR-Lexis.

([27]) Vt Euroopa Keskpanga suunise EKP/2012/27, 5. detsember 2012, üleeuroopalise automatiseeritud reaalajalise brutoarvelduste kiirülekandesüsteemi (TARGET2) kohta (ELT L 30, 30.1.2013, lk 1), IIa lisa Euroopa Keskpanga suunis EKP/2012/13, 18. juuli 2012, TARGET2-Securities kohta (ELT L 215, 11.8.2012, lk 19); Euroopa Keskpanga otsus EKP/2011/20, 16. november 2011, millega kehtestatakse väärtpaberite keskdepositooriumidele TARGET2-Securities teenustele juurdepääsu kõlblikkuskriteeriumide rakendamise üksikasjalikud eeskirjad ja kord (ELT L 319, 2.12.2011, lk 117). Vt ka Tel 2Si raamleping ja kollektiivleping.

([28]) Vt suunise EKP/2012/27 IIb lisa.

([29]) Vt Euroopa Parlamendi ja nõukogu määruse (EL) nr 909/2014, 23. juuli 2014, mis käsitleb väärtpaberiarvelduse parandamist Euroopa Liidus ja väärtpaberite keskdepositooriume ning millega muudetakse direktiive 98/26/EÜ ja 2014/65/EL ning määrust (EL) nr 236/2012 (ELT L 257, 28.8.2014, lk 1), artikli 30 lõige 5 ning komisjoni delegeeritud määruse (EL) 2017/392, 11. november 2016, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 909/2014 seoses regulatiivsete tehniliste standarditega, mis käsitlevad väärtpaberite keskdepositooriumide suhtes kohaldatavaid tegevuslubade andmise, järelevalve ja tegevusega seotud nõudeid (ELT L 65, 10.3.2017, lk 48), artikkel 68.

([30]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 909/2014, 23. juuli 2014, mis käsitleb väärtpaberiarvelduse parandamist Euroopa Liidus ja väärtpaberite keskdepositooriume ning millega muudetakse direktiive 98/26/EÜ ja 2014/65/EL ning määrust (EL) nr 236/2012(ELT L 257, 28.8.2014, lk 1).

([31]) Eurosüsteemi järelevaatamispoliitika raamistik, läbivaadatud redaktsioon (juuli 2016), avaldatud EKP veebilehelwww.ecb.europa.eu.

([32]) Avaldatud Rahvusvaheliste Arvelduste Panga veebilehel www.bis.org.

2.2 *EKPSi pädevus väärtpaberite arveldamise valdkonnas*

2.2.1 Väärtpaberite keskdepositooriumid on finantsturutaristud, mis on rangelt reguleeritud ja mille üle teostavad järelevalvet erinevad asutused vastavalt väärtpaberite keskdepositooriumide määrusele, milles on sätestatud finantsinstrumentide arveldamise nõuded ning väärtpaberite keskdepositooriumide korralduse ja tegevuse eeskirjad. Lisaks peavad väärtpaberite keskdepositooriumid võtma arvesse CPMI-IOSCO küberkerksuse suuniseid, mis on rakendatud küberkerksuse järelevaatamisootustes finantsturutaristute jaoks (detsember 2018) ([33]). Lisaks väärtpaberite keskdepositooriumide määruse kohaselt riiklikele pädevatele asutustele antud järelevalvepädevusele tegutsevad EKPSi liikmed „kaasatud asutustena", kes teostavad järelevaatamist väärtpaberite keskdepositooriumide korraldatavate väärtpaberiarveldussüsteemide üle, keskpankadena, kes emiteerivad kõige olulisemaid arveldusvaluutasid, ning keskpankadena, kelle juures arveldatakse tehingute raha pool ([34]). Sellega seoses on väärtpaberite keskdepositooriumide määruse põhjenduses 8 sedastatud, et asjaomane määrus ei tohiks piirata EKP ja riikide keskpankade vastutust tagada liidus ja teistes riikides tõhusad ja nõuetekohased arveldus- ja maksesüsteemid. Lisaks sedastatakse põhjenduses 8, et väärtpaberite keskdepositooriumide määrus ei tohiks takistada EKPSi liikmete juurdepääsu oma ülesannete täitmiseks vajalikule teabele ([35]), sealhulgas väärtpaberite keskdepositooriumide ja muude finantsturutaristute üle järelevalve teostamist ([36]).

2.2.2 Lisaks tegutsevad EKPSi liikmed sageli väärtpaberitehingute raha poole arveldusagentidena ja eurosüsteem pakub Tel 2Si kaudu arveldusteenuseid väärtpaberite keskdepositooriumidele. Eurosüsteemi järelevaatamine Tel 2Si üle on seotud tema volitustega tagada tõhusad ja usaldusväärsed arveldus- ja maksesüsteemid, samas kui väärtpaberite keskdepositooriumide pädevate ja kaasatud asutuste eesmärk on tagada nende süsteemide sujuv toimimine, arvelduste turvalisus ja tõhusus ning finantsturgude nõuetekohane toimimine vastavas jurisdiktsioonis.

2.2.3 Kavandatava määruse kohaselt ([37]) ei osale EKPSi keskpangad IKT-riskide kindlaksmääramisega seotud tehniliste standardite väljatöötamises. Samuti ei teavitata kavandatava määruse kohaselt ([38]) asjaomaseid asutusi IKTga seotud intsidentidest. EKPSi keskpank peaks olema kaasatud samal tasandil, mis on praegu sätestatud väärtpaberite keskdepositooriumide määruses, ning asjaomaseid asutusi tuleks teavitada IKTga seotud intsidentidest. Eurosüsteem on kaasatud asutus kõikide euroala väärtpaberite keskdepositooriumide ning mitme teise ELi väärtpaberite keskdepositooriumi jaoks. EKPSi keskpanku tuleks teavitada IKTga seotud intsidentidest, mis on seotud nende ülesannete täitmisega, sealhulgas väärtpaberite keskdepositooriumide ja muude finantsturutaristute järelevaatamisega. Väärtpaberite keskdepositooriumidele avalduvad riskid, sealhulgas IKT riskid, võivad ohustada väärtpaberite keskdepositooriumide usaldusväärset toimimist. Seetõttu on IKT-riskid asjaomaste asutuste jaoks olulised ning neile tuleks anda IKT-riskidest täielik ja üksikasjalik ülevaade, et riske hinnata ja mõjutada väärtpaberite keskdepositooriumide riskijuhtimist. Kavandatav määrus ei tohiks IKT-riskide suhtes ette näha vähem piiravaid nõudeid kui väärtpaberite keskdepositooriumide määruses ja kehtivates regulatiivsetes tehnilistes standardites sätestatud nõuded.

