EUROOPA
KOMISJON

Brüssel, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014

(EMPs kohaldatav tekst)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

SELETUSKIRI

1. ETTEPANEKU TAUST

- Ettepaneku põhjused ja eesmärgid

See ettepanek on osa digirahanduse paketist. See on meetmepakett, mille eesmärk on kasutada ja toetada digirahanduse potentsiaali innovatsiooni ja konkurentsi valdkonnas, maandades samal ajal riske See on kooskõlas komisjoni prioriteetidega muuta Euroopa digiajastule vastavaks ja rajada tulevikuks sobiv ja inimeste hüvanguks toimiv majandus. Digirahanduse pakett sisaldab ELi finantssektori uut digirahanduse strateegiat,[1] mille eesmärk on tagada, et EL kasutaks digirevolutsiooni võimalusi ja juhiks seda koos innovatiivsete Euroopa ettevõtjatega, et teha digirahanduse eelised kättesaadavaks tarbijatele ja ettevõtjatele. Lisaks sellele ettepanekule sisaldab pakett ka ettepanekut võtta vastu määrus krüptovaraturgude kohta,[2] ettepanekut võtta vastu määrus hajusraamatu tehnoloogial põhinevate turutaristute katsekorra kohta[3] ja ettepanekut võtta vastu direktiiv teatavate seonduvate ELi finantsteenuste normide selgitamiseks või muutmiseks[4]. Finantssektoris on digiteerimine ja tegevuskerksus ühe mündi kaks poolt. Digi- ehk info- ja kommunikatsioonitehnoloogia (IKT) tekitab nii võimalusi kui ka riske. Neid on vaja hästi mõista ja juhtida, eriti pingelisel ajal.

Seepärast on poliitikakujundajad ja järelevalveasutused keskendunud üha enam riskidele, mis tulenevad IKTst sõltumisest. Nad on eelkõige püüdnud suurendada ettevõtjate vastupanuvõimet standardite kehtestamise ning regulatiivse või järelevalvealase töö koordineerimise kaudu. Seda tööd on tehtud nii rahvusvahelisel kui ka Euroopa tasandil, nii tööstusharude lõikes kui ka mitmes konkreetses sektoris, sealhulgas finantsteenuste sektoris.

IKT-riskid on aga jätkuvalt probleem ELi finantssüsteemi tegevuskerksuse, suutlikkuse ja stabiilsuse jaoks. 2008. aasta finantskriisile järgnenud reformiga tugevdati peamiselt ELi finantssektori finantsvastupidavust[5]; IKT-riske käsitleti ainult kaudselt ja üksikutes valdkondades, osana meetmetest, millega tegeleti operatsiooniriskidega laiemalt.

ELi finantsteenuseid käsitlevates õigusaktides kriisi järel tehtud muudatustega loodi küll ühtne reeglistik, mis reguleerib suurt osa finantsteenustega seotud finantsriskidest, kuid need ei käsitlenud täielikult digitaalset tegevuskerksust. Viimasega seoses võetud meetmeid iseloomustasid mitmed omadused, mis piirasid nende tulemuslikkust. Näiteks olid need sageli kavandatud minimaalse ühtlustamise direktiivide või põhimõtetel põhinevate määrustena ning jätsid ühtsel turul palju ruumi erinevatele lähenemisviisidele. Lisaks on IKT-riske käsitletud operatsiooniriski kontekstis ainult piiratult või mittetäielikult. Peale selle on need meetmed finantsteenuseid käsitlevate valdkondlike õigusaktide lõikes erinevad. Seega ei vastanud sekkumine liidu tasandil täielikult sellele, mida Euroopa finantssektori ettevõtjad vajasid

---

1 Komisjoni 23. septembri 2020. aasta teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Euroopa Keskpangale, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele ELi digirahanduse strateegia kohta (COM(2020) 591).

2 Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb krüptovaraturge ja millega muudetakse direktiivi (EL) 2019/1937 (COM/2020/593).

3 Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu määrus hajusraamatu tehnoloogial põhinevate turutaristute katsekorra kohta (COM(2020) 594).

4 Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, millega muudetakse direktiive 2006/43/EÜ, 2009/65/EÜ, 2009/138/EL, 2011/61/EL, EL/2013/36, 2014/65/EL, (EL) 2015/2366 ja EL/2016/2341 (COM(2020)596).

5 Mitmesuguste vastu võetud meetmete põhieesmärk oli suurendada finantssektori ettevõtjate kapitaliressursse ja likviidsust ning vähendada turu- ja krediidiriske.

operatsiooniriskide juhtimiseks viisil, mis võimaldaks IKTga seotud intsidentide mõjuga toime tulla, sellele reageerida ja sellest taastuda. Samuti ei andnud see finantsjärelevalveasutustele kõige sobivamaid vahendeid ülesannete täitmiseks, et vältida kõnealuste IKT-riskide realiseerumisest tulenevat finantsilist ebastabiilsust.

Asjaolu, et ELi tasandil ei ole üksikasjalikke ja laiahaardelisi norme digitaalse tegevuskerksuse kohta, on toonud kaasa palju erinevaid riiklikke regulatiivseid algatusi (nt digitaalse tegevuskerksuse testimise kohta) ja järelevalvealaseid lähenemisviise (mis käsitlevad näiteks sõltuvust IKT-teenuseid osutavatest kolmandatest isikutest). Liikmesriikide tasandi meetmetel on aga ainult piiratud mõju, kuna IKT-riskid on laadilt piiriülesed. Lisaks on koordineerimata riiklikud algatused põhjustanud kattuvust, ebaühtlust, dubleerivaid nõudeid, suuri haldus- ja nõuete täitmisega seotud kulusid – eelkõige piiriüleste finantssektori ettevõtjate jaoks – või IKT-riskide avastamata ja järelikult käsitlemata jäämist. See olukord killustab ühtset turgu, kahjustab ELi finantssektori stabiilsust ja usaldusväärsust ning seab ohtu investorite ja tarbijate kaitse.

Seepärast on vaja luua ELi finantssektori ettevõtjate jaoks üksikasjalik ja laiahaardeline digitaalse tegevuskerksuse raamistik. See raamistik süvendab ühtse reeglistiku digiriski juhtimise mõõdet. Eelkõige tõhustab ja ühtlustab see IKT-riskide juhtimist finantssektori ettevõtjate poolt, kehtestab IKT-süsteemide põhjaliku testimise, suurendab järelevalveasutuste teadlikkust finantssektori ettevõtjate küberriskidest ja IKTga seotud intsidentidest ning annab finantsjärelevalveasutustele õiguse jälgida riske, mis tulenevad finantssektori ettevõtjate sõltuvusest kolmandast isikust IKT-teenuste osutajatest. Ettepanekuga luuakse ühtne intsidentidest teatamise mehhanism, mis aitab vähendada finantssektori ettevõtjate halduskoormust ja suurendada järelevalve tulemuslikkust.

- Kooskõla poliitikavaldkonnas praegu kehtivate õigusnormidega

Käesolev ettepanek on osa Euroopa ja rahvusvahelisel tasandil käimasolevast laiemast tööst, mille eesmärk on tugevdada küberturvalisust finantsteenuste valdkonnas ja käsitleda laiemalt operatsiooniriske[6].

See vastab ka Euroopa järelevalveasutuste 2019. aasta ühisele tehnilisele nõuandele,[7] milles kutsuti üles kasutama rahanduse valdkonnas IKT-riskide puhul ühtsemat lähenemisviisi ja soovitati komisjonil proportsionaalselt tugevdada finantsteenuste sektori digitaalset tegevuskerksust ELi sektoripõhise algatuse kaudu. Euroopa järelevalveasutuste nõuanne oli vastus komisjoni 2018. aasta finantstehnoloogia tegevuskavale[8].

- Kooskõla muude liidu tegevuspõhimõtetega

Nagu märkis president von der Leyen oma poliitilistes suunistes[9] ja nagu on mainitud teatises „Euroopa digituleviku kujundamine“,[10] on väga oluline, et Euroopa kasutaks ära kõik digiajastu hüved ning tugevdaks oma tööstust ja innovatsioonisuutlikkust ohututes ja eetilistes

---

6 Baseli pangajärelevalve komitee, „Cyber-resilience: Range of practices“, detsember 2018, ja „Principles for sound management of operational risk (PSMOR)“, oktoober 2014.

7 Euroopa järelevalveasutuste ühine nõuanne Euroopa Komisjonile, milles käsitletakse vajadust selliste seadusandlike paranduste järele, mis on seotud IKT-riskide juhtimise nõuetega ELi finantssektoris (JC 2019 26 (2019)).

8 Euroopa Komisjoni finantstehnoloogia tegevuskava (COM(2018) 109 final).

9 President Ursula Von Der Leyen, „Poliitilised suunised järgmisele Euroopa Komisjonile (2019–2024)“, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_et.pdf.

10 Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa digituleviku kujundamine“ (COM(2020) 67 final).

piirides. Euroopa andmestrateegias[11] on sätestatud neli sammast – andmekaitse, põhiõigused, turvalisus ja küberjulgeolek –, mis on andmepõhise ühiskonna olulised eeltingimused. Euroopa Parlament tegeleb digirahanduse aruandega, milles nõutakse muu hulgas ühist lähenemist finantssektori küberkerksusele[12]. ELi finantssektori ettevõtjate digitaalset tegevuskerksust suurendav õigusraamistik on nende poliitikaeesmärkidega kooskõlas. Ettepanek toetaks ka poliitikat, mille eesmärk on koroonaviirusest taastumine, kuna see tagaks, et suurem tuginemine digirahandusele käib käsikäes tegevuskerksusega.

Algatus säilitaks küberturvalisuse horisontaalse raamistiku (nt võrgu- ja infosüsteemide turvalisuse direktiiv ehk küberturvalisuse direktiiv) eelised. Finantssektor jääks tihedalt seotuks võrgu- ja infosüsteemide turvalisuse koostööorganiga ning finantsjärelevalveasutused saaksid vahetada asjakohast teavet olemasolevas võrgu- ja infosüsteemide ökosüsteemis. See algatus oleks kooskõlas Euroopa elutähtsate infrastruktuuride direktiiviga, mida vaadatakse praegu läbi, et suurendada elutähtsate infrastruktuuride kaitset ja vastupidavust muude kui küberohtude suhtes. Käesolev ettepanek on täielikult kooskõlas julgeolekuliidu strateegiaga,[13] milles nõuti algatust, mis käsitleks finantssektori digitaalset tegevuskerksust, sest see sektor sõltub palju IKT-teenustest ja on küberrünnete suhtes väga haavatav.

2. ÕIGUSLIK ALUS, SUBSIDIAARSUS JA PROPORTSIONAALSUS

- Õiguslik alus

Kavandatava määruse õiguslik alus on ELi toimimise lepingu artikkel 114.

Sellega kõrvaldatakse finantsteenuste siseturu tõkked ning parandatakse selle väljakujundamist ja toimimist, ühtlustades norme, mida kohaldatakse IKT-riskide juhtimise, teavitamise, testimise ja kolmandast isikust tulenevate IKT-riskide valdkonnas. Selles valdkonnas on praegu nii seadusandlikul kui ka järelevalvetasandil, samuti riiklikul ja ELi tasandil, lahknevusi, mis kujutavad endast finantsteenuste ühtse turu jaoks tõkkeid, sest piiriüleselt tegutsevad finantssektori ettevõtjad puutuvad kokku erinevate või kattuvate regulatiivsete nõuete või järelevalveootustega ning see võib takistada neid asutamisvabadust ja teenuste osutamise vabadust kasutamast. Erinevad normid moonutavad ka eri liikmesriikides tegutsevate sama tüüpi finantssektori ettevõtjate vahelist konkurentsi. Valdkondades, kus ühtlustamist ei ole toimunud või see on osaline või piiratud, võib lahknevate – kas juba jõustunud või riiklikul tasandil vastuvõtmisel ja rakendamisel – riiklike normide või lähenemisviiside arendamine kahjustada finantsteenuste puhul ühtse turu vabadusi. See kehtib eelkõige digitaalsete operatiivsete testimisraamistike ning kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalve puhul.

Kuna ettepanek mõjutab mitut ELi toimimise lepingu artikli 53 lõike 1 alusel vastu võetud Euroopa Parlamendi ja nõukogu direktiivi, võetakse samal ajal vastu ka direktiivi ettepanek, et kajastada kõnealuste direktiivide vajalikke muudatusi.

---

[11] Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele, „Euroopa andmestrateegia“ (COM(2020) 66 final).

[12] „Report with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets“ (2020/2034(INL)), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

[13] Komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele ELi julgeolekuliidu strateegia kohta (COM(2020) 605 final).

- Subsidiaarsus

Kuna finantsteenused on üksteisega väga tihedalt seotud, finantssektori ettevõtjad tegutsevad suuresti piiriüleselt ja finantssektor tervikuna sõltub suurel määral kolmandast isikust IKT-teenuste osutajatest, tuleb võimaldada suurt digitaalset tegevuskerksust, mis on üldistes huvides, et hoida ELi finantsturgude usaldusväärsust. Ebaühtlastest või osalistest raamistikest tulenevaid lahknevusi, kattuvusi või seda, et samade piiriüleselt tegutsevate või mitme tegevusloaga[14] finantssektori ettevõtjate suhtes kohaldatakse ühtsel turul erinevaid nõudeid, saab tõhusalt käsitleda ainult liidu tasandil.

Käesoleva ettepanekuga ühtlustatakse sügavalt integreeritud ja seotud sektori digitaalset tegevuskomponenti, millel enamikus muudes olulistes valdkondades on juba ühtsed normid ja järelevalve. IKTga seotud intsidentidest teatamise puhul saab halduskoormust ja rahalisi kulusid, mis on seotud erinevate liidu ja riiklikele ametiasutuste teavitamisega samast IKTga seotud intsidentist, vähendada vaid liidu ühtlustatud normidega. ELi meedet on vaja ka selleks, et edendada digitaalse tegevuskerksuse süvatestimise tulemuste vastastikust tunnustamist selliste piiriüleselt tegutsevate ettevõtjate puhul, mille suhtes liidu normide puudumise korral kohaldatakse või võidakse kohaldada eri liikmesriikides erinevaid raamistikke. Ainult liidu tasandi meetmega saab vähendada liikmesriikides kasutusele võetud testimist käsitlevate lähenemisviiside erinevusi. Kogu ELi hõlmavat meedet on vaja ka sellise probleemi lahendamiseks, et puuduvad asjakohased järelevalvevolitused kolmandast isikust IKT-teenuste osutajatest tulenevate riskide jälgimiseks, sealhulgas ELi finantssektori kontsentratsiooni- ja ülekandumisrisk.

- Proportsionaalsus

Kavandatavad normid ei lähe ettepaneku eesmärkide saavutamiseks vajalikust kaugemale. Need hõlmavad ainult neid aspekte, mida liikmesriigid üksi ei suuda saavutada ning mille puhul halduskoormus ja -kulud vastavad konkreetsetele ja üldistele eesmärkidele, mida soovitakse saavutada.

Proportsionaalsuse puhul on võetud arvesse nii kohaldamisala kui ka mahukust, kasutades kvalitatiivseid ja kvantitatiivseid hindamiskriteeriume. Nende eesmärk on tagada, et kuigi uued normid hõlmavad kõiki finantssektori ettevõtjaid, on nad samal ajal kohandatud vastavalt riskidele ja vajadustele, mis tulenevad nende konkreetsetest, suuruse ja äriprofiiliga seotud eripäradest. Proportsionaalsust hõlmavad ka normid IKT-riskide juhtimise, digitaalse tegevuskerksuse testimise, IKTga seotud olulistest sündmustest teatamise ja kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalve kohta.

- Vahendi valik

Meetmed, mida on vaja selleks, et reguleerida IKT-riskide juhtimist, IKTga seotud intsidentidest teatamist, testimist ja kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalvet, tuleb sätestada määruses, et üksikasjalikud nõuded oleksid tegelikult ja vahetult ühetaoliselt kohaldatavad, ilma et see piiraks proportsionaalsust ja käesoleva määrusega ette nähtud erinorme. Digitaalsete operatsiooniriskide ühtne käsitlemine aitab suurendada usaldust finantssüsteemi vastu ja säilitada selle stabiilsust. Kuna määruse kasutamine aitab vähendada regulatiivset keerukust, edendab järelevalvealast ühtsust ja suurendab õiguskindlust, aitab käesolev määrus piirata ka finantssektori ettevõtjate, eelkõige

[14] Ühel finantssektori ettevõtjal võib olla pangandus-, investeerimisühingu ja makseasutuse litsents, millest igaühe on välja andnud erinev järelevalveasutus ühes või mitmes liikmesriigis.

piiriüleselt tegutsevate ettevõtjate nõuete täitmisega seotud kulusid, mis omakorda aitab kõrvaldada konkurentsimoonutusi.

Tänu sellele määrusele kaovad ka õigusnormide erinevused ja liikmesriikide ebaühtlane regulatiivne või järelevalvealane lähenemine IKT-riskile ning seega kõrvaldatakse finantsteenuste ühtse turu, eelkõige asutamisvabaduse sujuva kasutamise ja piiriüleselt tegutsevate finantssektori ettevõtjate teenuste osutamise takistused.

Ühtse reeglistiku väljatöötamisel on enamasti kasutatud määruseid ning sellesse digitaalse tegevuskerksuse komponendi lisamiseks tuleks kasutada sama õiguslikku vahendit.

3. JÄRELHINDAMISE, SIDUSRÜHMADEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

- Praegu kehtivate õigusaktide järelhindamine või toimivuse kontroll

Üheski senises liidu õigusaktis, milles käsitletakse finantsteenuseid, ei ole keskendutud tegevuskerksusele ega käsitletud põhjalikult digiteerimisest tulenevaid riske, isegi mitte nendes, milles sisalduvad õigusnormid puudutavad üldisemalt operatsiooniriski mõõdet, mille üks alamkomponent on IKT-risk. Liidu sekkumine on seni aidanud käsitleda vajadusi ja probleeme 2008. aasta finantskriisi järel: krediidiasutused ei olnud piisavalt kapitaliseeritud, finantsturud ei olnud piisavalt integreeritud ja ühtlustamine oli tolle hetkeni olnud minimaalne. IKT-riski ei peetud sel ajal prioriteediks ja finantssektori allsektorite õigusraamistikud on seetõttu arenenud koordineerimata. Liidu tegevus on siiski saavutanud oma eesmärgi tagada finantsstabiilsus ja luua üks kogum ühtlustatud usaldatavusnõudeid ja turukäitumisnorme, mida kohaldatakse kogu ELis finantssektori ettevõtjate suhtes. Kuna tegurid, mis tingisid minevikus liidu õigusliku sekkumise, ei võimaldanud käsitleda spetsiifilistes või laiahaardelistes õigusnormides digitehnoloogia laialdast kasutamist rahanduses ja sellest tulenevaid riske, tundub otsene hindamine keeruline. Kaudset hindamist ja sellest tulenevaid seadusandlikke muudatusi on kajastatud igas käesoleva määruse osas.

- Konsulteerimine sidusrühmadega

Komisjon konsulteeris sidusrühmadega kogu käesoleva ettepaneku koostamise protsessi käigus, eelkõige

i) korraldas komisjon spetsiaalse avaliku konsultatsiooni (19. detsember 2019 – 19. märts 2020)[15];

ii) konsulteeris komisjon üldsusega esialgse mõjuhinnangu raames (19. detsember 2019–16. jaanuar 2020)[16];

iii) konsulteerisid komisjoni talitused kahel korral liikmesriikide ekspertidega panganduse, maksete ja kindlustuse eksperdirühma raames (18. mail 2020 ja 16. juulil 2020)[17];

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

iv) korraldasid komisjoni talitused 2020. aasta digitaalse finantsteabe ürituste sarja raames spetsiaalse veebiseminari digitaalse tegevuskerksuse kohta (19. mai 2020).

Avaliku konsultatsiooni eesmärk oli hankida komisjonile teavet ELi võimaliku valdkondadevahelise digitaalse tegevuskerksuse raamistiku väljatöötamiseks finantsteenuste valdkonnas. Vastustest nähtus laialdane toetus spetsiaalse raamistiku kehtestamisele ning meetmetele, mis keskenduvad neljale konsultatsioonis vaadeldud valdkonnale, kuid samal ajal rõhutati vajadust tagada proportsionaalsus ning käsitleda ja selgitada hoolikalt seost küberturvalisuse direktiivi horisontaalsete normidega. Komisjon sai esialgse mõjuhinnangu kohta kaks vastust, milles vastajad käsitlesid oma tegevusega seotud konkreetseid aspekte.

Liikmesriigid väljendasid 18. mail 2020 korraldatud panganduse, maksete ja kindlustuse eksperdirühma kohtumisel tugevat toetust finantssektori digitaalse tegevuskerksuse tugevdamisele meetmetega, mis on kavandatud kooskõlas komisjoni kirjeldatud nelja elemendiga. Liikmesriigid rõhutasid ka seda, et uued normid peavad olema selgelt seotud nii operatsiooniriski normidega (ELi finantsteenuseid käsitlevates õigusaktides) kui ka horisontaalsete normidega küberturvalisuse kohta (küberturvalisuse direktiiv). Teisel kohtumisel toonitasid mõned liikmesriigid, et vaja on tagada proportsionaalsus ja võtta arvesse väikeste ettevõtjate või suuremate gruppide tütarettevõtjate konkreetset olukorda ning anda järelevalvesse kaasatud riiklikele pädevatele asutustele tugevad volitused.