2.2.4 Lisaks peaksid liidu seadusandlikud organid selgitama kavandatava määruse ([39]) ja väärtpaberite keskdepositooriumide määrust täiendavate regulatiivsete tehniliste standardite koostoimet. Eelkõige on ebaselge, kas väärtpaberite keskdepositoorium tuleks vabastada kohustusest omada varutöötluskohta, kui tema kolmandast isikust IKT-teenuste osutajal on selline tegevuskoht ([40]). Kui väärtpaberite keskdepositoorium varutöötluskoha omamise kohustusest vabastatakse, on ebaselge, milline on sellise nõude õiguslik väärtus. Samuti osutatakse

([33]) Avaldatud EKP veebilehel www.ecb.europa.eu.

([34]) Vt määruse (EL) nr 909/2014 artikkel 12.

([35]) Vt ka väärtpaberite keskdepositooriumide määruse artikkel 13, artikli 17 lõige 4 ja artikli 22 lõige 6.

([36]) Vt Euroopa Keskpanga 6. aprilli 2017. aasta arvamuse (infotehnoloogia turvalisusega seotud kriitiliste infrastruktuuride tuvastamise kohta) (CON/2017/10) punkt 7.3; Euroopa Keskpanga 8. novembri 2018. aasta arvamuse (võrgu- ja infosüsteemide turvalisuse eesmärgil oluliste teenuste ja oluliste teenuste operaatorite määramise kohta) (CON/2018/47) punkt 7.2; Euroopa Keskpanga 2. mai 2019. aasta arvamuse (võrgu- ja infosüsteemide turvalisuse kohta) (CON/2019/17) punkt 3.5.2; ja Euroopa Keskpanga 11. novembri 2019. aasta arvamuse (võrgu- ja infosüsteemide turvalisuse kohta) (CON/2019/38) punkt 3.5.2.

([37]) Vt kavandatava määruse artikli 54 lõige 5 ja määruse (EL) nr 909/2014 artikli 45 lõige 7.

([38]) Vt kavandatava määruse artikli 54 lõige 4 ja määruse (EL) nr 909/2014 artikli 45 lõige 6.

([39]) Vt kavandatava määruse artikli 11 lõige 5.

([40]) Vt komisjoni delegeeritud määruse (EL) nr 2017/393, 11. november 2016, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 909/2014 seoses regulatiivsete tehniliste standarditega, mis käsitlevad väärtpaberite keskdepositooriumide suhtes kohaldatavaid tegevuslubade andmise, järelevalve ja tegevusega seotud nõudeid (ELT L 65, 10.3.2017, lk 48), artikli 78 lõige 3.

kavandatavas määruses ([41]) iga funktsiooni taasteajale ja sihtseisule ([42]), samas kui asjakohases regulatiivses tehnilises standardis eristatakse kriitilisi funktsioone ([43]) ja kriitilisi toiminguid ([44]) seoses väärtpaberite keskdepositooriumide kriitilistele funktsioonidele määratud taasteajaga. Liidu seadusandlikud organid peaksid täiendavalt selgitama ja kaaluma kavandatava määruse ja väärtpaberite keskdepositooriumide määrust täiendavate regulatiivsete tehniliste standardite koostoimet, et vältida vastandlike nõuete ohtu. Lõpetuseks tuleks täpsustada, et kavandatava määrusega laiendatakse erandeid, mis on tehtud väärtpaberite keskdepositooriumidele, mida käitavad teatavad avaliku sektori asutused väärtpaberite keskdepositooriumide määruse alusel ([45]).

2.3 *EKPSi pädevus väärtpaberite kliiringu valdkonnas*

2.3.1 EKPSi keskpankadele on antud kesksete vastaspoolte järelevaatamise pädevus. Sellega seoses teevad eurosüsteemi riikide keskpangad kesksete vastaspoolte järelevaatamis- ja järelevalveülesannete täitmisel sageli koostööd asjaomaste riiklike pädevate asutustega ning osalevad vastava keskse vastaspoole kolleegiumis, mis on loodud Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 ([46]) (edaspidi „Euroopa turu infrastruktuuri määrus“) alusel. Asjaomased eurosüsteemi liikmed ([47]) osalevad Euroopa turu infrastruktuuri määruses sätestatud kolleegiumide järelevalvetegevuses ning esindavad eurosüsteemi keskse vastaspoole emiteeriva keskpangana, kui euro on kliiritavate finantsinstrumentide (ja offshore-kesksete vastaspoolte, kes kliirivad märkimisväärse osa finantsinstrumentidest eurodes) jaoks üks kõige olulisemaid valuutasid. EKP on euroalaväliste kesksete vastaspoolte emiteeriv keskpank.

2.3.2 Kavandatava määruse kohaselt ([48]) ei osale EKPSi keskpangad IKT-riskide kindlaksmääramisega seotud tehniliste standardite väljatöötamises. Lisaks puuduvad kavandatavas määruses ([49]) viited Euroopa turu infrastruktuuri määruse kohastele taasteaja ja sihtseisu nõuetele ([50]). Kavandatavas õiguslikus raamistikus ei tohiks IKT-riskide suhtes ette näha vähem piiravaid nõudeid kui praegu kehtivad nõuded. Seetõttu on oluline sätestada kindel taasteaeg ja sihtseis, et tagada usaldusväärne talitluspidevuse juhtimise raamistik. Kindla taasteaja ja sihtseisu kehtestamine on ka üks CPMI-IOSCO finantsturutaristute põhimõtetest ([51]). Euroopa turu infrastruktuuri määruse praegune säte tuleks sisse jätta ning kavandatavat määrust tuleks vastavalt kohandada. EKPSi keskpangad tuleks kaasata teiseste õigusaktide ettevalmistamisse, samuti tuleks liidu seadusandlikel organitel täpsustada ja kaaluda kavandatava määruse ja täiendavate regulatiivsete tehniliste standardite koostoimet, et vältida vastandlike nõuete ja nõuete kattumise ohtu.

3. **Konkreetsed tähelepanekud usaldatavusnõuete täitmise järelevalve kohta**

3.1 Lisaks antakse määrusega (EL) nr 1024/2013 ([52]) (edaspidi „ühtse järelevalvemehhanismi määrus“) EKP-le eriülesanded seoses krediidiasutuste usaldatavusnõuete täitmise järelevalvega euroalal ning pannakse EKP-le vastutus ühtse järelevalvemehhanismi tõhusa ja järjepideva toimimise eest, mille raames jagatakse konkreetsed järelevalvega seotud ülesanded EKP ja osalevate riiklike pädevate asutuste vahel. Eelkõige on EKP ülesandeks krediidiasutusele tegevusloa andmine ja selle kehtetuks tunnistamine. EKP ülesanne on muu hulgas tagada vastavus asjakohastele liidu õigusnormidele, millega kehtestatakse krediidiasutuste suhtes usaldatavusnõuded, mille hulka kuulub nõue kehtestada kindel juhtimiskord, mis hõlmab usaldusväärseid riskijuhtimisprotsesse ja sisekontrollimehhanisme ([53]). Selleks on EKP-le antud kõik järelevalvevolitused krediidiasutuste tegevusse sekkumiseks, mis on

([41]) Vt kavandatava määruse artikli 11 lõige 6.
([42]) Vt kavandatava määruse artikli 3 lõige 17.
([43]) Vt komisjoni delegeeritud määruse (EL) nr 2017/392 artikli 76 lõike 2 punktid d ja e.
([44]) Vt komisjoni delegeeritud määruse (EL) nr 2017/392 artikli 78 lõiked 2 ja 3.
([45]) Vt määruse (EL) nr 909/2014 artikli 1 lõige 4.
([46]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 648/2012, 4. juuli 2012, börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.7.2012, lk 1).
([47]) Vt Euroopa turu infrastruktuuri määruse artikli 18 lõike 2 punktid g ja h.
([48]) Vt kavandatava määruse artikli 53 lõike 2 punkt b ja lõige 3 ning Euroopa turu infrastruktuuri määruse artikli 34 lõige 3.
([49]) Vt kavandatava määruse artikli 53 lõike 2 punkt a.
([50]) Vt Euroopa turu infrastruktuuri määruse artikkel 34.
([51]) Vt CPMI-IOSCO finantsturutaristute põhimõtted, mis on avaldatud Rahvusvaheliste Arvelduste Panga veebilehel www.bis.org.
([52]) Nõukogu määrus (EL) nr 1024/2013, 15. oktoober 2013, millega antakse Euroopa Keskpangale eriülesanded seoses krediidiasutuste usaldatavusnõuete täitmise järelevalve poliitikaga (ELT L 287, 29.10.2013, lk 63).
([53]) Vt määruse (EL) nr 1024/2013 artikli 4 lõike 1 punkt e ja artikli 6 lõige 4.

vajalikud tema ülesannete täitmiseks. EKP ja asjaomased riiklikud pädevad asutused on seega pädevad asutused, kes täidavad usaldatavusnõuete täitmise järelevalve ülesandeid vastavalt Euroopa Parlamendi ja nõukogu määrusele 2013/575/EL ([54]) (edaspidi „kapitalinõuete määrus“) ning Euroopa Parlamendi ja nõukogu direktiivile 2013/36/EL ([55]) (edaspidi „kapitalinõuete direktiiv“).

3.2 Kavandatavas määruses sedastatakse, et ühtset reeglistikku ja järelevalvesüsteemi tuleks edasi arendada, et need hõlmaksid digitaalset tegevuskerksust ja IKT turvalisust, laiendades finantsjärelevalveasutuste volitusi, mis tegelevad finantsstabiilsuse ja turu usaldusväärsuse kaitsmisega ([56]). Eesmärk on edendada laiahaardelist IKT- või operatsiooniriskide raamistikku, ühtlustades kõigi finantssektori ettevõtjate digitaalse tegevuskerksuse põhinõudeid ([57]). Eelkõige on kavandatava määruse eesmärk koondada kokku ja ajakohastada IKT-riskidega seotud nõuded, mida seni on käsitletud eraldiseisvates õigusaktides ([58]).

3.3 Finantssektori IKT-riskidega seotud nõuded on praegu hajutatud mitme liidu õigusakti, sealhulgas kapitalinõuete direktiivi ja mittesiduvate õigusaktide (nt EBA suunised) vahel, erinevad teineteisest ning on kohati puudulikud. Mõnel juhul on IKT-riski käsitletud kaudselt operatsiooniriski osana, mõnel juhul ei ole seda üldse käsitletud. Seda tuleks parandada, viies kavandatava määruse kooskõlla kõnealuste õigusaktidega. Selleks esitatakse kavandatava muutmisdirektiiviga rida muudatusettepanekuid, mis on vajalikud õigusselguse ja järjepidevuse tagamiseks seoses erinevate digitaalse tegevuskerksuse nõuete kohaldamisega. Paraku osundavad kavandatava muutmisdirektiiviga ette nähtud kapitalinõuete direktiivi muudatused ([59]) ainult situatsiooni- ja talitluspidevuse kavasid käsitlevatele sätetele ([60]), kuna neid kasutatakse kaudselt IKT-riski juhtimiseks.

3.4 Lisaks näeb kavandatav määrus ette ([61]), et finantssektori ettevõtjatel, sealhulgas krediidiasutustel, peab olema sisemine juhtimis- ja kontrolliraamistik, mis tagab kõikide IKT-riskide tulemusliku ja usaldusväärse juhtimise. Kavandatav määrus näeb ette ([62]) selles sätestatud nõuete kohaldamise individuaalsel ja konsolideeritud tasandil, kuid ilma, et see oleks piisavalt kooskõlastatud osundatud valdkondlike õigusaktidega. Lõpetuseks näeb kavandatav määrus ette ([63]), ilma et see piiraks kavandatavas määruses osundatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamisraamistikku käsitlevate sätete kohaldamist ([64]), et kapitalinõuete direktiivi artikli 4 kohaselt määratud pädevad asutused peavad tagama, et krediidiasutused täidaksid kavandatavas määruses sätestatud kohustusi, ilma et see piiraks EKP-le ühtse järelevalvemehhanismi määrusega antud eriülesandeid.