Ettepanekus tuginetakse ka tagasisidele, mis on saadud sidusrühmade ning ELi asutuste ja institutsioonidega toimunud kohtumistel, ning võetakse seda arvesse. Sidusrühmad, sealhulgas kolmandast isikust IKT-teenuste osutajad, on üldiselt väljendanud toetust. Saadud tagasiside analüüs näitab, et normide kavandamisel nõutakse proportsionaalsuse säilitamist ning põhimõtete- ja riskipõhise lähenemisviisi kasutamist. Institutsioonidest andsid oma panuse peamiselt Euroopa Süsteemsete Riskide Nõukogu (ESRN), Euroopa järelevalveasutused, Euroopa Liidu Küberturvalisuse Amet (ENISA) ja Euroopa Keskpank (EKP), samuti liikmesriikide pädevad asutused.

- Eksperdiarvamuste kogumine ja kasutamine

Käesoleva ettepaneku ettevalmistamisel tugines komisjon kvalitatiivsetele ja kvantitatiivsetele tõenditele, mis saadi tunnustatud allikatest, sealhulgas EBA ja ESMA kahest ühisest tehnilisest nõuandest. Neid täiendasid järelevalveasutuste, standardeid kehtestavate rahvusvaheliste asutuste ja juhtivate uurimisinstituutide konfidentsiaalne panus, avalikult kättesaadavad aruanded ning maailma finantssektori sidusrühmade kvantitatiivne ja kvalitatiivne panus.

- Mõju hindamine

Ettepanekule on lisatud mõjuhinnang,[18] mis esitati õiguskontrollikomiteele 29. aprillil 2020 ning kiideti heaks 29. mail 2020. Õiguskontrollikomitee soovitas mõnes valdkonnas parandusi, et i) anda rohkem teavet proportsionaalsuse tagamise viisi kohta; ii) näidata paremini seda, mil määral eelistatud variant erineb Euroopa järelevalveasutuste ühisest tehnilisest nõuandest ja miks see variant on optimaalne, ning iii) näidata täiendavalt, kuidas

[18] Komisjoni talituste töödokument – mõjuhinnang, mis on lisatud ettepanekule võtta vastu Euroopa Parlamendi ja nõukogu määrus, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014, 24.9.2020 (SWD(2020)198).

ettepanek on seotud kehtivate ELi õigusaktidega, sealhulgas praegu läbivaadatavate normidega. Mõjuhinnangut kohandati nimetatud punktide käsitlemiseks ja selles käsitleti ka õiguskontrollikomitee üksikasjalikumaid märkusi.

Komisjon kaalus digitaalse tegevuskerksuse raamistiku väljatöötamiseks mitut poliitikavarianti.

- „Ei tee midagi“ – tegevuskerksuse norme kehtestataks jätkuvalt olemasolevate, lahknevate sätetega ELi finantsteenuste kohta, osaliselt küberturvalisuse direktiiviga ja kehtivate või tulevaste riiklike kordadega.
- Variant 1 – suuremad kapitalipuhvrid: kehtestataks täiendavad kapitalipuhvrid, et suurendada finantssektori ettevõtjate võimet katta kahjum, mis võib tuleneda digitaalse tegevuskerksuse puudumisest.
- Variant 2 – finantsteenuste digitaalset tegevuskerksust käsitlev õigusakt: ELi tasandil võimaldataks laiahaardelist raamistikku ühtsete normidega, mis käsitlevad kõigi reguleeritud finantssektori ettevõtjate digitaalse tegevuskerksuse vajadusi ja loovad järelevalveraamistiku kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele.
- Variant 3 – finantsteenuste digitaalset tegevuskerksust käsitlev õigusakt koos tsentraliseeritud järelevalvega kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle: lisaks finantsteenuste digitaalset tegevuskerksust käsitleva õigusakti kehtestamisele (variant 2) loodaks uus asutus, mis teeks järelevalvet kolmandast isikust IKT-teenuste osutajate osutatavate teenuste üle.

Valiti variant 2, sest sellega saavutatakse enamik kavandatud eesmärkidest viisil, mis on tulemuslik, tõhus ja kooskõlas liidu muu poliitikaga. Ka suurem osa sidusrühmadest eelistab seda varianti.

Valitud variandiga kaasneks nii ühekordsete kui ka korduvate kulude kasv[19]. Ühekordsed kulud tulenevad peamiselt IT-süsteemidesse investeerimisest ja neid on seega keeruline kvantifitseerida, kuna ettevõtjate keerukas IT-keskkond ja eelkõige IT pärandsüsteemide seis on erinev. Suurte ettevõtjate puhul on need kulud siiski tõenäoliselt piiratud, kuna nad on juba teinud IKTsse olulisi investeeringuid. Ka väiksemate ettevõtjate kulud on eeldatavasti piiratud, sest nende väiksema riski tõttu kohaldataks proportsionaalseid meetmeid.

Valitud variandi majanduslik, sotsiaalne ja keskkonnamõju finantsteenuste sektoris tegutsevatele VKEdele oleks positiivne. Ettepanek annaks VKEdele selgust kohaldatavate normide koha, mis vähendab nõuete täitmisega seotud kulusid.

Valitud poliitikavariant avaldaks sotsiaalset mõju peamiselt tarbijatele ja investoritele. Kui ELi finantssüsteemi digitaalne tegevuskerksus oleks suurem, vähendaks see intsidentide arvu ja keskmisi kulusid. Suurem usaldus finantsteenuste sektori vastu oleks kasulik ühiskonnale tervikuna.

Mis puudutab keskkonnamõju, siis valitud poliitikavariant edendaks selliste viimase põlvkonna IKT-taristute ja -teenuste suuremat kasutamist, mis peaksid olema keskkonnasäästlikumad.

[19] Sama, lk 89–94.

- Õigusnormide toimivus ja lihtsustamine

Kui kaotataks IKTga seotud intsidentidest teatamise kattuvad nõuded, väheneks halduskoormus ja seonduvad kulud. Peale selle vähendab kulusid digitaalse tegevuskerksuse ühtlustatud testimine ja vastastikune tunnustamine ühtsel turul, seda eelkõige piiriüleste ettevõtjate jaoks, kellel võib muidu olla vaja teha liikmesriikides mitmeid teste[20].

- Põhiõigused

EL on pühendunud põhiõiguste kaitse kõrge taseme tagamisele. Kõik finantssektori ettevõtjate vahelised vabatahtlikud teabejagamise kokkulepped, mida käesoleva määrusega edendatakse, oleksid sellised, et teavet jagataks usaldusväärses keskkonnas, järgides täielikult liidu andmekaitsenorme, täpsemalt Euroopa Parlamendi ja nõukogu määrust (EL) 2016/679,[21] eelkõige olukorras, kus isikuandmete töötlemine on vajalik vastutava töötleja õigustatud huvi korral.

4. MÕJU EELARVELE

Mis puudutab mõju eelarvele, siis käesoleva määrusega nähakse ette Euroopa järelevalveasutuste suurem roll, andes neile volitused teha kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle piisavat järelevalvet, mistõttu kaasneks ettepanekuga suuremate ressursside eraldamine, eelkõige järelevalvemissioonide (nagu kohapealsed ja internetipõhised kontrollid ja auditid) tegemiseks, ja IKT turvalisuse valdkonnas spetsiifiliste eksperditeadmistega töötajate kasutamine.

Kõnealuste kulude maht ja jaotus sõltub uute järelevalvevolituste ulatusest ja Euroopa järelevalveasutuste (täpsetest) ülesannetest. Mis puudutab uusi inimressursse, siis EBA, ESMA ja EIOPA vajavad pärast ettepaneku sätete kohaldamise algust kokku 18 täistööajaga töötajat – iga asutus 6 täistööajaga töötajat (hinnanguliselt 15,71 miljonit eurot aastatel 2022–2027). Euroopa järelevalveasutustele tekivad ka täiendavad IT-kulud, lähetuskulud seoses kohapealsete kontrollidega ja tõlkekulud (hinnanguliselt 12 miljonit eurot aastatel 2022–2027), samuti muud halduskulud (hinnanguliselt 2,48 miljonit eurot aastatel 2022–2027). Kogukulud on aastatel 2022–2027 hinnangute järgi seega ligikaudu 30,19 miljonit eurot.

Tuleb märkida, et kuigi otseseks järelevalveks vajalike töötajate arv (nt uued töötajaid ja muud uute ülesannetega seotud kulud) sõltub aja jooksul järelevalvatavate kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate hulga ja suuruse muutumisest, rahastatakse asjaomaseid kulusid täielikult kõnealuste turuosaliste makstavatest tasudest. Järelikult ei ole nähtud ette mõju ELi eelarveassigneeringutele (v.a lisatöötajad), sest kõnealused kulud kaetakse täielikult tasudest saadavate vahenditega.

Käesoleva ettepaneku finantsmõju ja mõju eelarvele on üksikasjalikult selgitatud ettepanekule lisatud finantsselgituses.

---

[20] Sama.

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

5. MUU TEAVE

- Rakenduskavad ning järelevalve, hindamise ja aruandluse kord

Ettepanek sisaldab üldist kava konkreetsetele eesmärkidele avalduva mõju jälgimiseks ja hindamiseks, mistõttu peab komisjon vähemalt kolm aastat pärast jõustumist vaatama määruse läbi ja esitama Euroopa Parlamendile ja nõukogule oma peamised järeldused.

Läbivaatamine peab toimuma kooskõlas komisjoni parema õigusloome suunistega.

- Ettepaneku sätete üksikasjalik selgitus

Ettepanekus keskendutakse mitmele peamisele poliitikavaldkonnale, mis kujutavad endast omavahel seotud põhisambaid, mis on konsensuse alusel lisatud Euroopa ja rahvusvahelistesse suunistesse ja parimatesse tavadesse, mille eesmärk on parandada finantssektori küber- ja tegevuskerksust.

Määruse kohaldamisala ja vajalike meetmete proportsionaalsus (artikkel 2)

Selleks et tagada finantssektori suhtes kohaldatavate IKT-riskide juhtimise nõuete ühtsus, käsitletakse määruses mitmesuguseid liidu tasandil reguleeritud finantssektori ettevõtjaid, täpsemalt krediidiasutusi, makseasutusi, e-raha asutusi, investeerimisühinguid, krüptovarateenuse osutajaid, väärtpaberite keskdepositooriume, keskseid vastaspooli, kauplemiskohti, kauplemisteabehoidlaid, alternatiivsete investeerimisfondide valitsejaid ja fondivalitsejaid, aruandlusteenuste pakkujaid, kindlustus- ja edasikindlustusandjaid, kindlustusvahendajaid, edasikindlustusvahendajaid ja kõrvaltegevusena pakutava kindlustuse vahendajaid, tööandja kogumispensioni asutusi, reitinguagentuure, vannutatud audiitoreid ja audiitorühinguid, kriitilise tähtsusega võrdlusaluste haldureid ja ühisrahastamisteenuse osutajaid.

Selline kohaldamisala hõlbustab kõigi riskijuhtimiskomponentide ühetaolist ja sidusat kohaldamist IKTga seotud valdkondades, tagades samal ajal finantssektori ettevõtjatele IKT-riskidega seotud õiguslike kohustuste puhul võrdsed tingimused. Samal ajal tunnistatakse määruses, et finantssektori ettevõtjad on suuruse, äriprofiili või digiriskile avatuse poolest väga erinevad. Kuna suurematel finantssektori ettevõtjatel on rohkem ressursse, on näiteks ainult sellised ettevõtjad, mida ei liigitata mikroettevõtjateks, kohustatud kehtestama keerulise juhtimiskorra, looma spetsiaalsed juhtimisfunktsioonid, tegema pärast olulisi võrgu- ja infosüsteemide taristu muudatusi põhjalikke hindamisi, tegema korrapäraselt riskianalüüse IKT pärandsüsteemide kohta ning laiendama talitluspidevuse ning reageerimis- ja taastekavade testimist, et hõlmata esmase IKT-taristu ja varurajatiste puhul ümberlülitusstsenaariume. Peale selle peavad ainult need finantssektori ettevõtjad, mida käsitatakse digitaalse kerksuse süvatestimisel olulisena, tegema ohuteabel põhinevad läbistustestid.

Laiast kohaldamisalast hoolimata ei ole see ammendav. Täpsemalt ei hõlma käesolev määrus direktiivi 98/26/EÜ (arvelduse lõplikkuse kohta makse- ja väärtpaberiarveldussüsteemides)[22] artikli 2 punktis p määratletud süsteemikorraldajaid ega ühtki süsteemis osalejat, välja arvatud juhul, kui osaleja on ise liidu tasandil reguleeritud finantssektori ettevõtja ja seega käesoleva määrusega hõlmatud (st krediidiasutus, investeerimisühing, keskne vastaspool).

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

Kohaldamisalast jääb välja ka liidu saastekvootide register, mille haldamine toimub kooskõlas direktiiviga 2003/87/EÜ[23] komisjoni egiidi all.

Sellised väljajätud arvelduse lõplikkuse direktiivi kohaldamisalast võtavad arvesse vajadust vaadata täiendavalt läbi arvelduse lõplikkuse direktiivi kohaseid süsteemikorraldajaid ja süsteemis osalejaid puudutavad õiguslikud ja poliitilised küsimused, arvestades samal ajal nõuetekohaselt praegu keskpankade hallatavate maksesüsteemide[24] suhtes kohaldatavate raamistike mõju. Kuna need küsimused võivad hõlmata aspekte, mis ei ole seotud käesolevas määruses käsitletud probleemidega, jätkab komisjon selle hindamist, kas määruse kohaldamisala on vaja edaspidi laiendada ettevõtjatele ja IKT-taristutele, mis praegu sinna ei kuulu, ning milline oleks selle mõju.

Juhtimisega seotud nõuded (artikkel 4)

Käesoleva määruse eesmärk on viia finantssektori ettevõtjate äristrateegiad ja IKT-riskide juhtimine rohkem kooskõlla. Selleks peab juhtorgan mängima otsustavat ja aktiivset rolli IKT-riskide juhtimise raamistiku suunamisel ja edendama ranget küberhügieeni. Üldpõhimõte on see, et finantssektori ettevõtja IKT-riskide juhtimise eest vastutab täielikult juhtorgan, ja seda tuleb kajastada konkreetsetes nõuetes, nagu kõigi IKTga seotud funktsioonide puhul selgete rollide ja vastutusvaldkondade määramine, pidev osalemine IKT-riskide juhtimise järelevalve kontrollis ning kõigis heakskiitmis- ja kontrolliprotsessides ning IKT valdkonna investeeringute ja koolituste asjakohane jaotamine.

IKT-riskide juhtimise nõuded (artiklid 5–14)

Digitaalne tegevuskerksus põhineb kooskõlas Euroopa järelevalveasutuste tehnilise nõuandega hulgal olulistel põhimõtetel ja nõuetel, mis käsitlevad IKT-riskide juhtimise raamistikku. Kõnelused nõuded, mis lähtuvad asjakohastest rahvusvahelistest, riiklikest ja sektori kehtestatud standarditest, suunistest ja soovitustest, keskenduvad IKT-riskide juhtimise spetsiifilistele funktsioonidele (kindlaksmääramine, kaitsmine ja ennetamine, avastamine, reageerimine ja taastamine, õppimine ja arenemine ning kommunikatsioon). Selleks et kiiresti muutuva küberohtude maastikuga sammu pidada, peavad finantssektori ettevõtjad looma ja säilitama kerksed IKT-süsteemid ja -vahendid, mis minimeerivad IKT-riskide mõju, tegema jooksvalt kindlaks kõik IKT-riski allikad, kehtestama kaitse- ja ennetusmeetmed, avastama kiiresti anomaalse tegevuse, kehtestama spetsiifilise ja laiahaardelise talitluspidevuse poliitika ning katastroofi- ja taastamiskavad, mis on operatiivse talitluspidevuse poliitika lahutamatuks osaks. Viimasena nimetatud komponente on vaja selleks, et pärast IKTga seotud intsidente, eelkõige küberründe id, kiiresti taastuda, piirates kahju ja prioriseerides tegevuse ohutut jätkamist. Käesolev määrus ei näe ette konkreetset standardimist, vaid pigem lähtub Euroopa ja rahvusvaheliselt tunnustatud tehnilistest standarditest või sektori parimatest tavadest, kui need on täielikult kooskõlas järelevalvejuhistega selliste rahvusvaheliste standardite kasutamise ja inkorporeerimise kohta. Käesolevas määruses käsitletakse seoses finantssektori ettevõtja tegevuse digijäljega ka selliste füüsiliste taristute ja rajatiste terviklikkust, ohutust ja vastupidavust, mis toetavad tehnoloogia kasutamist ning asjaomaseid IKTga seotud protsesse ja inimesi.

---

[23] Euroopa Parlamendi ja nõukogu 13. oktoobri 2003. aasta direktiiv 2003/87/EÜ, millega luuakse ühenduses kasvuhoonegaaside saastekvootidega kauplemise süsteem ja muudetakse nõukogu direktiivi 96/61/EÜ (ELT L 275, 25.10.2003, lk 32).

[24] Eelkõige Euroopa Keskpanga 3. juuli 2014. aasta määrus (EL) nr 795/2014 süsteemselt oluliste maksesüsteemide järelevaatamise kohta.

IKTga seotud intsidentidest teatamine (artiklid 15–20)

IKTga seotud intsidentidest teatamise ühtlustamine ja lihtsustamine saavutatakse esiteks tänu finantssektori ettevõtjatele kehtestatavale üldisele nõudele luua ja rakendada juhtimisprotsess IKTga seotud intsidentide jälgimiseks ja logimiseks ning seejärel liigitada nad kriteeriumide põhjal, mis on kindlaks määratud määruses ja mida Euroopa järelevalveasutused on edasi arendanud olulisuse lävede kindlaksmääramise volituste raames. Teiseks tuleb pädevatele asutustele teatada ainult IKTga seotud intsidentidest, mida peetakse oluliseks. Teatamisel tuleks kasutada ühtset vormi ja menetlust, mille on välja töötanud Euroopa järelevalveasutused. Finantssektori ettevõtjad peaksid esitama esialgse, vahe- ja lõpparuande ning teavitama kasutajaid ja kliente, kui intsident mõjutab või võib mõjutada nende finantshuve. Pädevad asutused peaksid edastama intsidentide asjakohased üksikasjad teistele institutsioonidele või asutusele: Euroopa järelevalveasutustele, EKP-le ja direktiivi (EL) 2016/1148 alusel määratud ühtsetele kontaktpunktidele.

Selleks et algatada finantssektori ettevõtjate ja pädevate asutuste vaheline dialoog, mis aitaks mõju minimeerida ja teha kindlaks sobivad parandusmeetmed, tuleks IKTga seotud olulistest intsidentidest teatamist täiendada järelevalvealase tagasiside ja suunistega.

Lisaks tuleks liidu tasandil IKTga seotud intsidentidest teatamise tsentraliseerimise võimalust põhjalikumalt uurida Euroopa järelevalveasutuste, EKP ja ENISA ühisaruandes, milles hinnatakse seda, kas finantssektori ettevõtjate poolse IKTga seotud olulistest intsidentidest teatamise puhul oleks võimalik luua üks ELi keskus.

Digitaalse tegevuskerksuse testimine (artiklid 21–24)

IKT-riskide juhtimise raamistikus sisalduvaid võimeid ja funktsioone tuleks perioodiliselt testida, et teha kindlaks valmisolek ning avastada nõrkused, puudujäägid või lüngad ning rakendada kiiresti parandusmeetmed. Käesoleva määrusega on lubatud kohaldada digitaalse tegevuskerksuse testimise nõudeid proportsionaalselt, lähtudes finantssektori ettevõtjate suurusest ning äri- ja riskiprofiilist: kõik ettevõtjad peaksid testima IKT-vahendeid ja -süsteeme, kuid ainult need, mida pädevad asutused (lähtudes kriteeriumidest, mis on sätestatud käesolevas määruses ja mida Euroopa järelevalveasutused on edasi arendanud) käsitavad oluliste ja küberküpsetena, peaksid olema kohustatud tegema ohuteabel põhinevatel läbistustestidel põhinevat süvatestimist. Lisaks on käesolevas määruses sätestatud nõuded testijatele ja ohuteabel põhinevate läbistustestide tulemuste tunnustamine kogu liidus, kui finantssektori ettevõtjad tegutsevad mitmes liikmeriigis.

Kolmandast isikust tulenev IKT-risk (artiklid 25–39)

Määruse eesmärk on tagada kolmandast isikust tuleneva IKT-riski usaldusväärne jälgimine. Seda eesmärki aitab esiteks saavutada see, kui järgitakse põhimõtetel põhinevaid norme, mida kohaldatakse, kui finantssektori ettevõtjad jälgivad kolmandast isikust IKT-teenuste osutajatest tulenevat riski. Teiseks ühtlustatakse selle määrusega teenuse ja kolmandast isikust IKT-teenuste osutajatega olemasoleva suhte peamisi elemente. Need elemendid hõlmavad minimaalseid aspekte, mida peetakse äärmiselt oluliseks, et finantssektori ettevõtja saaks täielikult jälgida kolmandast isikust tulenevat IKT-riski lepingu sõlmimise, täitmise ja lõpetamise ning lepingujärgses etapis.