3.5 Eeltoodust tulenevalt on EKP arusaama kohaselt kavandatava määruse eesmärk krediidiasutuste puhul (välja arvatud kavandatava määruse sätted, mis käsitlevad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamisraamistikku) ([65]) kehtestada IKT-riskide juhtimiseks usaldatavusnõuete kohane sisejuhtimise raamistik, mis integreeritakse kapitalinõuete direktiiviga ette nähtud üldisesse sisejuhtimise raamistikku. Lisaks, võttes arvesse kavandatava raamistiku tuginemist usaldatavusnõuetele, on pädevateks asutusteks, kes vastutavad kavandatavas raamistikus ette nähtud kohustuste täitmise järelevalve eest, sealhulgas EKP, asutused, kes vastutavad pangajärelevalve eest vastavalt ühtse järelevalvemehhanismi määrusele.

([54]) Euroopa Parlamendi ja nõukogu määrus (EL) nr 575/2013, 26. juuni 2013, krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.6.2013, lk 1).

([55]) 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).

([56]) Vt kavandatava määruse põhjendus 8.

([57]) Vt kavandatava määruse põhjendus 11.

([58]) Vt kavandatava määruse põhjendus 12.

([59]) Vt kavandatava muutmisdirektiivi põhjendused 4 ja 5.

([60]) Vt kapitalinõuete direktiivi artikkel 85.

([61]) Vt kavandatava määruse artikli 4 lõige 1.

([62]) Vt kavandatava määruse artikli 25 lõiked 3 ja 4.

([63]) Vt kavandatava määruse artikkel 41.

([64]) Vt kavandatava määruse V peatüki II jagu.

([65]) Vt kavandatava määruse V peatüki II jagu.

3.6 Liidu seadusandlikud organid võiksid selguse ning kavandatava määruse ja kapitalinõuete direktiivi vahelise kooskõla tagamiseks seega kaaluda järgmisi ettepanekuid. Esiteks võiks kavandatava määruse nõudeid selgesõnaliselt käsitleda usaldatavusnõuetena, nagu seda on tehtud muu hulgas väärtpaberite keskdepositooriumide määruses ([66]). Teiseks võiks kavandatava muutmisdirektiivi põhjenduste sõnastust ([67]) täiendada, võttes arvesse, et kavandatava määruse nõuded ulatuvad situatsiooni- ja talitluspidevuse kavadest kaugemale. IKT-riskide juhtimise meetmed kuuluvad üldiselt kapitalinõuete direktiivi artiklis 74 ([68]) sätestatud kindla juhtimiskorra üldisemasse kohaldamisalasse. Kolmandaks tuleks kavandatavat määrust ([69]) muuta, et juhtida põhjendustes tähelepanu EKP pädevusele teostada krediidiasutuste usaldatavusnõuete täitmise järelevalvet aluslepingu ja ühtse järelevalvemehhanismi määruse alusel. Neljandaks tuleks läbi vaadata viide määruses sätestatud nõuete kohaldamisele individuaalsel ja konsolideeritud tasandil ([70]), kuna allkonsolideeritud ja konsolideeritud tasandeid ei ole kavandatavas määruses määratletud ning teatavat liiki vahendajate suhtes ei kohaldata asjaomaste õigusaktide alusel konsolideeritud järelevalvet (nt makseasutused). Lisaks peaks kavandatava määruse nõuete kohaldamine põhinema ainult vastavat liiki finantssektori ettevõtjate suhtes kohaldatavatel õigusaktidel. Krediidiasutuste puhul on ette nähtud selge seos kapitalinõuete direktiivi ja kavandatava määruse vahel ning seega kohaldatakse kavandatava määruse nõudeid automaatselt vastavalt kas individuaalsel, allkonsolideeritud või konsolideeritud tasandil ([71]). Lõpetuseks võiksid liidu seadusandlikud organid kaaluda üleminekusätete kehtestamist, et reguleerida kavandatava määruse jõustumise ja kavandatavas määruses ette nähtud regulatiivsete tehniliste standardite jõustumise vahelist ajavahemikku, arvestades, et mõnede vahendajate, sealhulgas krediidiasutuste, suhtes juba kehtivad IKT-riske käsitlevad eeskirjad, mida kohaldatakse konkreetsetes sektorites ning mis on üksikasjalikumad kui kavandatava määruse üldsätted.

3.7 EKP-le on ühtse järelevalvemehhanismi määruse alusel antud ülesanne tagada, et krediidiasutused järgiksid liidu õiguse nõudeid, mille kohaselt peavad krediidiasutusel olema usaldusväärsed riskijuhtimisprotsessid ja sisekontrollimehhanismid ([72]). Seega peab EKP tagama, et krediidiasutused rakendavad põhimõtteid ja protsesse, et hinnata ja juhtida operatsiooniriski, sealhulgas mudeliriski, ning hõlmata harvaesinevad, kuid väga tõsised juhtumid. Krediidiasutused on kohustatud määratlema operatsiooniriski asjaomaste põhimõtete ja protsesside tähenduses ([73]).

3.8 2017. aasta juulis võttis Euroopa Keskpanga (EKP) nõukogu EKP järelevalvenõukogu ettepaneku eelnõu alusel kooskõlas ühtse järelevalvemehhanismi määruse artikli 26 lõikega 8 ja artikli 6 lõikega 2 ning Euroopa Keskpanga määruse (EL) nr 468/2014 (EKP/2014/17) ([74]) artikli 21 lõikega 1 vastu ühtse järelevalvemehhanismi küberintsidentidest teatamise raamistiku (edaspidi „raamistik“). Raamistik koosneb siduvast teabe- ja/või aruandlusnõudest (krediidiasutustele adresseeritud üksikotsused) ühtse järelevalvemehhanismi määruse ([75]) artikli 10 alusel. Mõnes riigis on juba kehtestatud intsidentidest teatamise kord, mille kohaselt peab krediidiasutus teatama oma riiklikule pädevale asutusele kõikidest olulistest küberintsidentidest. Nendes riikides teatavad olulised krediidiasutused intsidentidest riiklikule pädevale asutusele, kes edastab need järelevalve alla kuuluvate üksuste nimel põhjendamatu

([66]) Vt väärtpaberite keskdepositooriumide määruse II peatüki 4. jao pealkiri „Usaldatavusnõuded“.

([67]) Vt kavandatava muutmisdirektiivi põhjendus 4.

([68]) Direktiivi 2013/36/EL artikkel 85 on üksnes täpsustus. Vt selles osa ka Euroopa Pangandusjärelevalve 29. novembri 2019. aasta suunised IKT- ja turvariskide juhtimiseks (edaspidi „EBA suunised“) lk 4, 11 ja 37, mille üldine õiguslik alus on selgesõnaliselt sätestatud direktiivi 2013/36/EL artiklis 74.

([69]) Vt kavandatava määruse artikli 41 lõige 1.

([70]) Vt kavandatava määruse artikli 25 lõiked 3 ja 4.

([71]) Vt ka kapitalinõuete direktiivi artikkel 109.

([72]) Vt ühtse järelevalvemehhanismi määruse artikli 4 lõike 1 punkt e.

([73]) Vt kapitalinõuete direktiivi artikkel 85.

([74]) Euroopa Keskpanga määrus (EL) nr 468/2014, 16. aprill 2014, millega kehtestatakse raamistik Euroopa Keskpanga ja riiklike pädevate asutuste vaheliseks ning riiklike määratud asutustega tehtavaks koostööks ühtse järelevalvemehhanismi raames (ühtse järelevalvemehhanismi raammäärus) (EKP/2014/17) (ELT L 141, 14.5.2014, lk 1).

([75]) Eelkõige peab küberintsidendist (võimalik pahatahtlik või juhuslik infoturbe rikkumine) teatama EKP-le, kui esineb vähemalt üks järgmistest tingimustest: 1) võimalik finantsmõju on 5 miljonit eurot ehk 0,1% esimese taseme põhiomavahenditest; 2) juhtumist on teavitatud avalikkust või see tekitab mainekahju; 3) juhtumist on teavitatud infojuhti väljaspool regulaarset aruandlust; 4) pank on juhtumist teatanud CERTile/CSIRTile, julgeolekuasutusele või politseile; 5) algatatud on avariitaaste- või talitluspidevusmenetlus või on esitatud küberkindlustuse nõue; 6) toimunud on õiguslike või regulatiivsete nõuete rikkumine; või 7) pank on sisemiste kriteeriumide ja eksperdiarvamuse (sealhulgas võimalik süsteemne mõju) põhjal otsustanud teavitada EKPd.

viivituseta EKP-le. Seetõttu on eespool nimetatud otsused adresseeritud ka nendele riiklikele pädevatele asutustele, et teave saaks raamistiku alusel edastatud EKP-le. EKP toetab liidu seadusandlike organite jõupingutusi krediidiasutustele kohaldatavate intsidentidest teavitamise eeskirjade ja kohustuste ühtlustamisel. Sellest tulenevalt on EKP valmis raamistikku muutma (ja vajaduse korral kehtetuks tunnistama), võttes arvesse kavandatava määruse vastuvõtmist tulevikus.

4. **Konkreetsed tähelepanekud IKT-riskide juhtimise, intsidentidest teatamise, tegevuskerksuse testimise ja kolmandast isikust tulenevate IKT-riskide kohta**

4.1 *IKT-riskide juhtimine*

4.1.1 EKP toetab kavandatavas määruses kindla ja tervikliku IKT-riskide juhtimise raamistiku kehtestamist, mis hõlmab CPMI-IOSCO küberkerksuse suuniseid ning on tihedalt seotud parimate tavadega, sealhulgas eurosüsteemi küberkerksuse järelevaatamisootustega finantsturutaristute kohta.

4.1.2 EKP toetab ettepanekut, mille kohaselt finantssektori ettevõtjad peaksid läbi viima riskihindamise iga võrgu- ja infosüsteemi taristus toimunud „olulise muudatuse“ osas ([76]). Sellegipoolest ei sisalda kavandatav määrus mõiste „oluline muudatus“ määratlust, tekitades ebasoovitava võimaluse mõiste erinevaks tõlgendamiseks finantssektori ettevõtjate poolt, mis võib lõppkokkuvõttes takistada kavandatava määruse ühtlustamiseesmärgi saavutamist. Õiguskindluse huvides võiksid liidu seadusandlikud organid kaaluda mõiste „oluline muudatus“ määratluse lisamist kavandatavasse määrusesse.

4.1.3 EKP üldiselt toetab ettepanekut, mille kohaselt finantssektori ettevõtjad, mis ei ole mikroettevõtjad, teavitavad pädevaid asutusi kõikidest IKT-katkestustest tingitud kuludest ja kahjudest ning IKTga seotud intsidentidest ([77]). Selleks et tagada süsteemi üldine tulemuslikkus ning vältida pädevate asutuste ja finantssektori ettevõtjate ülekoormamist liigse aruandlusega, võiksid liidu seadusandlikud organid siiski kaaluda asjakohaste künniste kehtestamist, mis võivad olla kvantitatiivsed.

4.1.4 EKP tunnustab finantssektori ettevõtjate võimalust delegeerida IKT-riskide juhtimise nõuete kontrollimine grupisisestele või -välistele ettevõtjatele, kui pädevad asutused on andnud selleks heakskiidu ([78]). Samal ajal on oluline, et liidu seadusandlikud organid täpsustaksid, kuidas toimub pädevate asutuste heakskiidu andmine juhul, kui finantssektori ettevõtja kuulub mitme pädeva asutuse järelevalve alla. Näiteks juhul, kui finantssektori ettevõtja on krediidiasutus, krüptovarateenuste osutaja ja/või makseteenuse pakkuja. Lõpetuseks, seoses finantssektori ettevõtjate kindlaksmääramise ja liigitamisega kavandatava määruse alusel ([79]) peab EKP varade liigitamisel otstarbekaks nõuda kavandatava määrusega finantssektori ettevõtjatelt ka asjaomaste varade kriitilisuse arvesse võtmist (st seda, kas need toetavad kriitilisi funktsioone).

4.2 *Intsidentidest teatamine*

4.2.1 EKP toetab kavandatava määruse püüet ühtlustada IKT-intsidentidest teatamise raamistikku liidus ning tsentraliseerida IKT-riskidega seotud olulistest sündmustest teatamist ([80]). Ühtlustatud raamistiku kehtestamine IKT-riskidega seotud olulistest sündmustest teatamiseks asjaomastele pädevatele asutustele ([81]) aitaks ühtlustada finantssektori ettevõtjate, sealhulgas krediidiasutuste, aruandluskoormust. Pädevate asutuste seisukohast oleks otstarbekas, kui intsidentidest teatamine oleks laialdasem ning ulatuks olemasolevate raamistikega hõlmatud küberintsidentidest kaugemale ([82]). Kavandatava määruse vastuvõtmiseks oleks vaja olemasolevad raamistikud, sealhulgas ühtse järelevalvemehhanismi küberintsidentidest teatamise raamistik, läbi vaadata ning vajadusel kehtetuks tunnistada. Täielikult ühtlustatud raamistiku saavutamiseks on äärmiselt oluline tagada, et kavandatavas määruses ette nähtud intsidentidest teatamist käsitlevate sätete kohaldamisala, sealhulgas kõik asjakohased määratlused, künnised ja aruandlusparameetrid, oleks täielikult kooskõlas asjaomaste raamistikega. Eriti oluline on