Eelkõige peavad suhet reguleerivad lepingud sisaldama teenuste täielikku kirjeldust, andmete töötlemise kohti, täielikke teenustaseme kirjeldusi, millele on lisatud kvantitatiivsed ja kvalitatiivsed tulemuseesmärgid, sätteid isikuandmetele ligipääsu, nende kättesaadavuse, tervikluse, turvalisuse ja kaitse kohta, garantiisid juurdepääsu, taastamise ja tagastamise kohta kolmandast isikust IKT-teenuste osutajate maksejõuetuse korral, kolmandast isikust IKT-teenuste osutajate etteteatamistähtaegu ja aruandekohustusi, finantssektori ettevõtja või

määratud kolmanda isiku pääsu-, kontrolli- ja auditeerimisõigusi, selgeid lõpetamisõigusi ja spetsiaalseid väljumisstrateegiaid. Kuna mõningaid nendest lepingulistest elementidest on võimalik standardida, edendatakse määrusega selliste lepingu tüüptingimuste vabatahtlikku kasutamist, mille komisjon töötas välja pilvandmetöötlusteenuse kasutamise jaoks.

Lisaks soovitakse määrusega edendada finantssektoris kolmandast isikust tulenevat IKT-riski käsitlevate järelevalvealaste lähenemisviiside ühtlustamist, kohaldades kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes liidu järelevalveraamistikku. Uue ühtlustatud õigusraamistiku kaudu saab Euroopa järelevalveasutus, mis on määratud iga kõnealuse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja juhtivaks järelevalveasutuseks, õiguse tagada, et selliste tehnoloogiateenuse osutajate üle, mis mängivad finantssektori toimimises kriitilist rolli, tehakse üleeuroopaliselt piisavat järelevalvet. Käesoleva määruse kohane järelevalveraamistik toetub finantsteenuste valdkonnas olemasolevale institutsioonilisele ülesehitusele, mis tähendab, et Euroopa järelevalveasutuste ühiskomitee tagab valdkondadevahelise koordineerimise kõigis IKT-riskiga seotud küsimustes kooskõlas oma küberturvalisust puudutavate ülesannetega ja teda toetab asjaomane allkomitee (järelevalvefoorum), mis valmistab ette kriitilise tähtsusega kolmandatest isikutest teenuseosutajatele suunatud individuaalseid otsuseid ja ühissoovitusi.

Teabe jagamine (artikkel 40)

Selleks et suurendada teadlikkust IKT-riskist, minimeerida selle levikut ning toetada finantssektori ettevõtjate kaitsevõimet ja ohtude avastamise meetodeid, võimaldab määrus finantssektori ettevõtjatel sõlmida kokkuleppeid küberohte puudutava teabe ja küberohuteadmuse omavaheliseks jagamiseks.

2020/0266 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS,

mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu riikide parlamentidele,

võttes arvesse Euroopa Keskpanga arvamust[25],

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[26],

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Info- ja kommunikatsioonitehnoloogia (IKT) toetab digiajastul keerukaid süsteeme, mida kasutatakse igapäevases ühiskondlikus tegevuses. See tagab majanduse toimimise sellistes olulistes sektorites nagu rahandus ja parandab ühtse turu toimimist. Suurem digiteerimine ja omavaheline seotus võimendavad ka IKT-riske, mis muudab ühiskonna tervikuna ja eelkõige finantssüsteemi küberohtude või IKT-katkestuste suhtes haavatavamaks. IKT-süsteemide lai kasutus ning ulatuslik digiteerimine ja ühendatus on tänapäeval liidu finantssektori ettevõtjate kõigi tegevusvaldkondade põhijooned, kuid nende tegevusraamistikud ei hõlma veel piisavalt digitaalset kerksust.

(2) Viimastel aastakümnetel on IKT kasutamine omandanud rahanduses otsustava tähtsusega rolli ning on tänapäeval kõigi finantssektori ettevõtjate tüüpiliste igapäevaste funktsioonide toimimise jaoks kriitilise tähtsusega. Digiteerimine hõlmab näiteks makseid (mille puhul kasutatakse sularaha ja paberipõhiste meetodite asemel üha rohkem digilahendusi), väärtpaberite kliirimist ja arveldamist, elektroonilist ja algoritmkauplemist, laenuandmis- ja rahastamistehinguid, vastastikust rahastamist, krediidireitinguid, kindlustuslepingute sõlmimist, kahjukäsitlust ja *back office*'i tegevust. Kogu finantssektor on muutunud valdavalt digitaalseks, kuid digiteerimine on süvendanud ka seoseid ja sõltuvust nii finantssektori sees kui ka finantssektori ja kolmandate isikute taristu ja kolmandast isikust teenuseosutajate vahel.

(3) Euroopa Süsteemsete Riskide Nõukogu (ESRN) on kinnitanud süsteemset küberriski käsitlevas 2020. aasta aruandes,[27] kuidas finantssektori ettevõtjate, finantsturgude ja

[25] [*lisada viide*] ELT C , , lk .
[26] [*lisada viide*] ELT C , , lk .

finantsturutaristu suur omavaheline seotus ning eelkõige nende IKT-süsteemide omavaheline sõltuvus võivad kujutada endast süsteemset haavatavust, sest lokaalsed küberintsidendid võivad kanduda kiiresti liidu ühest ligikaudu 22 000 finantssektori ettevõtjast[28] üle kogu finantssüsteemile, olenemata geograafilistest piiridest. Rahanduses toimuvad tõsised IKTga seotud rikkumised ei mõjuta ainult üksikuid finantssektori ettevõtjaid. Nad soodustavad ka lokaalsete haavatavuste levimist finantsülekannete kanalite kaudu ja võivad avaldada negatiivset mõju liidu finantssüsteemi stabiilsusele, põhjustades likviidsuse väljavoolu ning üldiselt vähendades kindlustunnet ja usaldust finantsturgude vastu.

(4) IKT-riskidele on viimastel aastatel pööranud tähelepanu riiklikud, Euroopa ja rahvusvahelised poliitikakujundajad, reguleerivad asutused ja standardeid kehtestavad asutused eesmärgiga püüda suurendada vastupidavust, kehtestada standardeid ja koordineerida regulatiivset või järelevalvetööd. Rahvusvahelisel tasandil püüavad Baseli pangajärelevalve komitee, makse- ja arveldussüsteemide komitee, finantsstabiilsuse nõukogu, finantsstabiilsuse instituut ning G7sse ja G20sse kuuluvate riikide rühmad anda eri jurisdiktsioonide pädevatele asutustele ja turukorraldajatele vahendeid oma finantssüsteemi kerksuse suurendamiseks.

(5) Hoolimata sihipärasest riiklikust ja Euroopa poliitikast ja seadusandlikest algatustest on IKT-riskid jätkuvalt probleem liidu finantssüsteemi tegevuskerksuse, suutlikkuse ja stabiilsuse jaoks. 2008. aasta finantskriisile järgnenud reformiga tugevdati peamiselt liidu finantssektori finantsvastupidavust ja sooviti kaitsta liidu konkurentsivõimet ja stabiilsust majanduslikust, usaldatavusnõuete ja turukäitumise seisukohast. Kuigi IKT turvalisus ja digitaalne kerksus on operatsiooniriski osa, on kriisijärgses regulatiivses tegevuskavas nendele vähem keskendutud ning neid on arendatud ainult mõnes liidu finantsteenuste poliitika ja regulatiivse maastiku osas või ainult üksikutes liikmesriikides.

(6) Komisjoni 2018. aasta finantstehnoloogia tegevuskavas[29] rõhutati, et väga oluline on muuta liidu finantssektor vastupidavamaks ka tegevuslikust vaatenurgast, et tagada selle tehnoloogiline ohutus ja hea toimimine ning kiire taastumine IKTga seotud rikkumistest ja intsidentidest, võimaldades kokkuvõttes osutada finantsteenuseid tulemuslikult ja sujuvalt kogu liidus ning ka pingelistes olukordades, kaitstes samal ajal tarbijate ja turu usaldust ja kindlustunnet.

(7) 2019. aprillis esitasid Euroopa Pangandusjärelevalve (EBA), Euroopa Väärtpaberiturujärelevalve (ESMA) ja Euroopa Kindlustus- ja Tööandjapensionide Järelevalve (EIOPA) (koos „Euroopa järelevalveasutused“) ühiselt kaks tehnilist nõuannet, milles kutsuti üles kasutama rahanduse valdkonnas IKT-riski puhul ühtset

---

27 ESRNi aruanne süsteemse küberriski kohta, veebruar 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Euroopa järelevalveasutuste läbivaatamist käsitlevale ettepanekule lisatud mõjuhinnangu (SWD(2017) 308) kohaselt on ligikaudu 5 665 krediidiasutust, 5 934 investeerimisühingut, 2 666 kindlustusandjat, 1 573 tööandja kogumispensioni asutust, 2 500 fondivalitsejat, 350 turutaristut (nagu kesksed vastaspooled, börsid, kliendi korralduste süsteemsed täitjad, kauplemisteabehoidlad ja mitmepoolsed kauplemissüsteemid), 45 reitinguagentuuri ja 2 500 tegevusloaga makseasutust ja e-raha asutust. Üksusi on seega kokku ligikaudu 21 233 ja see arv ei hõlma ühisrahastamisüksusi, vannutatud audiitoreid ega audiitorühinguid, krüptovarateenuse osutajaid ega võrdlusaluste haldureid.

29 Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Keskpangale, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Finantstehnoloogia tegevuskava: konkurentsivõimelisema ja innovatiivsema Euroopa finantssektori poole“ (COM(2018) 109 final), https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

lähenemisviisi ja soovitati proportsionaalselt tugevdada finantsteenuste sektori digitaalset tegevuskerksust liidu sektoripõhise algatuse kaudu.

(8) Liidu finantssektorit reguleerib ühtlustatud ühtne reeglistik ja juhib Euroopa Finantsjärelevalve Süsteem. Sätteid digitaalse tegevuskerksuse ja IKT turvalisuse kohta ei ole aga veel täielikult või järjepidevalt ühtlustatud, kuigi digitaalne tegevuskerksus on digiajastul finantsstabiilsuse ja turu usaldusväärsuse tagamiseks eluliselt tähtis ja mitte vähem oluline kui näiteks usaldatavus- või turukäitumisstandardid. Seepärast peaks ühtse reeglistiku ja järelevalvesüsteemiga hõlmama ka selle komponendi, laiendades selliste finantsjärelevalveasutuste volitusi, mis tegelevad finantsstabiilsuse ja turu usaldusväärsuse jälgimise ja kaitsmisega.

(9) Õigusnormide erinevused ja ebaühtlane regulatiivne või järelevalvealane lähenemine IKT-riskile tekitab finantsteenuste ühtsel turul takistusi ning pärsib asutamisvabaduse sujuvat kasutamist ja piiriüleselt tegutsevate finantssektori ettevõtjate teenuste osutamist. Moonutatud võib olla ka eri liikmesriikides tegutsevate sama tüüpi finantssektori ettevõtjate vaheline konkurents. Valdkondades, kus liidu tasandil ühtlustamine on olnud väga piiratud (digitaalse tegevuskerksuse testimine) või kus ühtlustamist ei ole toimunud (kolmandast isikust tuleneva IKT-riski jälgimine), võivad erinevused, mis tulenevad riiklikul tasandil kavandatud arendustest, tekitada uusi ühtse turu toimimist takistavaid tõkkeid ning kahjustada turuosalisi ja finantsstabiilsust.

(10) IKT-riski puudutavate sätete osaline käsitlemine liidu tasandil näitab, et olulistes valdkondades, nagu IKTga seotud intsidentidest teatamine ja digitaalne tegevuskerksus, on lüngad või kattuvus ning tekitab lisanduvate lahknevate riiklike normide või kattuvate normide mittekulutõhusa kohaldamise tõttu ebaühtlust. See on eriti kahjulik sellisele IKT-mahukale sektorile nagu rahandus, sest tehnoloogiariskid ei tunne piire ja finantssektor osutab oma teenuseid piiriüleselt, nii liidu sees kui ka väljaspool.

Piiriüleselt tegutsevatel või mitme tegevusloaga (ühel finantssektori ettevõtjal võib näiteks olla pangandus-, investeerimisühingu ja makseasutuse litsents, millest igaühe on välja andnud erinev pädev asutus ühes või mitmes liikmesriigis) üksikutel finantssektori ettevõtjatel on operatiivselt keeruline ise järjepidevalt ja kulutõhusalt IKT-riske käsitleda ja IKT-intsidentide negatiivset mõju leevendada.

(11) Kuna ühtse reeglistikuga ei ole kaasnenud laiahaardelist IKT- või operatsiooniriskide raamistikku, tuleb kõigi finantssektori ettevõtjate digitaalse tegevuskerksuse põhinõudeid rohkem ühtlustada. Suutlikkus ja üldine kerksus, mida finantssektori ettevõtjad nendele põhinõuetele tuginedes tegevuse katkestustega toimetulekuks arendaksid, aitaksid säilitada liidu finantsturgude stabiilsust ja usaldusväärsust ning seega tagada liidus investorite ja tarbijate kaitse kõrge taseme. Kuna käesoleva määruse eesmärk on edendada ühtse turu sujuvat toimimist, peaks see tuginema ELi toimimise lepingu artikli 114 sätetele, nagu neid tõlgendab Euroopa Liidu Kohus oma väljakujunenud kohtupraktikas.

(12) Käesoleva määrusega soovitakse esiteks koondada kokku ja ajakohastada IKT-riskidega seotud nõuded, mida seni on käsitletud eraldi eri määrustes ja direktiivides. Kuigi liidu nendes õigusaktides käsitleti finantsriski peamisi kategooriaid (nt krediidirisk, tururisk, vastaspoole krediidirisk ja likviidsusrisk, turukäitumise risk), ei saanud neis nende vastuvõtmise ajal käsitleda põhjalikult kõiki tegevuskerksuse komponente. Kui kõnealustes liidu õigusaktides käsitleti operatsiooniriski nõudeid põhjalikumalt, keskenduti sageli traditsioonilisele kvantitatiivsele riske käsitlevale lähenemisviisile (kehtestades IKT-riskide hõlmamiseks kapitalinõuded), mitte ei

sätestatud sihipäraseid kvalitatiivseid nõudeid, et edendada suutlikkust nõuetega, mis keskenduvad IKTga seotud intsidente puhul kaitsmise, avastamise, piiramise, taastamise ja parandamise suutlikkusele, või teatamise ja digitaalse testimise suutlikkuse loomisega. Nendes direktiivides ja määrustes sooviti peamiselt käsitleda põhinorme usaldatavusnõuete täitmise järelevalve, turu usaldusväärsuse või turukäitumise kohta.

IKT-riski käsitlevate õigusnormide koondamise ja ajakohastamise tulemusel koondatakse kõik sätted rahanduse digiriski kohta esimest korda ühtselt ühte õigusakti. Käesolev algatus peaks seega kõrvaldama mõningate kõnealuste õigusaktide lüngad või ebaühtsuse, muu hulgas neis kasutatud terminoloogia osas, ning selles tuleks osutada sõnaselgelt IKT-riskile, kehtestades sihipärased normid IKT-riskide juhtimise suutlikkuse, aruandlus ja testimise kohta ning kolmandast isikust tuleneva riski jälgimise kohta.

(13) Finantssektori ettevõtjad peaksid kasutama IKT-riski käsitlemisel sama lähenemisviisi ja samu põhimõtetel põhinevaid norme. Ühtsus aitab suurendada usaldust finantssüsteemi vastu ja säilitada selle stabiilsust, eelkõige IKT-süsteemide, -platvormide ja -taristu liigkasutamise ajal, millega kaasneb suurem digirisk.

Lisaks peaks esmane küberhügieen minimeerima IKT-katkestuste mõju ja kulu ning hoidma seega ära majandusele suurte kulude tekkimise.

(14) Määruse kasutamine aitab vähendada regulatiivset keerukust, edendab järelevalvealast ühtsust ja suurendab õiguskindlust, aidates samal ajal piirata nõuete täitmisega seotud kulusid, eelkõige piiriüleselt tegutsevate finantssektori ettevõtjate puhul, ning vähendada konkurentsimoonutusi. Seepärast tundub otsus kehtestada finantssektori ettevõtjate digitaalse tegevuskerksuse ühtne raamistik määrusega olevat kõige asjakohasem viis tagada, et liidu finantssektorid kohaldavad kõiki IKT-riskide juhtimise raamistiku komponente ühetaoliselt ja sidusalt.

(15) Praegu hõlmab küberturvalisuse üldine raamistik lisaks finantsteenuseid käsitlevatele õigusnormidele Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148[30]. Direktiivi kohaldatakse seitsme kriitilise sektori ja kolme liiki finantssektori ettevõtjate – krediidiasutused, kauplemiskohad ja kesksed vastaspooled – suhtes. Kuna direktiivis (EL) 2016/1148 on sätestatud mehhanism oluliste teenuste operaatorite identifitseerimiseks riiklikul tasandil, hõlmab selle kohaldamisala tegelikkuses ainult teatavaid liikmesriikide kindlaks määratud krediidiasutusi, kauplemiskohti ja keskseid vastaspooli ja ainult nemad on seega kohustatud täitma selles direktiivis sätestatud IKT turvalisuse ja intsidentidest teatamise nõudeid.

(16) Kuna käesoleva määrusega tõstetakse digitaalse kerksuse komponentide ühtlustamise taset, kehtestades IKT-riskide juhtimise ja IKTga seotud intsidentidest teatamise suhtes nõuded, mis on kehtivates finantsteenuseid käsitlevates liidu õigusaktides sätestatust rangemad, on tegemist suurema ühtlustamisega ka võrreldes direktiivis (EL) 2016/1148 sätestatud nõuetega. Sellest tulenevalt on käesolev määrus direktiivi (EL) 2016/1148 suhtes *lex specialis*.

On äärmiselt oluline tagada, et finantssektor ja liidu horisontaalne küberturvalisuse raamistik oleksid tugevalt seotud, sest see tagaks kooskõla liikmesriikides juba vastu

[30] Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

võetud küberturvalisuse strateegiatega ning võimaldaks teavitada finantsjärelevalveasutusi küberintsidentidest, mis mõjutavad teisi direktiiviga (EL) 2016/1148 hõlmatud sektoreid.

(17) Selleks et võimaldada sektoritevahelist õppimisprotsessi ja võtta tulemuslikult arvesse muude sektorite kogemusi küberohtudega tegelemisel, peaksid direktiivis (EL) 2016/1148 osutatud finantssektori ettevõtjad jääma selle direktiivi ökosüsteemi (nt võrgu- ja infoturbe koostöörühm ning küberturbe intsidentide lahendamise üksused).

Euroopa järelevalveasutused ja riiklikud pädevad asutused peaksid saama osaleda vastavalt strateegilise poliitika aruteludes ning võrgu- ja infoturbe koostöörühma tehnilises töös, vahetada teavet ja teha täiendavat koostööd direktiivi (EL) 2016/1148 alusel määratud ühtsete kontaktpunktidega. Käesoleva määruse kohaselt peaksid pädevad asutused konsulteerima ja tegema koostööd ka kooskõlas direktiivi (EL) 2016/1148 artikliga 9 määratud riiklike küberturbe intsidentide lahendamise üksustega.

(18) Samuti on oluline tagada kooskõla Euroopa elutähtsate infrastruktuuride direktiiviga, mida vaadatakse praegu läbi, et suurendada elutähtsate infrastruktuuride kaitset ja vastupidavust muude kui küberohtude suhtes, ja mis võib mõjutada finantssektorit[31].

(19) Pilvandmetöötlusteenuse pakkujad on üks direktiiviga (EL) 2016/1148 hõlmatud digitaalse teenuse osutajate kategooria. Seetõttu teevad nende üle järelkontrolli kooskõlas nimetatud direktiiviga määratud riiklikud asutused ning järelevalve piirdub selles õigusaktis sätestatud IKT turvalisuse ja intsidentidest teatamise nõuetega. Kuna käesoleva määrusega loodud järelevalveraamistikku kohaldatakse kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste, sealhulgas pilvandmetöötlusteenuse osutajate suhtes, kui nad osutavad IKT-teenuseid finantssektori ettevõtjatele, tuleks seda pidada direktiivi (EL) 2016/1148 kohase järelevalve täienduseks. Käeoleva määrusega loodud järelevalveraamistik peaks hõlmama pilvandmetöötlusteenuse osutajaid, kui ei ole olemas liidu horisontaalset mittesektoripõhist raamistikku, millega oleks loodud digitaalse järelevalve asutus.