([76]) Vt kavandatava määruse artikli 7 lõige 3.
([77]) Vt kavandatava määruse artikli 10 lõige 9.
([78]) Vt kavandatava määruse artikli 5 lõige 10.
([79]) Vt kavandatava määruse artikkel 7.
([80]) Vt kavandatava määruse artikkel 19.
([81]) Vt kavandatava määruse artikli 3 lõige 7 ning artiklid 17 ja 18.
([82]) Vt nt raamistik.

tagada kooskõla ühelt poolt kavandatava määruse ning teiselt poolt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 ([83]) (edaspidi „teine makseteenuste direktiiv“) ja Euroopa Pangandusjärelevalve olulistest intsidentidest teatamise suuniste (edaspidi „EBA suunised“) vahel. Kavandatav muutmisdirektiiv ([84]) sisaldab teise makseteenuste direktiivi muudatusi seoses intsidentidest teatamise piiritlemisega kavandatava määruse ja teise makseteenuste direktiivi vahel, mis mõjutaks peamiselt makseteenuse pakkujaid, kellele võidakse anda ka krediidiasutuse tegevusluba, ning pädevaid asutusi. Intsidentidest teatamise protsess ei ole piisavalt selge ning mõnede intsidentide osas on kattuvusi, ehk nendest tuleb teatada nii kavandatava määruse kui ka EBA suuniste alusel.

4.2.2 Kavandatavas määruses ([85]), teises makseteenuste direktiivis ja asjaomastes EBA suunistes ette nähtud olulistest intsidentidest teatamise nõuete kohaselt peaksid makseteenuse pakkujad esitama pärast intsidendi liigitamist selle kohta oma pädevale asutusele aruande. Tegelikult ei kajasta esialgsed aruanded intsidendi sisu, põhjust ega valdkondi, mida intsident mõjutab, ning makseteenuse pakkujad saavad selliseid eristusi teha alles hilisemas etapis, kui intsidendi kohta kogutakse põhjalikumat teavet. Seetõttu võiks esialgseid intsidentide aruandeid esitada nii kavandatava määruse kui EBA suuniste alusel; alternatiivina võiksid makseteenuse pakkujad otsustada ühtse aruandlusraamistiku kasuks ning oma aruannet hiljem täpsustada. Samasugust ebakindlust (näiteks intsidendi algse põhjuse osas) võib ilmneda ka vahe- ja lõpparuannetes. Ka siin võib kaasneda aruannete paralleelne esitamine pädevatele asutustele nii kavandatava määruse kui teise makseteenuste direktiivi alusel.

4.2.3 Mõned intsidendid, mida võib liigitada IKTga seotud intsidentideks, võivad mõjutada ka muid valdkondi ning seetõttu tuleks neist EBA suuniste kohaselt viivitamatult teatada. Näiteks kui intsidendil on IKTga seotud mõju, kuid samas on see mõjutanud ka makseteenuste osutamist otseselt ja/või muudes IKTga mitteseotud valdkondades või kanalites. Lisaks ei pruugi mõnede intsidentide puhul olla võimalik eristada operatsiooni- ja IKTga seotud intsidente. Kui asjaomane finantssektori ettevõtja on oluline krediidiasutus ja makseteenuse pakkuja, peaks ta kavandatava määruse kohaselt teavitama IKTga seotud intsidendist kaks korda, kahele pädevale asutusele. Eeltoodust tulenevalt peaks kavandatav määrus täpsustama, kuidas teise makseteenuste direktiivi ja EBA suuniste koosmõju praktikas toimib. Aruandluskohustuste ühtlustamise huvides oleks veelgi olulisem, et liidu seadusandlikud organid täpsustaksid topeltaruandluse küsimusi ning selgitaksid, kas ühelt poolt kavandatav määrus ning teiselt poolt teine makseteenuste direktiiv ja EBA suunised kehtiksid paralleelselt või tuleks kehtestada ühtsed intsidentidest teatamise nõuded.

4.2.4. Kavandatava määrusega kehtestatakse nõue ([86]), mille kohaselt peavad pädevad asutused aruande saamisel kinnitama teate kättesaamist ja esitama võimalikult kiiresti kogu vajaliku tagasiside või suunised finantssektori ettevõtjale, et eelkõige arutada parandusmeetmeid ettevõtja tasandil või viise kahjuliku mõju minimeerimiseks sektorite lõikes. See tähendab, et pädevad asutused peaksid aktiivselt osalema intsidentide haldamises ja parandamises ning samal ajal hindama järelevalve alla kuuluva üksuse reageerimist kriitilistele intsidentidele. EKP rõhutab, et vastutus ja omavastutus intsidendi parandamise ja tagajärgede eest peaks jääma ainult ja selgelt asjaomasele finantssektori ettevõtjale. Seetõttu teeb EKP ettepaneku piirduda tagasiside ja suuniste andmisel ainult kõrgetasemelise usaldatavusnõuete alase tagasiside ja suunistega. Laiem tagasiside nõuaks väga laialdaste tehniliste teadmistega spetsialistide kaasamist, keda usaldatavusjärelevalve asutuste talendipagas tavapäraselt ei sisalda.

4.3 *Digitaalse tegevuskerksuse testimine*

4.3.1 EKP toetab kavandatavas määruses sätestatud nõudeid ([87]) finantssektori ettevõtjate digitaalse tegevuskerksuse testimise kohta ning testimiskava olemasolu kohta igas ettevõtjas. Kavandatavas määruses ([88]) kirjeldatakse finantssektori ettevõtjatele mõeldud erinevat liiki teste. Testide liigid ei ole kõige selgemad ning mõned testid - näiteks ühilduvuse testid, küsimustikud või stsenaariumipõhised testid - on ESAde, pädevate asutuste või

([83]) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2015/2366, 25. november 2015, makseteenuste kohta siseturul, direktiivide 2002/65/EÜ, 2009/110/EÜ ning 2013/36/EL ja määruse (EL) nr 1093/2010 muutmise ning direktiivi 2007/64/EÜ kehtetuks tunnistamise kohta (ELT L 337, 23.12.2015, lk 35).

([84]) Vt kavandatava muutmisdirektiivi artikli 7 lõige 9.