(20) Selleks et omada täielikku kontrolli IKT-riskide üle, peab finantssektori ettevõtjatel olema laiahaardeline suutlikkus, mis võimaldab tugevat ja tulemuslikku IKT-riskide juhtimist, koos erimehhanismide ja -poliitikaga IKTga seotud intsidentidest teatamiseks, IKT-süsteemide, -kontrollide ja -protsesside testimiseks ning kolmandast isikust tulenevate IKT-riskide juhtimiseks. Finantssüsteemi digitaalse tegevuskerksuse mõõdupuud tuleks tõsta, võimaldades samal ajal finantssektori ettevõtjatel, mis ei ole komisjoni soovituses 2003/361/EÜ[32] määratletud mikroettevõtjad, kohaldada nõudeid proportsionaalselt.

(21) IKTga seotud intsidentidest teatamise läved ja taksonoomia on riiklikul tasandil väga erinevad. Kuigi Euroopa Liidu Küberturvalisuse Ameti (ENISA)[33] ja direktiivi (EL)

---

31 Nõukogu 8. detsembri 2008. aasta direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta (ELT L 345, 23.12.2008, lk 75).

32 Komisjoni 6. mai 2003. aasta soovitus mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta (ELT L 124, 20.5.2003, lk 36).

33 ENISA, „Reference Incident Classification Taxonomy“, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

2016/1148 kohase finantssektori ettevõtjate võrgu- ja infoturbe koostöörühma tehtava töö kaudu võib jõuda üksmeelele, esineb lävede ja taksonoomia valdkonnas jätkuvalt lahknevaid lähenemisviise või need võivad ülejäänud finantssektori ettevõtjate puhul tekkida. Sellega kaasnevad mitmed nõuded, mida finantssektori ettevõtjad peavad täitma, eelkõige tegutsedes liidus mitmes jurisdisktsioonis ja kuuludes finantsgruppi. Kõnealused lahknevused võivad takistada selliste uute ühetaoliste või tsentraliseeritud liidu mehhanismide loomist, mis kiirendaksid teatamisprotsessi ja toetaksid kiiret ja sujuvat pädevate asutuste vahelist teabevahetust, mis on äärmiselt oluline IKT-riskide käsitlemiseks suurte rünnete korral, millel võivad olla süsteemsed tagajärjed.

(22) Selleks et võimaldada pädevatel asutustel täita oma järelevalveülesandeid, saades täieliku ülevaate IKTga seotud intsidentide laadist, sagedusest, olulisusest ja mõjust, ning tõhustada asjaomaste avaliku sektori, sealhulgas õiguskaitse- ja kriisilahendusasutuste vahelist teabevahetust, tuleb sätestada normid, et täiendada IKTga seotud intsidentidest teatamise korda nõuetega, mida finantssektori allsektorit käsitlevad õigusaktid praegu ei sisalda, ning kõrvaldada kulude vähendamiseks kattuvused ja dubleerimine. Seepärast on oluline IKTga seotud intsidentidest teatamise korda ühtlustada, kohustades kõiki finantssektori ettevõtjaid teavitama ainult oma pädevaid asutusi. Lisaks peaks Euroopa järelevalveasutustel olema õigus täpsustada veelgi IKTga seotud intsidentidest teatamise elemente, nagu taksonoomia, tähtajad, andmekogumid, vormid ja kohaldatavad läved.

(23) Finantssektori mõnes allsektoris on digitaalse tegevuskerksuse testimise nõudeid välja töötatud mitmes koordineerimata riiklikus raamistikus, milles käsitletakse sama probleemi erineval viisil. See kahekordistab piiriüleste finantssektori ettevõtjate kulusid ja raskendab tulemuste vastastikust tunnustamist. Koordineerimata testimine võib seega ühtset turgu killustada.

(24) Kui testimist ei nõuta, jäävad haavatavused avastamata, mis tekitab finantssektori ettevõtjale ja kokkuvõttes ka finantssektori stabiilsusele ja usaldusväärsusele suurema riski. Ilma liidu sekkumiseta jääks digitaalse tegevuskerksuse testimine lünklikuks ja eri jurisdiktsioonid ei tunnustaks vastastikku testide tulemusi. Kuna on ebatõenäoline, et finantssektori muud allsektorid võtaksid selliseid skeeme mõistlikus ulatuses vastu, jääksid nad ilma võimalikust kasust, nagu haavatavuste ja riskide avastamine, kaitsevõime ja talitluspidevuse testimine ning tarbijate, tarnijate ja äripartnerite suurem kindlustunne. Kõnealuste kattuvuste, lahknevuste ja lünkade kõrvaldamiseks tuleb sätestada normid, mille eesmärk on tagada finantssektori ettevõtjate ja pädevate asutuste tehtavad koordineeritud testid ja millega edendataks oluliste finantssektori ettevõtjate puhul süvatestimise vastastikust tunnustamist.

(25) Finantssektori ettevõtjate sõltuvus IKT-teenustest tuleneb osaliselt nende vajadusest kohaneda tekkiva konkurentsivõimelise digitaalse maailmamajandusega, et suurendada oma tegevuse tõhusust ja vastata tarbijate nõudlusele. Sellise sõltuvuse laad ja ulatus on viimastel aastatel pidevalt muutunud ning aidanud vähendada kulusid finantsvahenduses ja võimaldanud finantstegevuste puhul äritegevust laiendada ja skaleerida, andes samal ajal mitmesugused IKT-vahendid keerukate siseprotsesside juhtimiseks.

(26) IKT-teenuste laialdast kasutust näitavad keerukad lepingupõhised kokkulepped, millest tulenevalt on finantssektori ettevõtjatel sageli raske leppida kokku lepingutingimustes, mis oleksid kohandatud vastavalt usaldatavusstandarditele või muudele regulatiivsetele nõuetele, mida nende suhtes kohaldatakse, või kasutada teatavaid õigusi, nagu pääsu- või auditeerimisõigused, juhul kui viimased on

kokkulepetes sätestatud. Paljude selliste lepingutega ei ole nähtud ette piisavaid kaitsemeetmeid, mis lubaksid tegevuse edasiandmise protsesse täies ulatuses jälgida, mistõttu ei saa finantssektori ettevõtja kõnealuseid seonduvaid riske hinnata. Kuna kolmandast isikust IKT-teenuste osutajad osutavad sageli standardteenuseid eri tüüpi klientidele, ei pruugi sellised lepingud alati olla piisavad finantssektoris osalejate individuaalsete või erivajaduste rahuldamiseks.

(27) Kuigi liidu mõned finantsteenuseid käsitlevad õigusaktid sisaldavad üldiseid norme tegevuse edasiandmise kohta, ei ole lepingulise aspekti järelevalve liidu õigusaktides täielikult sätestatud. Kuna puuduvad selged ja kohandatud liidu standardid, mida kohaldatakse kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingupõhiste kokkulepete suhtes, on IKT-riski väline allikas põhjalikult käsitlemata. Sellest tulenevalt on vaja kehtestada teatavad olulised põhimõtted, mis suunavad seda, kuidas finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski, ning millele lisanduvad peamised lepingulised õigused, mis puudutavad mitut lepingute täitmise ja lõpetamisega seotud elementi, eesmärgiga sätestada teatavad minimaalsed kaitsemeetmed, mis toetavad finantssektori ettevõtjate võimet jälgida tulemuslikult kõiki kolmandast isikust IKT-teenuste osutaja tasandil tekkivaid riske.

(28) Mis puudutab kolmandast isikust tulenevat IKT-riski ja sõltuvust kolmandast isikust IKT-teenuste osutajatest, siis puudub nii ühtsus kui ka ühtlustamine. Sellise spetsiifilise valdkonna nagu tegevuse edasiandmine käsitlemisel on tehtud mõningaid jõupingutusi (nt 2017. aasta soovitus pilveteenuse osutajatele tegevuse edasiandmise kohta[34]), kuid probleem, mis on seotud süsteemse riskiga, mille võib tekitada finantssektori seotus piiratud arvu kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega, on liidu õigusaktides vaevu tähelepanu saanud. Seda lünka liidu tasandil süvendab asjaolu, et ei ole konkreetseid volitusi ja vahendeid, mis võimaldaksid riiklikel järelevalveasutustel saada hästi aru sõltuvusest kolmandast isikust IKT-teenuste osutajatest ja jälgida piisaval määral riske, mis tulenevad selliste kolmandast isikust IKT-teenuste osutajatest sõltuvuste kontsentratsioonist.

(29) Võttes arvesse potentsiaalseid süsteemseid riske, mis kaasnevad tegevuse suurema edasiandmisega ja kolmandast isikust IKT-teenuste osutajate kontsentratsiooniga, ning selliste riiklike mehhanismide ebapiisavust, mis võimaldavad finantsjärelevalveasutustel kvantifitseerida, kvalifitseerida ja leevendada IKT-riskide tagajärgi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajates, on vaja luua asjakohane liidu järelevalveraamistik, mis võimaldab jälgida pidevalt selliste kolmandast isikust IKT-teenuste osutajate tegevust, mis on finantssektori ettevõtjate jaoks kriitilise tähtsusega.

(30) Kuna IKT-ohud on muutumas kompleksemaks ja keerukamaks, sõltuvad head avastamis- ja ennetamismeetmed suurel määral ohte ja haavatavusi puudutava teadmuse korrapärasest jagamisest finantssektori ettevõtjate vahel. Teabe jagamine aitab suurendada teadlikkust küberohtudest, mis omakorda suurendab finantssektori ettevõtjate suutlikkust hoida ära ohtude muutumist tegelikeks intsidentideks ning võimaldab finantssektori ettevõtjatel piirata paremini IKTga seotud intsidentide mõju ja tõhusamini taastuda. Liidu tasandi suuniste puudumise tõttu on sellist teadmuse jagamist pärssinud mitu tegurit, eelkõige ebakindlus seoses kooskõlaga andmekaitse-, monopolidevastaste ja vastutusnormidega.

[34] Soovitused pilveteenuse osutajatele tegevuse edasiandmise kohta (EBA/REC/2017/03), tühistatud EBA suunistega tegevuse edasiandmise kohta (EBA/GL/2019/02).

(31) Lisaks on kasuliku teabe jagamist takistanud kahtlused selle kohta, millist liiki teavet saab teiste turuosaliste või muude kui järelevalveasustega (nt ENISAga analüütilise sisendi andmiseks või Europoliga õiguskaitse otstarbel) jagada. Teabe jagamise ulatus ja kvaliteet on endiselt piiratud, killustunud, asjakohane teabevahetus toimub peamiselt lokaalselt (riiklike algatuste kaudu) ja puuduvad kogu liitu hõlmavad ühtsed teabe jagamise kokkulepped, mis oleks kohandatud vastavalt integreeritud finantssektori vajadustele.

(32) Seepärast tuleks finantssektori ettevõtjaid julgustada kasutama kollektiivselt oma individuaalseid teadmisi ja praktilisi kogemusi strateegilisel, taktikalisel ja operatiivsel tasandil, et suurendada oma suutlikkust küberohte piisavalt hinnata ja jälgida, end nende eest kaitsta ja neile reageerida. Seega tuleb liidu tasandil võimaldada mehhanismide loomist vabatahtlikult teabe jagamise kokkulepete jaoks, mis usaldusväärses keskkonnas sõlmimise korral aitaksid finantskogukonnal ennetada ohte ja reageerida neile ühiselt, piirates kiiresti IKT-riskide levikut ja takistades võimalikku ülekandumist finantskanalite kaudu. Neid mehhanisme tuleks kasutada täielikus kooskõlas kohaldatavate liidu konkurentsinormidega[35] ning viisil, mis tagab liidu andmekaitsenormide, eelkõige Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679[36] täieliku austamise, eriti olukorras, kus isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, nagu on osutatud nimetatud määruse artikli 6 lõike 1 punktis f.

(33) Hoolimata käesoleva määrusega ette nähtud laiast kohaldamisalast, tuleks digitaalse tegevuskerksuse normide kohaldamisel võtta arvesse finantssektori ettevõtjate suuruse, äriprofiili või digiriskile avatuse suuri erinevusi. Üldpõhimõte on see, et finantssektori ettevõtjad peaksid ressursside ja suutlikkuse suunamisel IKT-riskide juhtimise raamistiku rakendamisele võtma oma IKTga seotud vajaduste puhul nõuetekohaselt arvesse oma suurust ja äriprofiili; pädevad asutused peaksid aga jätkama sellise jaotuse hindamist ja läbivaatamist.

(34) Kuna suurematel finantssektori ettevõtjatel võib olla rohkem ressursse ning nad võivad kiiresti eraldada vahendeid juhtimisstruktuuride arendamiseks ja luua mitmesuguseid äristrateegiaid, peaksid ainult need finantssektori ettevõtjad, mis ei ole mikroettevõtjad käesoleva määruse tähenduses, olema kohustatud kehtestama keerukama juhtimiskorra. Sellistel ettevõtjatel on paremad vahendid, et luua eelkõige spetsiaalsed juhtimisfunktsioonid kolmandast isikust IKT-teenuste osutajatega sõlmitud järelevalvekokkulepete või kriisiohjamise jaoks, korraldada IKT-riskide juhtimine vastavalt kolme kaitseliiniga mudelile või võtta vastu personalijuhtimise dokument, milles on põhjalikult selgitatud pääsuõiguste põhimõtteid.

Samuti peaksid ainult sellised ettevõtjad olema kohustatud tegema pärast olulisi võrgu- ja infosüsteemide taristu ja protsesside muudatusi põhjalikke hindamisi, tegema korrapäraselt riskianalüüse IKT pärandsüsteemide kohta või laiendama talitluspidevuse ning reageerimis- ja taastekavade testimist, et hõlmata esmase IKT-taristu ja varurajatiste puhul ümberlülitusstsenaariume.

---

35 Komisjoni teatis „Suunised Euroopa Liidu toimimise lepingu artikli 101 kohaldatavuse kohta horisontaalkoostöö kokkulepete suhtes“ (2011/C 11/01).

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

(35) Kuna ainult neid finantssektori ettevõtjaid, mida käsitatakse digitaalse kerksuse süvatestimisel olulisena, tuleks kohustada tegema ohuteabel põhinevaid läbistusteste, tuleks selliste testide tegemisega kaasnevad haldusprotsessid ja rahalised kulud kanda üle väikesele protsendile finantssektori ettevõtjatele. Regulatiivse koormuse vähendamiseks tuleks ainult sellistelt finantssektori ettevõtjatelt, mis ei ole mikroettevõtjad, nõuda et nad esitaksid korrapäraselt pädevatele asutustele kõik IKT-katkestuste tekitatud kulud ja kahjud ning oluliste IKT-katkestuste järel tehtavate intsidendijärgsete läbivaatamiste tulemused.

(36) Selleks et tagada ühest küljest finantssektori ettevõtjate äristrateegiate ja teisest küljest IKT-riskide juhtimise täielik kooskõla ja üldine vastavus, tuleks juhtorganit kohustada täitma otsustavat ja aktiivset rolli IKT-riskide raamistiku suunamises ja kohandamises ning üldises digitaalse kerksuse strateegias. Lisaks sellele, et juhtorgani kasutatav lähenemisviis peaks keskenduma IKT-süsteemide kerksuse tagamise viisidele, peaks see hõlmama inimesi ja protsesse sellise poliitika kaudu, mis edendab ettevõtja igal tasandil kõigi töötajate suurt teadlikkust küberriskidest ja pühendumust tagada kõigil tasanditel range küberhügieen.

See, et kokkuvõttes on finantssektori ettevõtja IKT-riskide juhtimise eest vastutav juhtorgan, peaks olema selle laiahaardelise lähenemisviisi üldpõhimõte, mis peaks väljenduma juhtorgani pidevas osalemises IKT-riskide juhtimise järelevalve kontrollis.

(37) Juhtorgani täielik vastutus käib käsikäes sellise IKT-investeeringute taseme ja üldeelarve tagamisega, mis võimaldab finantssektori ettevõtjal täita digitaalse tegevuskerksuse miinimumnõudeid.

(38) Käesolevas määruses lähtutakse asjakohastest rahvusvahelistest, riiklikest ja sektori kehtestatud standarditest, suunistest ja soovitustest või küberriski juhtimise meetoditest[37] ning edendatakse funktsioone, mis hõlbustavad IKT-riskide juhtimise üldist struktureerimist. Kui finantssektori ettevõtjate loodud põhisuutlikkus vastab käesolevas määruses sätestatud funktsioonidest (kindlaksmääramine, kaitse ja ennetamine, avastamine, reageerimine ja taastamine, õppimine ja arenemine ning teabevahetus) tulenevate eesmärkide vajadustele, võivad finantssektori ettevõtjad kasutada teisiti piiritletud või kategoriseeritud IKT-riskide mudeleid.

(39) Selleks et muutuva küberohtude maastikuga sammu pidada, peaks finantssektori ettevõtjatel olema ajakohastatud IKT-süsteemid, mis on usaldusväärsed ja millel on piisav suutlikus mitte ainult andmetöötluse tagamiseks, mida on vaja teenuste osutamiseks, vaid ka tehnoloogilise kerksuse kindlustamiseks, mis võimaldab finantssektori ettevõtjatel tegeleda asjakohaselt täiendavate töötlemisvajadustega, mida võivad tekitada halvenenud turutingimused või muud ebasoodsad olukorrad. Kuigi käesoleva määrusega ei kaasne konkreetsete IKT-süsteemide, -vahendite või -tehnoloogia standardimist, eeldatakse selles, et finantssektori ettevõtjad kasutavad sobival viisil Euroopa ja rahvusvahelisel tasandil tunnustatud tehnilisi standardeid (nt

[37] CPMI-IOSCO, „Guidance on cyber resilience for financial market infrastructures“, https://www.bis.org/cpmi/publ/d146.pdf; „G7, Fundamental Elements of Cybersecurity for the Financial Sector“, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; riikliku standardi- ja tehnikainstituudi (NIST) küberturvalisuse kriisireguleerimise raamistik, https://www.nist.gov/cyberframework; finantsstabiilsuse nõukogu küberintsidentidele reageerimise ja nendest taastumise vahendid, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

ISO) või sektori parimaid tavasid, kui selline kasutus on täielikult kooskõlas konkreetsete järelevalvejuhistega rahvusvaheliste standardite kasutamise ja inkorporeerimise kohta.

(40) Tõhusaid talitluspidevuse ja taastekavasid on vaja selleks, et finantssektori ettevõtjad saaksid kohe ja kiiresti lahendada IKTga seotud intsidendid, eelkõige tulla toime küberrünnetega, piirates kahju ja seades prioriteediks tegevuse jätkamise ja taastemeetmed. Kuigi töötlus varusüsteemides peaks algama põhjendamatu viivituseta, ei tohiks see kuidagi seada ohtu võrgu- ja infosüsteemide terviklikkust ja turvalisust või andmete konfidentsiaalsust.

(41) Kuigi määrus lubab finantssektori ettevõtjatel määrata taastumisaja eesmärgid kindlaks paindlikult ja seega asjaomase funktsiooni laadi ja kriitilisust ning konkreetseid ärivajadusi täielikult arvesse võttes, tuleks siiski nõuda, et kõnealuste eesmärkide seadmisel hinnataks võimalikku kogumõju turu tõhususele.

(42) Finantssektoris on küberrünnete olulised tagajärjed võimendunud, kuna selles valdkonnas on palju suurem oht, et pahatahtlikud isikud taotlevad rahalist tulu otse allika juures. Selleks et niisuguseid riske maandada ja takistada seda, et IKT-süsteemid kaotavad oma terviklikkuse või ei ole saadaval, toimub konfidentsiaalsete andmetega seotud rikkumine või füüsiline IKT-taristu saab kahjustada, tuleks märkimisväärselt parandada IKTga seotud intsidentidest teatamist finantssektori ettevõtjate poolt.

IKTga seotud intsidentidest teatamist tuleks ühtlustada kõigi finantssektori ettevõtjate puhul, kohustades neid teavitama ainult oma pädevaid asutusi. Kuigi teatamise kohustus oleks kõigil finantssektori ettevõtjatel, peaks selle ulatus olema erinev, sest asjakohaseid olulisuse lävesid ja tähtaegu tuleks kohandada eesmärgiga kajastada ainult IKTga seotud olulisi intsidente. Otsene teatamine võimaldaks finantsjärelevalveasutustel pääseda juurde IKTga seotud teabele. Finantsjärelevalveasutused peaksid sellegipoolest edastama selle teabe muu kui finantsvaldkonna avaliku sektori asutustele (võrgu- ja infosüsteemide pädevad asutused, riiklikud andmekaitseasutused ja õiguskaitseasutused kuritegelikku laadi intsidentide puhul). Teavet IKTga seotud intsidentide kohta tuleks edastada vastastikku: finantsjärelevalveasutused peaksid edastama finantssektori ettevõtjale kogu vajaliku tagasiside või suunised ning Euroopa järelevalveasutused peaksid jagama anonüümseks muudetud andmeid sündmusega seotud ohtude ja haavatavuste kohta, et aidata kaasa laiemale ühisele kaitsele.