([85]) Vt kavandatava määruse artikli 17 lõige 3.

([86]) Vt kavandatava määruse artikkel 20.

([87]) Vt kavandatava määruse artiklid 21 ja 22.

([88]) Vt kavandatava määruse artikli 22 lõige 1.

finantssektori asutuste poolt tõlgendatavad. Lisaks puuduvad suunised testimise sageduse kohta. Üks võimalik lähenemisviis on sätestada üldised testimisnõuded kavandatavas määruses ning testide liikide täpsem kirjeldus regulatiivsetes ja rakenduslikes tehnilistes standardites.

4.3.2 Ohuteabel põhinev läbistustestimine on tõhus vahend kaitsemeetmete ja valmisoleku testimiseks. Seetõttu kutsub EKP finantssektori ettevõtjaid üles viima läbi ohuteabel põhinevaid läbistustestimisi. See vahend võimaldab testida mitte üksnes tehnilisi meetmeid, vaid ka töötajaid ja protsesse. Asjaomaste testide tulemused võivad oluliselt suurendada testitavate ettevõtjate kõrgema juhtkonna turvateadlikkust. ELi TIBER-raamistik (European Framework for Threat Intelligence Based Ethical Red-teaming) ([89]) ja muud väljaspool liitu juba kättesaadavad ohuteabel põhineva läbistustestimise vahendid on peamine meetod, mille abil ettevõtjad saavad ise hinnata, testida, rakendada ja parandada oma küberkerksust ja -kaitsevõimet.

4.3.3 Enamikus liikmesriikides, kus ELI TIBER-raamistik on rakendatud, ei osale järelevaatamis- ja järelevalveasutused aktiivselt TIBER-XX kohaliku programmi rakendamises ning TIBERi kübermeeskond (TCT) tegutseb peaaegu kõigil juhtudel nendest funktsioonidest sõltumatult. Seepärast tuleks kavandatavas määruses sätestatud ohuteabel põhinevatel läbistustestidel tuginevat süvatestimist ([90]) rakendada pigem finantsökosüsteemi tugevdamise ja finantsstabiilsuse suurendamise vahendina, kui puhtalt järelevalvevahendina. Lisaks puudub uue kõrgetasemelise küberkerksuse testimise raamistiku väljatöötamiseks vajadus, kuna liikmesriigid on juba laialdaselt vastu võtnud ELi TIBER-raamistiku, mis on praegu ELis ainus selline raamistik.

4.3.4 Testijatele esitatavad nõuded ei peaks sisalduma kavandatava määruse põhiosas, kuna ohuteabel põhineva läbistustestimise sektor on alles arenemas ning konkreetsete nõuete kehtestamine võib takistada innovatsiooni. Sellest hoolimata on EKP seisukohal, et sõltumatuse tagamiseks testimise läbiviimisel ei tohiks finantssektori ettevõtjad kasutada testijaid, kellel on grupi ettevõtjatega sõlmitud tööleping või töövõtuleping, või kes on muul viisil testitavate finantssektori ettevõtjate omanduses ja/või kontrolli all.

4.3.5 Killustatuse ohu vähendamiseks ning ühtlustamise tagamiseks tuleks kavandatava määrusega kehtestada üks ohuteabel põhineva läbistustestimise raamistik, mida kohaldatakse kogu liidu finantssektori suhtes. Killustatus võib suurendada nii pädevate asutuste kui ka finantseerimisasutuste kulusid ning tehnilisi, operatsioonilisi ja rahalisi vajadusi. Sellised kulud ja nõuded võivad lõppkokkuvõttes avaldada negatiivset mõju testide vastastikusele tunnustamisele. Puudulik ühtlustatus ning sellest tulenevad vastastikuse tunnustamise probleemid on eriti olulised finantseerimisasutuste jaoks, kellel võib olla mitu tegevusluba ja/või kes võivad tegutseda liidu mitmes jurisdiktsioonis. Regulatiivsed ja rakenduslikud tehnilised standardid, mis tuleb kavandatava määruse kohaselt ohuteabel põhineva läbistustestimise jaoks koostada, peaksid olema kooskõlas ELi TIBER-raamistikuga. Samuti toetab EKP võimalust osaleda kõnealuste regulatiivsete ja rakenduslike tehniliste standardite ettevalmistamisel koostöös ESAdega.

4.3.6 Pädevate asutuste aktiivne osalemine testide läbiviimisel võib põhjustada huvide konflikti teise funktsiooniga, mida nad täidavad, st finantssektori ettevõtjate testimisraamistiku hindamisega. Sellest tulenevalt teeb EKP ettepaneku jätta kavandatavast määrusest välja pädevate asutuste mis tahes kohustused seoses dokumentide valideerimise ja ohuteabel põhineva läbistustestimise tõendi väljastamisega.

4.4 Kolmandast isikust tulenevad IKT-riskid

4.4.1 EKP toetab kolmandast isikust teenuseosutajast tulenevate IKT-riskide kindlaksmääramiseks ja juhtimiseks oluliste põhimõtete ja tugeva järelevalveraamistiku kehtestamist, sõltumata sellest, kas asjaomased teenuseosutajad kuuluvad samasse finantssektori ettevõtjate gruppi. IKT-riskide tõhusaks kindlaksmääramiseks ja juhtimiseks on oluline nõuetekohaselt kindlaks määrata ja liigitada muu hulgas kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad. Kuigi EKP toetab delegeeritud õigusaktide vastuvõtmist ([91]), et täiendada liigitamisel kasutatavaid kriteeriume ([92]), tuleks EKPga enne selliste delegeeritud õigusaktide vastuvõtmist konsulteerida.

([89]) Avaldatud EKP veebilehel www.ecb.europa.eu.
([90]) Kavandatava määruse artiklid 23 ja 24.
([91]) Vt kavandatava määruse artikli 28 lõige 3.
([92]) Vt kavandatava määruse artikli 28 lõige 2.