(43) Tuleks kavandada uusi mõttevahetusi, et käsitleda IKTga seotud intsidentidest teatamise võimalikku tsentraliseerimist, kasutades ühte keskset ELi keskust, mis kas saaks otseselt asjakohaseid teateid ja teavitaks automaatselt riiklikke pädevaid asutusi või üksnes tsentraliseeriks riiklike pädevate asutuste edastatud teateid ja mängiks koordinaatori rolli. Euroopa järelevalveasutused peaksid koostama EBA ja ENISAga konsulteerides teatavaks kuupäevaks ühisaruande, milles uuritakse sellise keskse ELi keskuse loomise teostatavust.

(44) Selleks et saavutada kindel digitaalne tegevuskerksus ja rahvusvahelistest standarditest (nt G7 põhielemendid ohuteabel põhineva läbistustestimise jaoks) lähtudes peaksid finantssektori ettevõtjad oma IKT-süsteeme ja töötajaid korrapäraselt testima, et teha kindlaks nende tulemuslikkus ennetamisel, avastamisel, reageerimisel ja taastamisel eesmärgiga leida ja käsitleda võimalikke IKTga seotud haavatavusi. Reageerimaks sellele, et finantssektori ettevõtjate küberturvalisuse valmisolek on finantssektori allsektorites ja nende lõikes erinev, peaks testimine hõlmama mitmesuguseid

vahendeid ja meetmeid alates põhinõuete hindamisest (nt haavatavuste hindamine ja skaneerimine, avatud lähtekoodiga tarkvara analüüsimine, võrgu turvalisuse hindamine, lünkade analüüsimine, füüsilise turvalisuse läbivaatamine, küsimustikud ja skaneerimistarkvara lahendused, võimalusel lähtekoodi ülevaatamine, stsenaariumipõhine testimine, ühilduvuse testimine, jõudlustestid või läbivtestimine) süvatestimiseni (nt ohuteabel põhinevad läbistustestid finantssektori ettevõtjate jaoks, mis on IKT seisukohast piisavalt küpsed, et selliseid teste teha). Järelikult peaksid digitaalse tegevuskerksuse testid olema oluliste finantssektori ettevõtjate (nagu suured krediidiasutused, börsid, väärtpaberite keskdepositooriumid ja kesksed vastaspooled) puhul raskemad. Samal ajal peaksid digitaalse tegevuskerksuse testid olema olulisemad mõningate allsektorite puhul, millel on peamine süsteemne roll (nt maksed, pangandus, kliiring ja arveldus) ja vähem olulised muude allsektorite puhul (nt varahaldurid, reitinguagentuurid). Piiriülesed finantssektori ettevõtjad, mis kasutavad liidus oma asutamis- või teenuste osutamise vabadust, peaksid oma päritoluliikmesriigis vastama ühele süvatestimise nõuete kogumile (nt ohuteabel põhinevad läbistustestid) ning kõnealune test peaks hõlmama IKT-taristut kõigis jurisdiktsioonides, kus piiriülene grupp liidus tegutseb, võimaldades seega piiriülestel gruppidel kanda testimiskulusid ainult ühes jurisdiktsioonis.

(45) Selleks et tagada kolmandast isikust tuleneva IKT-riski usaldusväärne jälgimine, on vaja sätestada põhimõtetel põhinevad normid, et suunata finantssektori ettevõtjates sellise riski jälgimist, mis tekib seoses kolmandast isikust IKT-teenuste osutajatele edasiantud funktsioonidega ja üldisemalt seoses kolmandast isikust IKT-teenuste osutajatest sõltumisega.

(46) Finantssektori ettevõtjal peaks igal ajal olema täielik vastutus käesoleva määruse kohaste kohustuste täitmise eest. Kolmandast isikust IKT-teenuste osutaja tasandil tekkinud riski proportsionaalsel jälgimisel tuleks võtta nõuetekohaselt arvesse IKTga seotud sõltuvuste ulatust, keerukust ja olulisust, teenuste kriitilisust või olulisust, lepingupõhiste kokkulepetega hõlmatud protsesse või funktsioone ja lõpuks hoolika hindamise põhjal võimalikku mõju finantsteenuste jätkumisele ja kvaliteedile ettevõtja ja grupi tasandil, nagu on asjakohane.

(47) Sellises järelevalves tuleks kasuta kolmandast isikust tulenevat IKT-riski käsitlevat strateegilist lähenemisviisi, mille formaliseerimiseks on finantssektori ettevõtja juhtorgan võtnud vastu spetsiaalse strateegia, mille alus on kõigi kõnealuste IKT-teenuseid osutavatest kolmandatest isikutest sõltuvuste pidev uurimine. Selleks et suurendada järelevalvealast teadlikkust IKT-teenuseid osutavatest kolmandatest isikutest sõltumisest ja toetada veelgi käesoleva määrusega loodud järelevalveraamistikku, peaksid finantsjärelevalveasutused saama registritelt korrapäraselt olulist teavet ja neil peaks olema võimalik küsida vajaduse korral selle väljavõtteid.

(48) Lepingupõhiste kokkulepete ametlikku sõlmimist peaks toetama ja sellele peaks eelnema põhjalik lepingueelne analüüs ning lepingute lõpetamise peaks tingima vähemalt selliste asjaolude kogum, millest nähtuvad kolmandast isikust IKT-teenuste osutaja puudujäägid.

(49) Selleks et käsitleda kolmandast isikust IKT-teenuste osutajate kontsentratsiooniriski süsteemset mõju, tuleks edendada tasakaalustatud lahendust läbi paindliku ja järgjärgulise lähenemisviisi, sest jäigad ülempiirid või ranged piirangud võivad pärssida äritegevust ja lepinguvabadust. Finantssektori ettevõtjad peaksid lepingupõhiseid kokkuleppeid põhjalikult hindama, et teha kindlaks kõnealuse riski

tekkimise tõenäosus, ning analüüsima muu hulgas põhjalikult edasiantud tegevuste edasiandmise kokkuleppeid, eelkõige juhul, kui need on sõlmitud kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajatega. Selles etapis ja selleks, et saavutada tasakaal lepinguvabaduse kaitsmise kohustuse ja finantsstabiilsuse tagamise kohustuse vahel, ei peeta sobivaks näha ette kolmandast isikust IKT-teenuste osutajatega seotud rangeid ülempiire ja piiranguid. Euroopa järelevalveasutus, mis on määratud tegema järelevalvet iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja üle (juhtiv järelevalveasutus), peaks pöörama järelevalveülesannete täitmisel erilist tähelepanu sellele, et mõista täielikult sõltuvuste ulatust ja avastada konkreetsed olukorrad, kus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suur kontsentratsioon liidus tekitab tõenäoliselt survet liidu finantssüsteemi stabiilsusele ja usaldusväärsusele, ning nägema ette dialoogi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega, juhul kui selline risk on tuvastatud[38].

(50) Selleks et oleks võimalik korrapäraselt hinnata ja jälgida kolmandast isikust IKT-teenuste osutaja võimet osutada finantssektori ettevõtjale turvaliselt teenuseid, avaldamata negatiivset mõju ettevõtja kerksusele, peaksid peamised lepinguelemendid olema kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingute täitmisel ühtlustatud. Need elemendid hõlmavad ainult vähimaid lepinguaspekte, mida peetakse oluliseks, et võimaldada finantssektori ettevõtjal jälgida IKT-teenuse stabiilsusest ja turvalisusest sõltuvat digitaalset tegevuskerksust.

(51) Lepingupõhistes kokkulepetes tuleks esitada eelkõige funktsioonide ja teenuste täielik kirjeldus ning kõnealuste funktsioonide täitmise ja andmete töötlemise kohad ning täielikud teenustaseme kirjeldused, millele on lisatud kvantitatiivsed ja kvalitatiivsed tulemuseesmärgid kokku lepitud teenustasemete piires, et finantssektori ettevõtja saaks teha tulemuslikku järelevalvet. Mis puudutab finantssektori ettevõtja võimet tagada kolmandast isikust tuleneva riski jälgimine, siis selle oluliste elementidena tuleks käsitada ka sätteid isikuandmetele ligipääsetavuse, nende kättesaadavuse, tervikluse, turvalisuse ja kaitse kohta ning garantiisid juurdepääsu, taastamise ja tagastamise kohta kolmandast isikust IKT-teenuste osutaja maksejõuetuse, kriisilahenduse või äritegevuse lõpetamise korral.

(52) Selleks et tagada, et finantssektori ettevõtjatel on täielik kontroll kõigi muudatuste üle, mis võivad kahjustada nende IKT turvalisust, tuleks sätestada kolmandast isikust IKT-teenuste osutaja etteteatamistähtajad ja aruandekohustused selliste muudatuste puhuks, mis võivad oluliselt kahjustada kolmandast isikust IKT-teenuste osutaja võimet täita tulemuslikult kriitilise tähtsusega või olulisi funktsioone, sealhulgas IKTga seotud intsidendi korral viimati nimetatu abi lisatasuta või eelnevalt kindlaks määratud tasu eest.

(53) Finantssektori ettevõtja jooksvas järelevalves kolmandast isikust IKT-teenuste osutaja tegevuse üle on äärmiselt olulisteks vahenditeks finantssektori ettevõtja või määratud kolmanda isiku pääsu-, kontrolli- ja auditeerimisõigused, samuti kõnealuse teenuseosutaja täielik koostöö kontrollide ajal. Ka finantssektori ettevõtja pädeval asutusel peaksid olema need õigused ehk õigus teadete alusel kontrollida ja auditeerida kolmandast isikust IKT-teenuste osutajat, juhul kui konfidentsiaalsuse nõue on täidetud.

[38] Kui peaks tekkima domineerivaks peetava kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja poolse kuritarvitamise risk, peaks finantssektori ettevõtjatel olema võimalus esitada Euroopa Komisjonile või riiklikele konkurentsiõiguse asutustele ametlik või mitteametlik kaebus.

(54) Lepingupõhistes kokkulepetes tuleks näha ette selged lõpetamisõigused ja nendega seotud lühimad etteteatamistähtajad, samuti spetsiaalsed väljumisstrateegiad, mis võimaldavad eelkõige kohustuslikke üleminekuperioode, mille jooksul kolmandast isikust IKT-teenuste osutajad peaksid jätkama asjaomaste funktsioonide täitmist, et vähendada katkestuste riski finantssektori ettevõtja tasandil või võimaldada viimasel lülituda tulemuslikult ümber teistele kolmandast isikust IKT-teenuste osutajatele või otsustada kasutada siselahendusi, olenevalt osutatud teenuse keerukusest.

(55) Lisaks võib selliste lepingu tüüptingimuste vabatahtlik kasutamine, mille komisjon on töötanud välja pilvandmetöötlusteenuste jaoks, olla finantssektori ettevõtjatele ja nende kolmandast isikust IKT-teenuste osutajatele mugavam, suurendades täielikus kooskõlas finantsteenuseid käsitlevas määruses sätestatud nõuete ja ootustega õiguskindlust finantssektoris pilvandmetöötlusteenuste kasutamise puhul. See töö tugineb meetmetele, mida kavandati juba 2018. aasta finantstehnoloogia tegevuskavas, mis näitas komisjoni kavatsust julgustada ja hõlbustada selliste lepingu tüüptingimuste väljatöötamist, mida finantssektori ettevõtjad saaks kasutada pilvandmetöötlusteenuste edasiandmisel, lähtudes valdkonnaüleste pilvandmetöötlusteenuste sidusrühmade jõupingutustest, mida komisjon on finantssektori osalusel edendanud.

(56) Selleks et edendada selliste järelevalvealaste lähenemisviiside ühtlustamist ja tõhusust, mis käsitlevad finantssektorile kolmandatest isikutest tulenevat IKT-riski, tugevdada selliste finantssektori ettevõtjate digitaalset tegevuskerksust, mis sõltuvad operatiivsete funktsioonide puhul kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatest, ning seega aidata säilitada liidu finantssüsteemi stabiilsust ja finantsteenuste ühtse turu usaldusväärsust, tuleks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes kohaldada liidu järelevalveraamistikku.

(57) Kuna erikäsitlus on õigustatud ainult kriitilise tähtsusega kolmandast isikust teenuseosutajate puhul, tuleks liidu järelevalveraamistiku kohaldamiseks luua nende kindlaksmääramise mehhanism eesmärgiga võtta arvesse finantssektoris kõnealustest kolmandast isikust IKT-teenuste osutajatest sõltumise mõõdet ja laadi, mis tähendab kvantitatiivseid ja kvalitatiivseid kriteeriume, millele tuginedes põhineks järelevalvega hõlmatus kriitilisuse parameetritel. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatel, mis ei ole eespool osutatud kriteeriumide põhjal automaatselt järelevalve alla määratud, peaks olema võimalus järelevalveraamistikku vabatahtlikult kohaldada, kuid need kolmandast isikust IKT-teenuste osutajad, mille suhtes juba kohaldatakse eurosüsteemi tasandil kehtestatud järelevalvemehhanismide raamistikke eesmärgiga toetada Euroopa Liidu toimimise lepingu artikli 127 lõikes 2 osutatud ülesandeid, peaksid olema vabastatud.

(58) Nõue, et kolmandast isikust IKT-teenuste osutajad, keda loetakse olevat kriitilise tähtsusega, peavad olema liidus asutatud, ei puuduta andmete lokaliseerimist, sest käesoleva määrusega ei kaasne uusi nõudeid, mille kohaselt tuleks andmeid talletada või töödelda liidus.

(59) See raamistik ei tohiks piirata liikmesriikide pädevust teha ise järelevalvemissioone, mis puudutavad kolmandast isikust IKT-teenuste osutajaid, mis ei ole käesoleva määruse kohaselt kriitilise tähtsusega, kuid mida võib riiklikul tasandil käsitada olulistena.

(60) Selleks et kasutada finantsteenuste valdkonna praegust mitmetasandilist institutsioonilist ülesehitust, peaks Euroopa järelevalveasutuste ühiskomitee jätkuvalt tagama üldise sektoritevahelise koordineerimise kõigis IKT-riskiga seotud küsimustes kooskõlas oma küberturvalisust puudutavate ülesannetega ja teda peaks toetama uus

allkomitee (järelevalvefoorum), mis valmistab ette kriitilise tähtsusega kolmandatest isikutest IKT-teenuste osutajatele suunatud individuaalseid otsuseid ja ühissoovitusi – eelkõige kriitilise tähtsusega kolmandatest isikutest IKT-teenuste osutajate järelevalvekavade võrdlemise kohta – ning teeb kindlaks IKT kontsentratsiooniriskiga seotud probleemide lahendamise parimad tavad.

(61) Selleks et selliste kolmandast isikust IKT-teenuste osutajate üle, mis mängivad finantssektori toimimises kriitilist rolli, tehtaks liidu mastaabis samaulatuslikku järelevalvet, tuleks iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja puhul määrata üks Euroopa järelevalveasutus juhtivaks järelevalveasutuseks.

(62) Juhtivatel järelevalveasutustel peaksid olema vajalikud volitused, et teha uurimisi, kohapealseid ja kaugkontrolle kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajates, pääseda juurde kõigile asjaomastele ruumidele ja kohtadele ning saada täielikku ja ajakohastatud teavet, mis võimaldaks saada tegeliku ülevaate sellise finantssektori ettevõtjaid ja kokkuvõttes liidu finantssüsteemi ohustava IKT-riski liigist, mõõtmest ja mõjust, mis tuleneb kolmandast isikust.

Euroopa järelevalveasutustele järelevalves juhtiva rolli andmine on eeltingimus, et saada aru IKT-riski süsteemsest mõõtmest rahanduses ja seda käsitleda. Liidu jalajälg seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega ja sellega seotud võimalikud IKT kontsentratsiooniriski probleemid eeldavad ühist lähenemisviisi liidu tasandil. Mitme auditi tegemine ja pääsuõiguste kasutamine eraldi paljude pädevate asutuste poolt ja vähese koordineerimisega või koordineerimiseta ei annaks kolmandast isikust tulenevast IKT-riskist täielikku ülevaadet, vaid looks tarbetut liiasust, koormust ja keerukust kolmandast isikust IKT-teenuste osutajatele, kellel tuleb tegeleda rohkete taotlustega.

(63) Peale selle peaksid juhtivad järelevalveasutused saama esitada IKT-riski küsimuses soovitusi ja sobivaid parandusmeetmeid, samuti vastuväiteid teatavatele lepingupõhistele kokkulepetele, mis kokkuvõttes mõjutavad finantssektori ettevõtja või finantssüsteemi stabiilsust. Juhtivate järelevalveasutuste esitatud oluliste soovituste järgimist peaksid riiklikud pädevad asutused võtma nõuetekohaselt arvesse, kui nad täidavad oma funktsiooni, mis on seotud finantssektori ettevõtjate usaldatavusnõuete täitmise järelevalvega.

(64) Järelevalveraamistik ei asenda mingil viisil või mingis osas finantssektori ettevõtjates kolmandast isikust IKT-teenuste osutajate kasutamisest tulenava riski juhtimist, sealhulgas kohustus jälgida jooksvalt nende lepingupõhiseid kokkuleppeid kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega, ega mõjuta finantssektori ettevõtjate täielikku vastutust kõigi käesoleva määruse ja finantsteenuseid käsitlevate õigusaktide kohaste nõuete rahuldamise ja täitmise eest. Selleks et vältida dubleerimist ja kattuvust, peaksid pädevad asutused hoiduma üksi selliste meetmete võtmisest, mille eesmärk on jälgida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate riske. Kõik sellised meetmed tuleks enne järelevalveraamistikus kooskõlastada ja kokku leppida.

(65) Selleks et edendada rahvusvahelisel tasandil selliste parimate tavade ühtlustamist, mida järgitakse kolmandast isikust IKT-teenuste osutajate digiriski juhtimise läbivaatamisel, tuleks Euroopa järelevalveasutusi julgustada sõlmima koostöökokkuleppeid kolmandate riikide asjaomaste pädevate järelevalve- ja reguleerivate asutustega, et hõlbustada kolmandast isikust tulenevat IKT-riski käsitlevate parimate tavade väljatöötamist.

(66) Selleks et kasutada ära pädevate asutuste ekspertide tehnilisi teadmisi operatsiooni- ja IKT-riskide juhtimise alal, peaksid juhtivad järelevalveasutused toetuma riikide järelevalvekogemusele ja looma spetsiaalsed uurimisrühmad iga üksiku kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja jaoks, moodustades multidistsiplinaarsed meeskonnad, et toetada järelevalvetegevuse, sealhulgas kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kohapealsete kontrollide ja vajalike järelmeetmete ettevalmistamist ja tegelikku elluviimist.

(67) Pädevatel asutustel peaksid olema kõik käesoleva määruse kohaldamise tagamiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused. Halduskaristused tuleks üldiselt avaldada. Kuna finantssektori ettevõtjad ja kolmandast isikust IKT-teenuste osutajad võivad olla asutatud eri liikmesriikides ja nende üle võivad järelevalvet teha eri valdkondade pädevad asutused, tuleks vastastikuse teabevahetuse ja järelevalvetegevuses abistamise kaudu tagada tihe koostöö asjakohaste pädevate asutuste vahel, sealhulgas EKPga seoses talle nõukogu määrusega (EL) nr 1024/2013[39] antud eriülesannetega, ning konsulteerimine Euroopa järelevalveasutustega.

(68) Selleks et täiendavalt kvantifitseerida ja kvalifitseerida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate määramise kriteeriume ja ühtlustada järelevalvetasusid, tuleks komisjonile anda õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu õigusakte, milles täpsustatakse veelgi süsteemset mõju, mida kolmandast isikust IKT-teenuste osutaja maksejõuetus võib avaldada teenindatavatele finantssektori ettevõtjatele, selliste globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate arvu, mis sõltuvad asjaomasest kolmandast isikust IKT-teenuste osutajast, teataval turul tegutsevate kolmandast isikust IKT-teenuste osutajate arvu, teisele kolmandast isikust IKT-teenuste osutajale ülemineku kulusid, nende liikmesriikide arvu, kus asjaomane kolmandast isikust IKT-teenuste osutaja osutab teenuseid ja tegutsevad asjaomast kolmandast isikust IKT-teenuste osutajat kasutavad finantssektori ettevõtjad ning järelevalvetasude summat ja nende tasumise viisi.

On eriti oluline, et komisjon korraldaks oma ettevalmistava töö käigus asjakohaseid konsultatsioone, muu hulgas ekspertide tasandil, ja et need konsultatsioonid korraldataks kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes[40] sätestatud põhimõtetega. Selleks et tagada võrdne osalemine delegeeritud õigusaktide ettevalmistamises, saavad Euroopa Parlament ja nõukogu kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel on süstemaatiline juurdepääs komisjoni eksperdirühmade kohtumistele, kus valmistatakse ette delegeeritud õigusakte.

(69) Kuna käesoleva määruse ja Euroopa Parlamendi ja nõukogu direktiiviga (EL) 20xx/xx[41] kaasneb täieliku kooskõla tagamiseks selliste IKT-riskide juhtimist käsitlevate sätete konsolideerimine, mis sisalduvad mitmes liidu finantsteenuste õigustiku määruses ja direktiivis, sealhulgas määrustes (EÜ) nr 1060/2009, (EL) nr 648/2012 (EL) nr 600/2014 ja (EL) nr 909/2014, tuleks osutatud määruseid muuta, et selgitada, et asjakohased IKT-riskiga seotud sätted sisalduvad käesolevas määruses.

---

39 Nõukogu 15. oktoobri 2013. aasta määrus (EL) nr 1024/2013, millega antakse Euroopa Keskpangale eriülesanded seoses krediidiasutuste usaldatavusnõuete täitmise järelevalve poliitikaga (ELT L 287, 29.10.2013, lk 63).

40 ELT L 123, 12.5.2016, lk 1.

41 [*lisada täielik viide*]

Tehnilised standardid peaksid tagama käesolevas määruses sätestatud nõuete järjekindla ühtlustamise. Kuna Euroopa järelevalveasutustel on põhjalikud eriteadmised, tuleks teha neile ülesandeks töötada komisjonile esitamiseks välja regulatiivsete tehniliste standardite eelnõud, mille puhul ei ole vaja teha poliitilisi otsuseid. Regulatiivsed tehnilised standardid tuleks töötada välja IKT-riskide juhtimise, aruandluse, testimise ja kolmandast isikust tuleneva IKT-riski usaldusväärse jälgimise põhinõuete valdkonnas.

(70) On eriti oluline, et komisjon korraldaks oma ettevalmistava töö käigus asjakohaseid konsultatsioone, muu hulgas ekspertide tasandil. Komisjon ja Euroopa järelevalveasutused peaksid tagama, et kõik finantssektori ettevõtjad saavad kõnealuseid standardeid ja nõudeid kohaldada viisil, mis on proportsionaalne nende ja nende tegevuse laadi, ulatuse ja keerukusega.

(71) Selleks et parandada IKTga seotud oluliste intsidentide teadete võrreldavust ja tagada läbipaistvus seoses lepingupõhiste kokkulepetega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate IKT-teenuste kasutamist, tuleks Euroopa järelevalveasutustele anda volitused koostada rakenduslike tehniliste standardite eelnõud, millega kehtestatakse finantssektori ettevõtjatele mõeldud standardmallid, -vormid ja -menetlused IKTga seotud olulisest intsidendist teatamiseks ning standardmallid teaberegistrile. Nende standardite väljatöötamisel peaksid Euroopa järelevalveasutused võtma arvesse finantssektori ettevõtjate suurust ja keerukust ning nende tegevuse laadi ja sellega seotud riski taset. Komisjonil peaks olema õigus võtta need rakenduslikud tehnilised standardid vastu ELi toimimise lepingu artikli 291 kohaste rakendusaktidega ja kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 15. Kuna määrustes (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014 sisalduvatel tehnilistel regulatiivsetel ja rakenduslikel tehnilistel standarditel põhinevate delegeeritud õigusaktide ja rakendusaktidega on juba täpsustatud täiendavaid nõudeid, on asjakohane anda Euroopa järelevalveasutustele kas eraldi või ühiskomitee kaudu kõigile korraga volitused esitada komisjonile regulatiivsed ja rakenduslikud tehnilised standardid selliste delegeeritud õigusaktide ja rakendusaktide vastuvõtmiseks, millega võetakse üle ja ajakohastatakse kehtivaid IKT-riskide juhtimise norme.

(72) Sellega kaasneb erinevates finantsteenuste valdkondades vastu võetud kehtivate delegeeritud õigusaktide ja rakendusaktide hilisem muutmine. Selliste operatsiooniriski käsitlevate artiklite kohaldamisala, millega anti kõnealustes õigusaktides volitus võtta vastu delegeeritud õigusakte ja rakendusakte, tuleks muuta, et kanda käesolevasse määrusesse üle kõik sellised sätted digitaalse tegevuskerksuse kohta, mis praegu sisalduvad kõnealustes määrustes.

(73) Kuna käesoleva määruse eesmärke, eelkõige kõigi finantssektori ettevõtjate kõrge digitaalse tegevuskerksuse tase, ei suuda liikmesriigid piisavalt saavutada, sest need eeldavad paljude selliste lahknevate õigusnormide ühtlustamist, mis sisalduvad praegu kas mõnes liidu õigusaktis või eri liikmesriikide õigussüsteemis, küll aga saab neid ulatuse ja mõju tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale,

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese

1. Käesolevas määruses sätestatakse järgmised ühetaolised nõuded, mis käsitlevad finantssektori ettevõtjate äriprotsesse toetavate võrgu- ja infosüsteemide turvalisust ja mida on vaja digitaalse tegevuskerksuse ühtlaselt kõrge taseme saavutamiseks:

   (a) finantssektori ettevõtjate suhtes kohaldatavad nõuded, mis puudutavad

   – info- ja kommunikatsioonitehnoloogia (IKT) riskide juhtimist;

   – pädevate asutuste teavitamist IKTga seotud olulistest intsidentidest;

   – digitaalse tegevuskerksuse testimist;

   – küberohte ja haavatavusi puudutava teabe ja teadmuse jagamist;

   – meetmeid kolmandast isikust tulenevate IKT-riskide usaldusväärseks juhtimiseks finantssektori ettevõtjate poolt;

   (b) kolmandast isikust IKT-teenuste osutajate ja finantssektori ettevõtjate vahel sõlmitud lepingupõhiseid kokkuleppeid käsitlevaid nõudeid;

   (c) järelevalveraamistikku selliste kriitilise tähtsusega IKT-teenuste osutajate jaoks, kes osutavad teenuseid finantssektori ettevõtjatele;

   (d) norme, mis käsitlevad pädevate asutuste koostööd ning pädevate asutuste poolset järelevalvet ja nõuete täitmise tagamist kõigis käesoleva määrusega hõlmatud küsimustes.

2. Mis puudutab finantssektori ettevõtjaid, mida käsitatakse oluliste teenuste operaatoritena vastavalt riigisisestele õigusnormidele, millega on üle võetud direktiivi (EL) 2016/1148 artikkel 5, siis käesolevat määrust käsitatakse nimetatud direktiivi artikli 1 lõike 7 kohaldamisel sektoripõhise liidu õigusaktina.

Artikkel 2

Isikuline kohaldamisala

1. Käesolevat määrust kohaldatakse järgmiste üksuste suhtes:

   (a) krediidiasutused,

   (b) makseasutused,

   (c) e-raha asutused,

   (d) investeerimisühingud,

   (e) krüptovarateenuse osutajad, krüptovara emitendid, varapõhiste tokenite emitendid ja oluliste varapõhiste tokenite emitendid,

   (f) väärtpaberite keskdepositooriumid,

   (g) kesksed vastaspooled,

(h) kauplemiskohad,

(i) kauplemisteabehoidlad,

(j) alternatiivsete investeerimisfondide valitsejad,

(k) fondivalitsejad,

(l) aruandlusteenuste pakkujad,

(m) kindlustus- ja edasikindlustusandjad,

(n) kindlustusvahendajad, edasikindlustusvahendajad ja kõrvaltegevusena pakutava kindlustuse vahendajad,

(o) tööandja kogumispensioni asutused,

(p) reitinguagentuurid,

(q) vannutatud audiitorid ja audiitorühingud,

(r) kriitilise tähtsusega võrdlusaluste haldurid,

(s) ühisrahastamisteenuse osutajad,

(t) väärtpaberistamise registrid,

(u) kolmandast isikust IKT-teenuste osutajad.

2. Käeoleva määruse kohaldamisel nimetatakse punktides a–t osutatud üksusi koos finantssektori ettevõtjateks.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

(1) „digitaalne tegevuskerksus“ – finantssektori ettevõtja võime luua, tagada ja vaadata läbi oma tegevuse terviklikkust tehnoloogilisest vaatenurgast, tagades kas otseselt või kaudselt kolmandast isikust IKT-teenuste osutajate teenuste kasutamise kaudu kogu IKTga seotud suutlikkuse, mida on vaja selliste võrgu- ja infosüsteemide turvalisuse käsitlemiseks, mida finantssektori ettevõtja kasutab ning mis toetavad finantsteenuste jätkuvat osutamist ja nende kvaliteeti;

(2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2016/1148 artikli 4 punktis 1 määratletud võrgu- ja infosüsteem;

(3) „võrgu- ja infosüsteemide turvalisus“ – direktiivi (EL) 2016/1148 artikli 4 punktis 2 määratletud võrgu- ja infosüsteemide turvalisus;

(4) „IKT-risk“ – mõistlikult tuvastatav asjaolu võrgu- ja infosüsteemide kasutamisel (sealhulgas häire, suutvuse puudus, tõrge, katkestus, kahjustus, väärkasutus, kadu või muud liiki pahatahtlik või mittepahatahtlik sündmus), mis realiseerumise korral võib seada ohtu võrgu- ja infosüsteemide, tehnoloogiast sõltuva vahendi või protsessi, operatsiooni ja protsessi toimimise või teenuste osutamise turvalisuse, seades seeläbi ohtu andmete, tarkvara või mõne muu IKT-teenuste ja -taristu komponendi tervikluse või kättesaadavuse või rikkudes konfidentsiaalsust või tekitades kahju füüsilisele IKT-taristule või muu negatiivse tagajärje;

(5) „teabevara“ – materiaalne või mittemateriaalne teabekogu, mida tasub kaitsta;

(6) „IKTga seotud intsident“ – ettenägematu tuvastatud ilming võrgu- ja infosüsteemides, mis tuleneb pahatahtlikust tegevusest või mitte ning seab ohtu võrgu- ja infosüsteemide või nende süsteemide töödeldava, talletatava või edastatava teabe turvalisuse või avaldab negatiivset mõju finantssektori ettevõtja osutatavate finantsteenuste kättesaadavusele, konfidentsiaalsusele, jätkuvusele või autentsusele;

(7) „IKTga seotud oluline intsident“ – IKTga seotud intsident, millel võib olla suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega funktsioone;

(8) „küberoht“ – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[42] artikli 2 punktis 8 määratletud küberoht;

(9) „küberrünne“ – IKTga seotud pahatahtlik intsident, mis kujutab endast ohusubjekti katset hävitada, paljastada, muuta, desaktiveerida või varastada vara, saada varale loata juurdepääs või kasutada vara ilma loata;

(10) „ohuteadmus“ – teave, mida on agregeeritud, teisendatud, analüüsitud, tõlgendatud või rikastatud, et anda otsuste tegemiseks vajalik kontekst, ning mis tagab asjakohase ja piisava arusaamise IKTga seotud intsidendi või küberohu mõju leevendamiseks, sealhulgas küberründe tehnilised üksikasjad, ründe toimepanijad ning nende töömeetodid ja ajendid;

(11) „süvakaitse“ – IKTga seotud strateegia, mis integreerib inimesi, protsesse ja tehnoloogiat, et luua ettevõtjas mitmel tasandil ja mitmes mõõtmes eri tõkkeid;

(12) „haavatavus“ – vara, süsteemi, protsessi või kontrolli nõrkus, tundlikkus või viga, mida oht võib ära kasutada;

(13) „ohuteabel põhinev läbistustestimine“ – tingimused, mis matkivad taktikat, tehnikat ja menetlusi, mida kasutavad tegelikud ohusubjektid, keda tajutakse tegeliku küberohu tekitajatena, ning mis võimaldavad teha ettevõtja kriitilise tähtsusega töötavate tarbesüsteemide kontrollitud, kohandatud, teadmuspõhise (punane tiim) testi;

(14) „kolmandast isikust tulenev IKT-risk“ – IKT-risk, mis võib finantssektori ettevõtjat ohustada, kui ta kasutab kolmandast isikust IKT-teenuste osutajate või nende alltöövõtjate IKT-teenuseid;

(15) „kolmandast isikust IKT-teenuste osutaja“ – ettevõtja, mis osutab digi- ja andmeteenuseid, sealhulgas pilvandmetöötlus-, tarkvara-, andmeanalüüsi- ja andmekeskuse teenuste osutajad, kuid välja arvatud riistvarakomponentide pakkujad ja liidu õiguse alusel tegevusloa saanud ettevõtjad, mis osutavad Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/1972[43] artikli 2 punktis 4 määratletud elektroonilise side teenuseid;

(16) „IKT-teenused“ – digi- ja andmeteenused, mida osutatakse IKT-süsteemide kaudu ühele või mitmele sise- või väliskasutajale, sealhulgas andmete edastamise,

---

[42] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

[43] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud) (ELT L 321, 17.12.2018, lk 36).

sisestamise, talletamise ja töötlemise teenused, aruandlusteenused, andmete seire ning äri- ja otsustustoeteenused;

(17) „kriitilise tähtsusega või oluline funktsioon“ – funktsioon, mille häiritud, vigane või ebaõnnestunud täitmine kahjustaks oluliselt finantssektori ettevõtja tegevusloast tulenevate tingimuste ja kohustuste või tema muude, kohaldatavate finantsteenuseid käsitlevate õigusaktide kohaste kohustuste jätkuvat täitmist või tema finantstulemusi või teenuste ja tegevuse usaldusväärsust või jätkuvust;

(18) „kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja“ – kolmandast isikust IKT-teenuste osutaja, kes on määratud vastavalt artiklile 29 ja kelle suhtes kohaldatakse artiklites 30–37 osutatud järelevalveraamistikku;

(19) „kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutaja“ – kolmandast isikust IKT-teenuste osutaja, kes on kolmandas riigis asutatud juriidiline isik, kes ei ole alustanud äritegevust / ei tegutse liidus ning on sõlminud finantssektori ettevõtjaga IKT-teenuste osutamiseks lepingupõhise kokkuleppe;

(20) „kolmandas riigis asutatud IKT alltöövõtja“ – IKT alltöövõtja, kes on kolmandas riigis asutatud juriidiline isik, kes ei ole alustanud äritegevust / ei tegutse liidus ning on sõlminud lepingupõhise kokkuleppe kas kolmandast isikust IKT-teenuste osutajaga või kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajaga;

(21) „IKT kontsentratsioonirisk“ – 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 finantssektori ettevõtja ja kokkuvõttes liidu finantssüsteemi kui terviku suutlikkus täita kriitilise tähtsusega funktsioone või tulla toime muud liiki negatiivse mõju, sealhulgas suure kahjuga;

(22) „juhtorgan“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 36, direktiivi 2013/36/EL artikli 3 lõike 1 punktis 7, direktiivi 2009/65/EÜ artikli 2 lõike 1 punktis s, määruse (EL) nr 909/2014 artikli 2 lõike 1 punktis 45, Euroopa Parlamendi ja nõukogu määruse (EL) 2016/1011[44] artikli 3 lõike 1 punktis 20, Euroopa Parlamendi ja nõukogu määruse (EL) 20xx/xx[45] artikli 3 lõike 1 punktis u määratletud juhtorgan või vastavad isikud, kes tegelikult juhivad üksust või täidavad põhifunktsioone kooskõlas liidu või liikmesriikide asjakohaste õigusaktidega;

(23) „krediidiasutus“ – Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013[46] artikli 4 lõike 1 punktis 1 määratletud krediidiasutus;

(24) „investeerimisühing“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 1 määratletud investeerimisühing;

(25) „makseasutus“ – direktiivi (EL) 2015/2366 artikli 1 lõike 1 punktis d määratletud makseasutus;

---

44 Euroopa Parlamendi ja nõukogu 8. juuni 2016. aasta määrus (EL) 2016/1011, mis käsitleb indekseid, mida kasutatakse võrdlusalustena finantsinstrumentide ja -lepingute puhul või investeerimisfondide tootluse mõõtmiseks, ning millega muudetakse direktiive 2008/48/EÜ ja 2014/17/EL ning määrust (EL) nr 596/2014 (ELT L 171, 29.6.2016, lk 1).

45 [*lisada täielik pealkiri ja ELT üksikasjad*]

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

(26) „e-raha asutus“ – Euroopa Parlamendi ja nõukogu direktiivi 2009/110/EÜ artikli 2 punktis 1 punktis d määratletud e-raha asutus[47];

(27) „keskne vastaspool“ – määruse (EL) nr 648/2012 artikli 2 lõikes 1 määratletud keskne vastaspool;

(28) „kauplemisteabehoidla“ – määruse (EL) nr 648/2012 artikli 2 punktis 2 määratletud kauplemisteabehoidla;

(29) „väärtpaberite keskdepositoorium“ – määruse nr 909/2014 artikli 2 lõike 1 punktis 1 määratletud väärtpaberite keskdepositoorium;

(30) „kauplemiskoht“ – direktiivi/2014/65/EL artikli 4 lõike 1 punktis 24 määratletud kauplemiskoht;

(31) „alternatiivse investeerimisfondi valitseja“ – direktiivi 2011/61/EL artikli 4 lõike 1 punktis b määratletud alternatiivse investeerimisfondi valitseja;

(32) „fondivalitseja“ – direktiivi 2009/65/EÜ artikli 2 lõike 1 punktis b määratletud fondivalitseja;

(33) „aruandlusteenuse pakkuja“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 63 määratletud aruandlusteenuse pakkuja;

(34) „kindlustusandja“ – direktiivi 2009/138/EÜ artikli 13 punktis 1 määratletud kindlustusandja;

(35) „edasikindlustusandja“ – direktiivi 2009/138/EÜ artikli 13 punktis 4 määratletud edasikindlustusandja;

(36) „kindlustusvahendaja“ – direktiivi (EL) 2016/97 artikli 2 punktis 3 määratletud kindlustusvahendaja;

(37) „kõrvaltegevusena pakutava kindlustuse vahendaja“ – direktiivi (EL) 2016/97 artikli 2 punktis 4 määratletud kõrvaltegevusena pakutava kindlustuse vahendaja;

(38) „edasikindlustusvahendaja“ – direktiivi (EL) 2016/97 artikli 2 punktis 5 määratletud edasikindlustusvahendaja;

(39) „tööandja kogumispensioni asutus“ – direktiivi 2016/2341 artikli 1 punktis 6 määratletud tööandja kogumispensioni asutus;

(40) „krediidiasutus“ – määruse (EL) nr 1060/2009 artikli 3 lõike 1 punktis a määratletud krediidiasutus;

(41) „vannutatud audiitor“ – direktiivi 2006/43/EÜ artikli 2 punktis 2 määratletud vannutatud audiitor;

(42) „audiitorühing“ – direktiivi 2006/43/EÜ artikli 2 punktis 3 määratletud audiitorühing;

(43) „krüptovarateenuse osutaja“ – määruse (EL) 202x/xx artikli 3 lõike 1 punktis n määratletud krüptovarateenuse osutaja [*väljaannete talitus: lisada viide krüptovaraturgude määrusele*];

---

47 Euroopa Parlamendi ja nõukogu 16. septembri 2009. aasta direktiiv 2009/110/EÜ, mis käsitleb e-raha asutuste asutamist ja tegevust ning usaldatavusnormatiivide täitmise järelevalvet ning millega muudetakse direktiive 2005/60/EÜ ja 2006/48/EÜ ning tunnistatakse kehtetuks direktiiv 2000/46/EÜ (ELT L 267, 10.10.2009, lk 7).

(44) „krüptovara emitent“ – artikli 3 lõike 1 punktis h määratletud krüptovara emitent [*ELT: lisada viide krüptovaraturgude määrusele*];

(45) „varapõhiste tokenite emitent“ – artikli 3 lõike 1 punktis i määratletud varapõhiste tokenite emitent [*ELT: lisada viide krüptovaraturgude määrusele*];

(46) „oluliste varapõhiste tokenite emitent“ – artikli 3 lõike 1 punktis j määratletud oluliste varapõhiste tokenite emitent [*ELT: lisada viide krüptovaraturgude määrusele*];

(47) „kriitilise tähtsusega võrdlusaluste haldur“ – määruse xx/202x artikli x punktis x määratletud kriitilise tähtsusega võrdlusaluste haldur [*ELT: lisada viide võrdlusaluste määrusele*];

(48) „ühisrahastamisteenuse osutaja“ – määruse (EL) xx/202x artikli x punktis x määratletud ühisrahastamisteenuse osutaja [*väljaannete talitus: lisada viide ühisrahastusmääruse*];

(49) „väärtpaberistamise register“ – määruse (EL) 2017/2402 artikli 2 punktis 23 määratletud väärtpaberistamise register;

(50) „mikroettevõtja“ – soovituse 2003/361/EÜ lisa artikli 2 lõikes 3 määratletud finantssektori ettevõtja.

II PEATÜKK

IKT-RISKIDE JUHTIMINE

I JAGU

Artikkel 4

Juhtimine ja organisatsioon

1. Finantssektori ettevõtjatel on sisemine juhtimis- ja kontrolliraamistik, mis tagab kõigi IKT-riskide tulemusliku ja usaldusväärse juhtimise.

2. Finantssektori ettevõtja juhtorgan määrab kindlaks ja kiidab heaks kõigi artikli 5 lõikes 1 osutatud IKT-riskide juhtimise raamistikuga seotud kokkulepete rakendamise, teeb selle üle järelevalvet ja on selle eest vastutav.