4.4.2 Järelevalveraamistiku struktuuri osas ([93]) on vaja täiendavalt selgitada ühiskomitee rolli. Samal ajal toetab EKP oma kaasamist järelevalvefoorumisse vaatlejana, kuna see võimaldab EKP-le samasugust juurdepääsu dokumentidele ja teabele nagu hääleõiguslikel liikmetel ([94]). EKP soovib juhtida liidu seadusandlike organite tähelepanu asjaolule, et EKP panustaks oma vaatlejarollis järelevalvefoorumi töösse nii emiteeriva keskpangana, kes vastutab turutaristute järelevaatamise eest, kui ka krediidiasutuste usaldatavusnõuete täitmise järelevalveasutusena. Täiendavalt märgib EKP, et lisaks järelevalvefoorumis vaatlejana tegutsemisele kuuluks EKP pädeva asutusena ka ühisesse kontrollirühma. Selles osas võiksid liidu seadusandlikud organid täiendavalt kaaluda ühiste kontrollirühmade koosseisu ([95]), et tagada asjaomaste pädevate asutuste asjakohane esindatus. Samuti leiab EKP, et ühistes kontrollirühmades osalejate maksimaalset arvu tuleks suurendada, võttes arvesse kolmandast isikust teenuseosutajate pakutavate IKT-teenuste kriitilisust, keerukust ja ulatust.

4.4.3 EKP juhib tähelepanu asjaolule, et kavandatava määruse kohaselt võib juhtiv järelevalveasutus takistada kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal täiendavate alltöövõtulepingute sõlmimist, kui i) kavandatav alltöövõtja on kolmandast isikust IKT-teenuste osutaja või kolmandas riigis asutatud IKT-alltöövõtja ning ii) alltöövõtt on seotud finantssektori ettevõtja kriitilise tähtsusega või olulise funktsiooniga. EKP soovib rõhutada, et neid volitusi saab juhtiv järelevalveasutus kasutada alltöövõtulepingute kontekstis ainult juhul, kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja sõlmib alltöövõtulepingu kriitilise tähtsusega või olulise funktsiooni täitmiseks eraldiseisva juriidilise isikuga, mis on asutatud kolmandas riigis. EKP arusaama kohaselt ei tohiks juhtiv järelevalveasutus kasutada selliseid volitusi, et takistada kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonide allhanke korras tellimist sellelt kolmandas riigis asuvalt teenuseosutajalt. Näiteks võib tegevuse seisukohast olla võimalik, et kriitilise tähtsusega andmeid ja/või teavet talletatakse või töödeldakse väljaspool Euroopa Majanduspiirkonda (EMP) asuvates rajatistes. Sellisel juhul ei pruugi juhtiva järelevalveasutuse volitused anda pädevatele asutustele piisavat õigust pääseda juurde kogu teabele, ruumidele, taristule ja personalile, mis on vajalikud finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonide täitmiseks. Tagamaks, et pädevad asutused saaksid oma ülesandeid täita takistusteta, teeb EKP ettepaneku anda juhtivale järelevalveasutusele õiguse piirata ka väljaspool EMPd asuvate rajatiste kasutamist kriitilise tähtsusega kolmandast isikuste IKT-teenuste osutajate poolt. Seda õigust võiks kasutada konkreetsetel juhtudel, kui kavandatava määruse kohaselt ei ole asjaomaste kolmandate riikide ametiasutustega sõlmitud halduskokkuleppeid ([96]) või kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate esindajad ei taga asjaomase kolmanda riigi raamistikus piisavat kindlust juurdepääsu kohta järelevaatamis- või järelevalveülesannete täitmiseks vajalikule teabele, ruumidele, taristule ja personalile.

4.4.4 Lõpetuseks võib nõue, mille kohaselt pädevad asutused peavad võtma järelmeetmeid juhtiva järelevalveasutuse soovituste osas ([97]), osutuda ebatõhusaks, kuna pädevatel asutustel ei pruugi olla terviklikku ülevaadet iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja riskidest. Lisaks võib pädevatelt asutustelt nõuda meetmete võtmist nende järelevalve alla kuuluvate finantssektori ettevõtjate suhtes, kui kriitilise tähtsusega kolmandast isikust teenuseosutajad soovitusi ei järgi. Kavandatava määruse kohaselt ([98]) võivad pädevad asutused nõuda, et nende järelevalve alla kuuluvad finantssektori ettevõtjad peataksid ajutiselt teenuste osutamise kriitilise tähtsusega kolmanda isiku poolt või lõpetaksid kriitilise tähtsusega kolmandast isikust teenuseosutajatega sõlmitud kehtivad lepingud. Kavandatavaid järelmeetmeid on keeruline lahti mõtestada konkreetseteks tegevusteks. Täpsemalt ei ole selge, kas järelevalve alla kuuluval finantssektori ettevõtjal on võimalik kriitilise tähtsusega kolmandast isikust teenuseosutajaga sõlmitud leping peatada või lõpetada. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja võib olla selle finantssektori ettevõtja jaoks oluline teenuseosutaja; samuti võivad tekkida lepingujärgsed või muud kulud ja kahjud, mida finantssektori ettevõtja peab lepingu peatamise või lõpetamise tõttu kandma. Lisaks ei toeta see lähenemisviis järelevaatamise ühtlustamist, kuna pädevad asutused võivad tõlgendada sama soovitust erinevalt. Lõppkokkuvõttes võib see takistada kavandatavat ühtlustamist ja järjepidevat lähenemisviisi kriitilise tähtsusega kolmandast isikust tulenevate IKT-riskide jälgimisel liidu tasandil. Eeltoodut arvesse võttes võiksid liidu seadusandlikud organid kaaluda võimalust anda õiguslikele järelevalveasutustele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes konkreetsed volitused, võttes arvesse Meroni doktriiniga kehtestatud piiranguid, mida Euroopa Kohus on ESMA kohtuasjas tehtud otsuses osaliselt leevendanud ([99]).

([93]) Vt kavandatava määruse artikkel 29.
([94]) Vt kavandatava määruse artikli 29 lõige 3.
([95]) Vt kavandatava määruse artikkel 35.
([96]) Vt kavandatava määruse artikli 39 lõige 1.
([97]) Vt kavandatava määruse artikli 29 lõige 4 ning artikkel 37.
([98]) Vt kavandatava määruse artikli 37 lõige 3.
([99]) Vt Euroopa Kohtu otsus (suurkoda), 22. jaanuar 2014, Suurbritannia ja Põhja-Iiri Ühendkuningriik versus Euroopa Parlament ja Euroopa Liidu Nõukogu, määrus (EL) nr 236/2012 — Kohtuasi C-270/12.

Teksti redaktsiooni ettepanekud, mille puhul EKP on soovitanud ettepandud määrust muuta, on esitatud eraldi tehnilises töödokumendis koos selgitustega. Tehniline töödokument on avaldatud inglise keeles EUR-Lexis.

Frankfurt Maini ääres, 4. juuni 2021

EKP president
Christine LAGARDE