   Esimese lõigu kohaldamisel juhtorgan

   (a) omab lõppvastutust finantssektori ettevõtja IKT-riskide juhtimise eest;

   (b) määrab kõigi IKTga seotud funktsioonide puhul kindlaks selged rollid ja vastutusvaldkonnad;

   (c) määrab IKT-riski puhul kindlaks finantssektori ettevõtja sobiva taluvustaseme, nagu on osutatud artikli 5 kõike 9 punktis b;

   (d) kiidab heaks finantssektori ettevõtja IKT talitluspidevuse poliitika ja IKT taastekava, millele on osutatud artikli 10 lõigetes 1 ja 3, teeb nende üle järelevalvet ja vaatab nende rakendamise perioodiliselt läbi;

   (e) kiidab heaks ja vaatab perioodiliselt läbi IKT auditikavad, IKT auditid ja nende olulised muudatused;

(f) näeb ette ja vaatab perioodiliselt läbi sobiva eelarve finantssektori ettevõtja digitaalse tegevuskerksuse vajaduste rahuldamiseks, pidades silmas igat liiki ressursse, sealhulgas IKT-riskide teemalised koolitused ja kõigi asjaomaste töötajate oskused;

(g) kiidab heaks ja vaatab perioodiliselt läbi finantssektori ettevõtja poliitika kokkulepete kohta, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate IKT-teenuste kasutamist;

(h) on nõuetekohaselt teavitatud kolmandast isikust IKT-teenuste osutajatega sõlmitud kokkulepetest, mis käsitlevad IKT-teenuste kasutamist, kõigist asjakohastest kavandatud olulistest muudatustest, mis on seotud kolmandast isikust IKT-teenuste osutajatega, ning kõnealuste muudatuste võimalikust mõjust kriitilise tähtsusega või olulistele funktsioonidele, mille suhtes kohaldatakse kõnealuseid kokkuleppeid, ning saab muu hulgas riskianalüüside kokkuvõtteid, et hinnata nende muudatuste mõju;

(i) on nõuetekohaselt teavitatud IKTga seotud intsidentidest ja nende mõjust ning reageerimis-, taaste- ja parandusmeetmetest.

3. Finantssektori ettevõtjad, mis ei ole mikroettevõtjad, loovad rolli, mille täitja jälgib kolmandast isikust IKT-teenuste osutajatega sõlmitud kokkuleppeid IKT-teenuste kasutamise kohta, või annavad kõrgema juhtkonna liikmele vastutuse seonduva riski ja asjakohaste dokumentide järelevalve eest.

4. Juhtorgani liikmed käivad korrapäraselt erikoolitustel, et neil oleks piisavad teadmised ja oskused, et mõista ja hinnata IKT-riske ning nende mõju finantssektori ettevõtja tegevusele, ning et need teadmised ja oskused oleksid ajakohased.

II JAGU

Artikkel 5

IKT-riskide juhtimise raamistik

1. Finantssektori ettevõtjatel on usaldusväärne, laiahaardeline ja hästi dokumenteeritud IKT-riskide juhtimise raamistik, mis võimaldab neil käsitleda IKT-riske kiiresti, tõhusalt ja laiahaardeliselt ning tagada kõrgel tasemel digitaalne tegevuskerksus, mis vastab nende ärivajadustele, suurusele ja keerukusele.

2. Lõikes 1 osutatud IKT-riskide juhtimise raamistik sisaldab strateegiaid, poliitikat ja menetlusi ning IKT-protokolle ja -vahendeid, mida on vaja kaitsmaks nõuetekohaselt ja tulemuslikult kõiki asjaomaseid füüsilisi komponente ja taristuid, sealhulgas riistvara, servereid, kõiki asjaomaseid ruume, andmekeskuseid ja tundlikke määratud alasid, et tagada, et kõik need füüsilised elemendid on riskide, sealhulgas kahju ja loata juurdepääsu või kasutamise eest piisavalt kaitstud.

3. Finantssektori ettevõtjad minimeerivad IKT-riskide mõju, võttes kasutusele asjakohased strateegiad, põhimõtted, menetlused, protokollid ja vahendid, nagu on määratud kindlaks IKT-riskide juhtimise raamistikus. Nad esitavad vastavalt pädevate asutuste nõudmisele täieliku ja ajakohastatud teabe IKT-riskide kohta.

4. Lõikes 1 osutatud IKT-riskide juhtimise raamistiku osana rakendavad finantssektori ettevõtjad, mis ei ole mikroettevõtjad, kooskõlas järelevalvesuunistega tunnustatud rahvusvahelistel standarditel põhineva infoturbe halduse süsteemi ja ajakohastavad seda korrapäraselt.

5. Finantssektori ettevõtjad, mis ei ole mikroettevõtjad, tagavad, et IKT juhtimise funktsioonid, kontrollifunktsioonid ja siseauditifunktsioonid on sobivalt eraldatud vastavalt kolme kaitseliiniga mudelile või sisemisele riskijuhtimis- ja kontrollimudelile.

6. Lõikes 1 osutatud IKT-riskide juhtimise raamistik on dokumenteeritud ja seda vaadatakse läbi vähemalt kord aastas ning IKTga seotud oluliste intsidentide korral, võttes arvesse järelevalvejuhiseid või -järeldusi, mis tulenevad asjaomastest digitaalse tegevuskerksuse testidest või auditiprotsessidest. Seda täiustatakse pidevalt, lähtudes rakendamises ja järelevalves saadud õppetundidest.

7. Lõikes 1 osutatud IKT-riskide juhtimise raamistikku auditeerivad korrapäraselt IKT audiitorid, kellel on piisavad teadmised, oskused ja pädevus IKT-riskide valdkonnas. IKT-audite sagedus ja fookus vastab finantssektori ettevõtjate IKT-riskidele.

8. Rakendatakse ametlikke järelmeetmeid, sealhulgas normid IKT-auditite kriitilise tähtsusega tulemuste õigeaegse kontrollimise ja parandamise kohta, võttes arvesse auditi läbivaatamise järeldusi ja pidades nõuetekohaselt silmas finantssektori ettevõtja teenuste ja tegevuse laadi, ulatust ja keerukust.

9. Lõikes 1 osutatud IKT-riskide juhtimise raamistik sisaldab digitaalse tegevuskerksuse strateegiat, milles on sätestatud raamistiku rakendamise viis. Sel põhjusel sisaldab see meetodeid IKT-riski käsitlemiseks ja konkreetsete IKT eesmärkide saavutamiseks,

   (a) selgitades, kuidas toetab IKT-riskide juhtimise raamistik finantssektori ettevõtja äristrateegiat ja eesmärke;

   (b) määrates kooskõlas finantssektori ettevõtja riskivalmidusega kindlaks IKT-riski taluvuse taseme ning analüüsides IKT-katkestuste mõju taluvust;

   (c) seades selged infoturbe-eesmärgid;

   (d) selgitades IKT etalonarhitektuuri ja konkreetsete ärieesmärkide saavutamiseks vajalikke muudatusi;

   (e) koostades ülevaate mitmesugustest mehhanismidest, mis on võetud kasutusele IKTga seotud intsidentide mõju avastamiseks, selle eest kaitsmiseks ja selle ennetamiseks;

   (f) näidates IKTga seotud oluliste intsidentide arvu ja ennetusmeetmete tulemuslikkust;

   (g) määrates ettevõtja tasandil kindlaks tervikliku mitme IKT-teenuste osutajaga strateegia, millest on näha peamised sõltuvused kolmandast isikust IKT-teenuste osutajatest ja milles on selgitatud kolmandast isikust teenuseosutajate valiku põhjuseid;

   (h) tehes digitaalse tegevuskerksuse teste;

   (i) koostades kommunikatsioonistrateegia IKTga seotud intsidentide jaoks.

10. Kui pädevad asutused on andnud oma heakskiidu, võivad finantssektori ettevõtjad delegeerida IKT-riskide juhtimise nõuete täitmise kontrollimise ülesanded grupisisestele või -välistele ettevõtjatele.

Artikkel 6

IKT-süsteemid, -protokollid ja -vahendid

1. Finantssektori ettevõtjad kasutavad ja hoiavad ajakohasena IKT-süsteeme, -protokolle ja -vahendeid, mis vastavad järgmistele tingimustele:

   (a) süsteemid ja vahendid vastavad tegevuse elluviimist toetavate operatsioonide laadile, mitmekesisusele, keerukusele ja ulatusele;

   (b) nad on usaldusväärsed;

   (c) nad on piisavalt võimsad, et töödelda täpselt andmeid, mida on vaja õigeaegseks tegevuste elluviimiseks ja teenuste osutamiseks ning tellimuste, sõnumite või tehingumahtude tippasemega toimetulekuks vastavalt vajadusele, muu hulgas uue tehnoloogia kasutuselevõtu korral;

   (d) nad on tehnoloogiliselt kerksad, et tulla asjakohaselt toime täiendava teabe töötlemise vajadustega vastavalt sellele, mida on vaja halvenenud turutingimuste korral või muus ebasoodsas olukorras.

2. Kui finantssektori ettevõtjad kasutavad rahvusvaheliselt tunnustatud tehnilisi standardeid ja sektori juhtivaid tavasid infoturbe ja IKT sisekontrollide valdkonnas, kasutavad nad neid standardeid ja tavasid kooskõlas asjakohaste järelevalvesoovitustega nende inkorporeerimise kohta.

Artikkel 7

Kindlaksmääramine

1. Artikli 5 lõikes 1 osutatud IKT-riskide juhtimise raamistiku osana määravad finantssektori ettevõtjad kindlaks, liigitavad ja dokumenteerivad asjakohaselt kõik IKTga seotud ärifunktsioonid, neid funktsioone toetavad teabevarad ning IKT-süsteemide konfiguratsioonid ja seosed sisemiste ja väliste IKT-süsteemidega. Finantssektori ettevõtjad vaatavad vastavalt vajadusele ja vähemalt kord aastas läbi teabevarade liigituse ja asjakohaste dokumentide asjakohasuse.

2. Finantssektori ettevõtjad teevad jooksvalt kindlaks kõik IKT-riskide allikad, eelkõige riskid, mis tulenevad muudest finantssektori ettevõtjatest või nende kaudu, ning hindavad küberohte ja IKT haavatavusi, mis on olulised nende IKTga seotud ärifunktsioonide ja teabevarade jaoks. Finantssektori ettevõtjad vaatavad korrapäraselt ja vähemalt kord aastas läbi neid mõjutavad riskistsenaariumid.

3. Finantssektori ettevõtjad, mis ei ole mikroettevõtjad, teevad riskihindamise alati, kui võrgu- ja infosüsteemide taristus, protsessides või menetlustes, mis mõjutavad nende funktsioone, tugiprotsesse või teabevarasid, tehakse oluline muudatus.

4. Finantssektori ettevõtjad teevad kindlaks kõik IKT-süsteemide kontod, muu hulgas kaugasukohtades, võrguressursid ja riistvara ning kaardistavad füüsilised seadmed, mida käsitatakse olevat kriitilise tähtsusega. Nad kaardistavad IKT-varade konfiguratsiooni ning erinevate IKT-varade vahelised seosed ja sõltuvused.

5. Finantssektori ettevõtjad teevad kindlaks ja dokumenteerivad kõik protsessid, mis sõltuvad kolmandast isikust IKT-teenuste osutajatest, ning seosed kolmandast isikust IKT-teenuste osutajatega.

6. Lõigete 1, 4 ja 5 kohaldamisel on finantssektori ettevõtjatel asjakohane varu, mida nad ajakohastavad korrapäraselt.

7. Finantssektori ettevõtjad, mis ei ole mikroettevõtjad, teevad korrapäraselt ja vähemalt kord aastas spetsiifilisi IKT-riskide hindamisi, milles käsitletakse kõiki IKT pärandsüsteeme, eelkõige enne ja pärast vanade ja uute tehnoloogiate, rakenduste või süsteemide ühendamist.

Artikkel 8

Kaitse ja ennetus

1. Selleks et piisavalt kaitsta IKT-süsteeme ja luua reageerimismeetmed, jälgivad ja kontrollivad finantssektori ettevõtjad pidevalt IKT-süsteemide ja -vahendite toimimist ning minimeerivad kõnealuste riskide mõju, võttes kasutusele asjakohased IKT turvalisuse vahendid, põhimõtted ja menetlused.

2. Finantssektori ettevõtjad koostavad, hangivad ja rakendavad IKT turvalisuse strateegiaid, põhimõtteid, menetlusi, protokolle ja vahendeid, mille eesmärk on eelkõige tagada IKT-süsteemide kerksus, jätkuvus ja kättesaadavus ning ranged andmete turvalisuse, konfidentsiaalsuse ja tervikluse standardid nii nende jõudeoleku, kasutamise kui ka edastamise jaoks.

3. Lõikes 2 osutatud eesmärkide saavutamiseks kasutavad finantssektori ettevõtjad tipptasemel IKT-tehnoloogiaid ja -protsesse, mis

   (a) tagavad teabeedastusvahendite turvalisuse;

   (b) minimeerivad andmelaostuse või -kao riski, loata juurdepääsu võimaluse ja tehnilised puudused, mis võivad takistada äritegevust;

   (c) hoiavad ära teabe lekkimise;

   (d) tagavad, et teave on kaitstud halva haldamise või töötlemisega seotud riskide, sealhulgas ebapiisava dokumenteerimise eest.

4. Finantssektori ettevõtjad teevad artikli 5 lõikes 1 osutatud IKT-riskide juhtimise raamistiku osana järgmist:

   (a) töötavad välja ja dokumenteerivad infoturbepoliitika, milles määratakse kindlaks normid nende ja nende klientide IKT-ressursside, andmete ja teabevarade konfidentsiaalsuse, tervikluse ja kättesaadavuse kaitsmiseks;

   (b) kasutavad riskipõhist lähenemisviisi, loovad usaldusväärse võrgu- ja taristuhalduse, kasutades sobivaid tehnikaid, meetodeid ja protokolle, muu hulgas võttes kasutusele automatiseeritud mehhanismid, et isoleerida küberrünnete korral nendest mõjutatud teabevarad;

   (c) rakendavad poliitikameetmeid, mille kohaselt antakse füüsiline ja virtuaalne juurdepääs IKT-süsteemi ressurssidele ning andmetele ainult siis, kui seda on vaja õiguspäraste ja heakskiidetud funktsioonide ja tegevuste jaoks, ning kehtestavad sel eesmärgil poliitika, menetlused ja kontrollid, mis käsitlevad pääsuõigusi ja nende usaldusväärset haldamist;

   (d) rakendavad poliitikameetmeid ja protokolle tugeva autentimismehhanismi jaoks, lähtudes asjakohastest standarditest ja spetsiaalsetest kontrollisüsteemidest, millega takistatakse juurdepääsu krüptovõtmetele, mille puhul andmed krüptitakse heakskiidetud andmete liigitamise tulemuste ja riskihindamise protsesside põhjal;

(e) rakendavad IKT-muudatuste (sh tark-, riist- ja püsivara komponentide muudatused, süsteemi- või turvamuudatused) juhtimise valdkonnas poliitikameetmeid, menetlusi ja kontrolle, mis põhinevad riskihindamisel ja on lahutamatu osa finantssektori ettevõtja üldisest muudatuste juhtimise protsessist, eesmärgiga tagada, et kõik IKT-süsteemide muudatused on kontrollitult registreeritud, testitud, hinnatud, heakskiidetud, rakendatud ja kontrollitud;

(f) omavad sobivat ja laiahaardelist poliitikat paikade ja uuenduste jaoks.

Punkti b kohaldamisel kujundavad finantssektori ettevõtjad võrguühenduste taristu viisil, mis võimaldab need silmapilkselt katkestada, ning tagavad nende rühmitamise ja segmenteerimise, et minimeerida ja takistada ülekandumist, eelkõige omavahel seotud finantsprotsesside puhul.

Punkti e kohaldamisel kiidavad asjaomased juhtimisliinid IKT-muudatuste juhtimise protsessi heaks ja selle protsessi puhul on olemas konkreetsed protokollid hädaolukorras muudatuste tegemiseks.

Artikkel 9

Avastamine

1. Finantssektori ettevõtjatel on kooskõlas artikliga 15 mehhanismid, mis võimaldavad kohe avastada anomaalset tegevust, sealhulgas IKT-võrgu jõudluse probleeme ja IKTga seotud intsidente, ning leida kõik võimalikud olulised nõrgad lülid.

   Kõiki esimeses lõigus osutatud avastamismehhanisme testitakse korrapäraselt kooskõlas artikliga 22.

2. Lõikes 1 osutatud avastamismehhanism võimaldab mitmetasandilist kontrolli, määrab kindlaks alarmiläved ja -kriteeriumid, mis käivitavad IKTga seotud intsidendi avastamise ja IKTga seotud intsidendile reageerimise protsessid, ning loovad automaatsed häiremehhanismid asjaomastele töötajatele, kes tegelevad IKTga seotud intsidentidele reageerimisega.

3. Võttes nõuetekohaselt arvesse oma suurust ning äri- ja riskiprofiile, näevad finantssektori ettevõtjad ette piisavad ressursid ja piisava suutlikkuse, et jälgida kasutajate tegevust, IKT anomaaliate esinemist ja IKTga seotud intsidente, eriti küberründe id.

4. Artikli 2 lõike 1 punktis l osutatud finantssektori ettevõtjatel on lisaks süsteemid, mis võimaldavad tulemuslikult kontrollida kauplemisaruannete terviklikkust, märgata andmete väljajäämist ja ilmseid vigu ning nõuda vigaste aruannete uuesti esitamist.

Artikkel 10

Reageerimine ja taastamine

1. Finantssektori ettevõtjad kehtestavad artikli 5 lõikes 1 osutatud IKT-riskide juhtimise raamistiku osana ja artiklis 7 sätestatud kindlaksmääramise nõuete põhjal spetsiaalse ja laiahaardelise IKT talitluspidevuse poliitika, mis on finantssektori ettevõtja operatiivse talitluspidevuse poliitika lahutamatu osa.

2. Finantssektori ettevõtjad rakendavad lõikes 1 osutatud IKT talitluspidevuse poliitikat, kasutades spetsiaalseid, asjakohaseid ja dokumenteeritud kokkuleppeid, kavasid, menetlusi ja mehhanisme, mille eesmärk on

(a) registreerida kõik IKTga seotud intsidendid;

(b) tagada finantssektori ettevõtja kriitilise tähtsusega funktsioonide jätkumine;

(c) reageerida kõigile IKTga seotud intsidentidele (eelkõige, kuid mitte ainult küberrünnetele) ja lahendada need kiiresti, asjakohaselt ja tulemuslikult viisil, mis piirab kahju ning prioriseerib tegevuse jätkamist ja taastemeetmeid;

(d) aktiveerida viivitamata spetsiaalsed kavad, et võimaldada piiramismeetmeid, -protsesse ja -tehnoloogiaid, mis vastavad igale IKTga seotud intsidendi liigile ning hoiavad ära suurema kahju, samuti kohandatud reageerimis- ja taastamismenetlused, mis on kehtestatud kooskõlas artikliga 11;

(e) hinnata esialgset mõju, kahjustust ja kahju;

(f) näha ette kommunikatsiooni- ja kriisiohjemeetmed, mis tagavad, et ajakohastatud teave edastatakse kooskõlas artikliga 13 kõigile asjaomastele asutusesisestele töötajatele ja välistele sidusrühmadele ning kooskõlas artikliga 17 pädevatele asutustele.

3. Finantssektori ettevõtjad rakendavad artikli 5 lõikes 1 osutatud IKT-riskide juhtimise raamistiku osana seonduvat IKT taastekava, mille kohta tehakse muude kui mikroettevõtjate puhul sõltumatu audit.

4. Finantssektori ettevõtjad koostavad sobivad IKT talitluspidevuse kavad ning säilitavad ja testivad neid perioodiliselt, eelkõige seoses kriitilise tähtsusega või oluliste funktsioonidega, mis on antud edasi või mille kohta on sõlmitud kolmandast isikust IKT-teenuste osutajatega kokkulepped.

5. Finantssektori ettevõtjad teevad oma laiahaardelise IKT-riskide juhtimise raames järgmist:

(a) testivad IKT talitluspidevuse poliitikat ja IKT taastekava vähemalt kord aastas ja pärast IKT-süsteemide olulisi muudatusi;

(b) testivad kooskõlas artikliga 13 koostatud kriisikommunikatsioonikavasid.

Punkti a kohaldamisel lisavad finantssektori ettevõtjad, mis ei ole mikroettevõtjad, testimiskavadesse stsenaariumid, mis käsitlevad küberründeid ja esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust, varundamist ja varurajatisi, mida on vaja artiklis 11 sätestatud kohustuste täitmiseks.

Finantssektori ettevõtjad vaatavad oma IKT talitluspidevuse poliitika ja IKT taastekava korrapäraselt läbi, võttes arvesse kooskõlas esimese lõiguga tehtud testide tulemusi ja soovitusi, mis tulenevad auditikontrollidest või järelevalvest.

6. Finantssektori ettevõtjatel, mis ei ole mikroettevõtjad, on kriisiohjefunktsioon, mis kehtestab IKT talitluspidevuse poliitika või IKT taastekava aktiveerimisel selged menetlused sisemise ja välise kriisikommunikatsiooni juhtimiseks kooskõlas artikliga 13.

7. Finantssektori ettevõtjad dokumenteerivad oma tegevused enne katkestusi ja nende ajal, kui aktiveeritakse IKT talitluspidevuse poliitika või IKT taastekava. Need dokumendid on kergesti kättesaadavad.

8. Artikli 2 lõike 1 punktis f osutatud finantssektori ettevõtjad esitavad pädevatele asutustele vaatlusalusel perioodil tehtud IKT talitluspidevuse testide või muude sarnaste testide tulemuste koopiad.

9. Finantssektori ettevõtjad, mis ei ole mikroettevõtjad, teavitavad pädevaid asutusi kõigist IKT-katkestuste tekitatud kuludest ja kahjudest ning IKTga seotud intsidentidest.

Artikkel 11

Varunduspoliitika ja taastemeetodid

1. Selleks et tagada IKT-süsteemide taastamine minimaalse seisuaja ja piiratud katkestusega, töötab finantssektori ettevõtja IKT-riskide juhtimise raamistiku osana välja

   (a) varunduspoliitika, milles täpsustatakse varundatavate andmete maht ja minimaalne varundamissagedus, lähtudes teabe kriitilisusest või andmete tundlikkusest;

   (b) taastemeetodid.

2. Varusüsteemid alustavad töötlust põhjendamatu viivituseta, välja arvatud juhul, kui see seaks ohtu võrgu- ja infosüsteemide turvalisuse või andmete tervikluse või konfidentsiaalsuse.

3. Varundatud andmete taastamisel oma süsteemide abil kasutavad finantssektori ettevõtjad IKT-süsteeme, mille töökeskkond on põhisüsteemi omast erinev, mis ei ole viimasega otseselt ühendatud ja mis on turvaliselt kaitstud loata juurdepääsu või IKT korruptsiooni eest.

   Artikli 2 lõike 1 punktis g osutatud finantssektori ettevõtjate puhul võimaldavad sellised kavad taastada katkestuse ajal kõik tehingud, et keskne vastaspool saaks oma tegevust kindlalt jätkata ja viia arveldamine lõpule kavandatud kuupäeval.

4. Finantssektori ettevõtjatel on IKT-alane varusuutlikkus koos ärivajaduste rahuldamiseks piisavate ja asjakohaste ressursside, võimete, funktsioonidega.

5. Artikli 2 lõike 1 punktis f osutatud finantssektori ettevõtjad tagavad, et neil või nende kolmandast isikust IKT-teenuste osutajatel on vähemalt üks varutöötluskoht, millel on ärivajaduste rahuldamiseks piisavad ja asjakohased ressursid, võimekus, funktsioonid ja personalikorraldus.

   Varutöötluskoht:

   (a) asub peamisest töötluskohast geograafiliselt eemal, et tagada nende erinev riskiprofiil ja vältida, et varutöötluskohta kahjustab peamisele töötluskohale mõju avaldanud sündmus;

   (b) suudab sarnaselt peamise töötluskohaga tagada kriitilise tähtsusega teenuste järjepidevuse või sellise teenuste taseme, mida on vaja, et finantssektori ettevõtja täidaks oma kriitilise tähtsusega funktsioone vastavalt taaste-eesmärkidele;

   (c) on finantssektori ettevõtja töötajatele koheselt ligipääsetav, et tagada kriitilise tähtsusega teenuste jätkumine juhul, kui peamist töötluskohta ei saa enam kasutada.

6. Iga funktsiooni taasteaja ja sihtseisu kindlaksmääramisel võtavad finantssektori ettevõtjad arvesse võimalikku üldist mõju turu tõhususele. Selliste ajaliste eesmärkidega tagatakse, et äärmuslike stsenaariumide korral tagatakse teenused kokkulepitud tasemel.

7. IKTga seotud intsidendist taastumisel teevad finantssektori ettevõtjad mitmeid kontrolle, sealhulgas kooskõlastavad võrdlemised, et tagada kõrgeimal tasemel andmete terviklus. Neid kontrolle tehakse ka välistelt sidusrühmadelt saadud andmete rekonstrueerimisel, et tagada kõigi andmete kooskõla eri süsteemides.

Artikkel 12

Õppimine ja areng

1. Finantssektori ettevõtjatel peab olema nende suurusele, äri- ja riskiprofiilile vastav suutlikkus ja personal, et koguda teavet haavatavuste, küberohtude ja IKTga seotud intsidentide, eelkõige küberrünnete kohta, ning analüüsida nende tõenäolist mõju nende digitaalsele tegevuskerksusele.

2. Finantssektori ettevõtjad kehtestavad IKTga seotud intsidentide järgsed kontrollid, mida tehakse pärast põhitegevuse olulisi IKT-häireid, analüüsides häire põhjuseid ja tehes kindlaks, mida on vaja IKT-operatsioonides või artiklis 10 osutatud IKT talitluspidevuse poliitikas muuta.

   Muudatuste tegemisel peavad finantssektori ettevõtjad (v.a mikroettevõtjad) teatama nendest pädevatele asutustele.

   Esimeses lõigus osutatud IKTga seotud intsidentide järgse kontrolli käigus tehakse kindlaks, kas järgiti kehtestatud korda ja kas võetud meetmed olid tulemuslikud, sealhulgas seoses järgmisega:

   (a) turvahoiatustele reageerimise ning IKTga seotud intsidentide mõju ja nende tõsiduse kindlakstegemise kiirus;

   (b) kriminalistika-analüüsi kvaliteet ja kiirus;

   (c) intsidendi eskaleerimise tulemuslikkus finantssektori ettevõtjas;

   (d) sise- ja välissuhtluse tulemuslikkus.

3. Õppetunnid, mis on saadud artiklite 23 ja 24 kohaselt läbi viidud digitaalse tegevuskerksuse testimise käigus ning reaalses elus toimunud IKTga seotud intsidentidest (eelkõige küberründed) ja talitluspidevuse või taastekavade käivitamisega seotud probleemidest, samuti vastaspooltega vahetatud ja järelevalve käigus hinnatud asjakohane teave inkorporeeritakse nõuetekohaselt jooksvalt IKT-riskide hindamise protsessi. Nende tulemuste põhjal vaadatakse asjakohaselt läbi artikli 5 lõikes 1 osutatud IKT-riski juhtimise raamistiku vastavad osad.

4. Finantssektori ettevõtjad jälgivad artikli 5 lõikes 9 sätestatud digitaalse kerksuse strateegia rakendamise tulemuslikkust. Nad kaardistavad, kuidas on IKT-riskid aja jooksul arenenud, analüüsivad IKTga seotud intsidentide, eelkõige küberrünnete sagedust, liiki, ulatust ja muutusi ning nende mustreid, et mõista IKT-riski taset ning parandada finantssektori ettevõtja küberküpsust ja valmisolekut.

5. Kõrgema astme IKT-töötajad esitavad juhtorganile vähemalt kord aastas aruande lõikes 3 osutatud leidude kohta ja annavad soovitusi.

6. Finantssektori ettevõtjad töötavad oma personali koolituskavade raames kohustuslike moodulitena välja IKT turvateadlikkuse suurendamise programmid ja tegevuskerksuse koolitused. Neid rakendatakse kõigi töötajate ja kõrgema juhtkonna liikmete suhtes.

Finantssektori ettevõtjad jälgivad pidevalt tehnoloogia arengut, muu hulgas selleks, et mõista uue tehnoloogia võimalikku mõju IKT turvanõuetele ja digitaalsele tegevuskerksusele. Nad hoiavad end kursis uusimate IKT-riski juhtimise protsessidega, võideldes tõhusalt praeguste või uute küberründevormide vastu.

Artikkel 13

Kommunikatsioon

1. Artikli 5 lõikes 1 osutatud IKT-riski juhtimise raamistiku alusel peavad finantssektori ettevõtjad kehtestama kommunikatsioonikavad, mis võimaldavad IKTga seotud intsidente või olulisi haavatavusi teha klientidele ja vastaspooltele ning vajaduse korral ka üldsusele teatavaks vastutustundlikult.

2. Artikli 5 lõikes 1 osutatud IKT-riski juhtimise raamistiku alusel rakendavad finantssektori ettevõtjad personali ja väliseid sidusrühmi puudutavat kommunikatsioonipoliitikat. Personali kommunikatsioonipoliitikas võetakse arvesse vajadust eristada töötajaid, kes osalevad IKT-riski juhtimises (eelkõige reageerimises ja taastes) ja töötajaid, keda tuleb teavitada.

3. Vähemalt ühele isikule ettevõtjas tehakse ülesandeks rakendada IKTga seotud intsidentide kommunikatsioonistrateegiat ning täita sel eesmärgil avaliku ja meediaga suhtleva pressiesindaja rolli.

Artikkel 14

IKT-riski juhtimise vahendite, meetodite, protsesside ja põhimõtete edasine ühtlustamine

Euroopa Pangandusjärelevalve (EBA), Euroopa Väärtpaberiturujärelevalve (ESMA) ning Euroopa Kindlustus- ja Tööandjapensionide Järelevalve (EIOPA) töötavad Euroopa Liidu Küberturvalisuse Ametiga (ENISA) konsulteerides välja regulatiivsete tehniliste standardite eelnõud järgmistel eesmärkidel:

(a) määrata kindlaks artikli 8 lõikes 2 osutatud IKT turvapõhimõtetesse, menetlustesse, protokollidesse ja vahenditesse lisatavad elemendid, et tagada võrkude turvalisus, võimaldada piisavaid kaitsemeetmeid sissetungide ja andmete väärkasutamise vastu, säilitada andmete autentsus ja terviklus, sealhulgas krüptomeetodeid kasutades, ning tagada andmete täpne ja kiire suuremate häireteta ülekandmine;

(b) näha ette, kuidas artikli 8 lõikes 2 osutatud IKT turvapõhimõtete, -menetluste ja -vahenditega inkorporeeritakse turvakontrollid süsteemidesse algusest peale (sisseprojekteeritud turve) ning võimaldatakse kohanduda muutuvate ohtudega ja kasutada süvakaitsetehnoloogiat;

(c) täpsustada artikli 8 lõike 4 punktis b osutatud asjakohaseid tehnikaid, meetodeid ja protokolle;

(d) töötada välja artikli 8 lõike 4 punktis c osutatud pääsuõiguste halduse kontrolli täiendavad komponendid ja nendega seotud personalipoliitika, milles määratakse kindlaks pääsuõigused, õiguste andmise ja tühistamise menetlused, IKT-riskidega seotud anomaalse käitumise jälgimine asjakohaste näitajate alusel, sealhulgas võrgu kasutamise mustrite, tundide, IT-tegevuse ja tundmatute seadmete alusel;

(e) arendada edasi artikli 9 lõikes 1 sätestatud elemente, mis võimaldavad kõrvalekaldeid kiiresti avastada, ning artikli 9 lõikes 2 osutatud kriteeriume,

mis käivitavad IKTga seotud intsidentide tuvastamise ja neile reageerimise protsessid;

(f) täpsustada artikli 10 lõikes 1 osutatud IKT talitluspidevuse poliitika komponente;

(g) täpsustada artikli 10 lõikes 5 osutatud IKT talitluspidevuse kavade testimist tagamaks, et selles võetakse nõuetekohaselt arvesse stsenaariume, mille korral kriitilise tähtsusega või olulise funktsiooni täitmise kvaliteet halveneb vastuvõetamatu tasemeni või funktsiooni täitmine ebaõnnestub, ning võetakse nõuetekohaselt arvesse mis tahes asjaomase kolmandast isikust IKT-teenuse osutaja maksejõuetuse või muude tõrgete võimalikku mõju ja vajaduse korral poliitilisi riske vastavate teenuseosutajate jurisdiktsioonides;

(h) täpsustada artikli 10 lõikes 3 osutatud IKT taastekava komponente.

EBA, ESMA ja EIOPA esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*ELT: palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus võtta vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas vastavalt määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10 kuni 14.

III PEATÜKK

IKTga SEOTUD INTSIDENDID HALDAMINE, LIIGITAMINE ja ARUANDLUS

Artikkel 15

IKTga seotud intsidentide haldamise protsess

1. Finantssektori ettevõtjad kehtestavad IKTga seotud intsidentide haldamise protsessi nende avastamiseks, haldamiseks ja nendest teatamiseks ja rakendavad seda, samuti määravad kindlaks hoiatustena toimivad varajase hoiatamise näitajad.

2. Finantssektori ettevõtjad kehtestavad asjakohased protsessid, et tagada IKTga seotud intsidentide järjepidev ja integreeritud jälgimine, käsitlemine ja järelmeetmed, et tagada algpõhjuste kindlakstegemine ja kõrvaldamine selliste intsidentide edaspidiseks vältimiseks.

3. Lõikes 1 osutatud IKTga seotud intsidentide haldamise protsess hõlmab järgmist:

(a) menetluste kehtestamine IKTga seotud intsidentide tuvastamiseks, jälgimiseks, logimiseks, kategoriseerimiseks ja liigitamiseks vastavalt nende prioriteetsusele ning mõjutatud teenuste tõsidusele ja kriitilisusele kooskõlas artikli 16 lõikes 1 osutatud kriteeriumidega;

(b) selliste rollide ja ülesannete määramine, mis tuleb aktiveerida eri liiki IKTga seotud intsidentide ja stsenaariumide puhul;

(c) kommunikatsioonikavade koostamine artikli 13 kohaseks töötajate, väliste sidusrühmade ja meedia teavitamiseks ning klientide teavitamiseks asutusesisese eskaleerimiskorra kehtestamine, mis hõlmab IKTga seotud

kliendikaebusi, ning vajaduse korral teabe andmiseks vastaspooltena tegutsevatele finantssektori ettevõtjatele;

(d) selle tagamine, et olulistest IKTga seotud intsidentidest teatatakse asjaomasele kõrgemale juhtkonnale, ning juhtorgani teavitamine suurematest IKTga seotud intsidentidest, selgitades IKTga seotud intsidentide mõju, nendele reageerimist ja nende tõttu kehtestatud lisakontrolle;

(e) IKTga seotud intsidentidele reageerimise menetluste kehtestamine, et leevendada mõju ja tagada teenuste õigeaegne taastamine ja turvalisus.

Artikkel 16

IKTga seotud intsidentide liigitamine

1. Finantssektori ettevõtjad liigitavad IKTga seotud intsidendid ja määravad nende mõju kindlaks järgmiste kriteeriumide alusel:

(a) IKTga seotud intsidendi põhjustatud häirest mõjutatud kasutajate või finantssektori vastaspoolte arv ning see, kas IKTga seotud intsident on kahjustanud mainet;

(b) IKTga seotud intsidendi kestus, sealhulgas teenuse seisaku aeg;

(c) IKTga seotud intsidendist mõjutatud geograafilised piirkonnad, eriti kui see mõjutab rohkem kui kahte liikmesriiki;

(d) IKTga seotud intsidendiga kaasnev andmekadu, näiteks tervikluse, konfidentsiaalsuse või kättesaadavuse kadu;

(e) kui suurt mõju avaldab IKTga seotud intsident finantssektori ettevõtja IKT-süsteemidele;

(f) mõjutatud teenuste, sealhulgas finantssektori ettevõtja tehingute ja tegevuse kriitilisus;

(g) IKTga seotud intsidendi nii absoluutne kui ka suhteline majanduslik mõju.

2. Euroopa järelevalveasutused töötavad Euroopa järelevalveasutuste ühiskomitee (edaspidi „ühiskomitee“) kaudu ning pärast konsulteerimist Euroopa Keskpanga (EKP) ja ENISAga välja ühiste regulatiivsete tehniliste standardite eelnõu, milles täpsustatakse järgmist:

(a) lõikes 1 sätestatud kriteeriumid, sealhulgas olulisuse läved selliste oluliste IKTga seotud intsidentide kindlaksmääramiseks, mille suhtes kohaldatakse artikli 17 lõikes 1 sätestatud teatamiskohustust;

(b) kriteeriumid, mida pädevad asutused peavad kohaldama, et hinnata oluliste IKTga seotud intsidentide olulisust teiste liikmesriikide jurisdiktsioonides, ning IKTga seotud intsidente käsitlevate aruannete üksikasjad, mida jagatakse teiste pädevate asutustega vastavalt artikli 17 lõigetele 5 ja 6.

3. Lõikes 2 osutatud ühiste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse rahvusvahelisi standardeid ning ENISA väljatöötatud ja avaldatud spetsifikaate, sealhulgas vajaduse korral muude majandussektorite spetsifikaate.

Euroopa järelevalveasutused esitavad kõnealused ühiste regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*väljaannete talitus*: *palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu lõikes 2 osutatud regulatiivsed tehnilised standardid kooskõlas määruse (EL) nr 1093/2010, (EL) nr 1094/2010 või (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 17

IKTga seotud olulistest intsidentidest teatamine

1. Finantssektori ettevõtjad teatavad olulistest IKTga seotud intsidentidest artiklis 41 osutatud asjaomasele pädevale asutusele lõikes 3 sätestatud tähtaja jooksul.

   Esimese lõigu kohaldamisel koostavad finantssektori ettevõtjad pärast kogu asjakohase teabe kogumist ja analüüsimist intsidendi kohta aruande, kasutades artiklis 18 osutatud vormi, ning esitavad selle pädevale asutusele.

   Aruanne sisaldab kogu teavet, mida pädev asutus vajab, et teha kindlaks olulise IKTga seotud intsidendi tähtsus ja hinnata võimalikku piiriülest mõju.

2. Kui oluline IKTga seotud intsident mõjutab või võib mõjutada teenuse kasutajate ja klientide finantshuve, teavitavad finantssektori ettevõtjad põhjendamatu viivituseta oma teenuse kasutajaid ja kliente olulisest IKTga seotud intsidendist ning annavad neile võimalikult kiiresti teada kõigist meetmetest, mis on võetud sellise intsidendi kahjuliku mõju leevendamiseks.

3. Finantssektori ettevõtjad peavad artiklis 41 osutatud pädevale asutusele esitama:

   (a) esialgse teate viivitamata, kuid hiljemalt tööpäeva lõpuks, või kui oluline IKTga seotud intsident leidis aset hiljem kui 2 tundi enne tööpäeva lõppu, siis 4 tunni jooksul alates järgmise tööpäeva algusest, või kui teatamiskanalid ei ole kättesaadavad, siis niipea, kui need on kättesaadavad;

   (b) vahearuande hiljemalt nädal pärast punktis a osutatud esialgset teadet, mille järel vajaduse korral saadetakse ajakohastatud teated iga kord, kui on uut teavet, samuti pädeva asutuse konkreetse taotluse korral;

   (c) lõpparuande, kui algpõhjuste analüüs on lõpule viidud, olenemata sellest, kas leevendusmeetmeid on juba rakendatud või mitte, ja kui hinnangud saab asendada tegelike mõjunäitajatega, kuid mitte hiljem kui üks kuu pärast esialgse aruande saatmist.

4. Finantssektori ettevõtjad võivad delegeerida käesoleva artikli kohased teatamiskohustused kolmandast isikust teenuseosutajale üksnes pärast seda, kui selle on heaks kiitnud artiklis 41 osutatud asjaomane pädev asutus.

5. Pärast lõikes 1 osutatud aruande saamist esitab pädev asutus põhjendamatu viivituseta intsidendi üksikasjad:

   (a) vastavalt kas EBA-le, ESMA-le või EIOPA-le;

   (b) EKP-le, kui see on asjakohane artikli 2 lõike 1 punktides a, b ja c osutatud finantssektori ettevõtjate puhul, ning

   (c) direktiivi (EL) 2016/1148 artikli 8 kohaselt määratud ühtsele kontaktpunktile.

6. EBA, ESMA või EIOPA ning EKP hindavad olulise IKTga seotud intsidendi olulisust teiste asjaomaste avaliku sektori asutuste jaoks ning teavitavad neid sellest võimalikult kiiresti. EKP teavitab Euroopa Keskpankade Süsteemi liikmeid maksesüsteemi jaoks asjakohastest probleemidest. Selle teavituse alusel võtavad pädevad asutused vajaduse korral kõik vajalikud meetmed finantssüsteemi stabiilsuse viivitamatuks kaitsmiseks.

Artikkel 18

Aruannete sisu ja vormide ühtlustamine

1. Euroopa järelevalveasutused töötavad ühiskomitee kaudu ning pärast ENISA ja EKPga konsulteerimist välja:

   (a) ühiste regulatiivsete tehniliste standardite eelnõu, et:

      (1) määrata kindlaks olulistest IKTga seotud intsidentidest teatamise aruannete sisu;

      (2) täpsustada tingimusi, mille alusel võivad finantssektori ettevõtjad delegeerida käesolevas peatükis sätestatud teatamiskohustused kolmandast isikust teenuseosutajale, kui pädev asutus on selle eelnevalt heaks kiitnud;

   (b) ühiste rakenduslike tehniliste standardite eelnõu, et kehtestada standardvormid, -mallid ja -menetlused, mida finantssektori ettevõtjad kasutavad olulistest IKTga seotud intsidentidest teatamiseks.

   Euroopa järelevalveasutused esitavad lõike 1 punktis a osutatud ühiste regulatiivsete tehniliste standardite eelnõu ja lõike 1 punktis b osutatud ühiste rakenduslike tehniliste standardite eelnõu komisjonile hiljemalt xx 202x [*väljaannete talitus*: *palun lisada kuupäev: 1 aasta pärast jõustumist*].

   Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu lõike 1 punktis a osutatud ühised regulatiivsed tehnilised standardid kooskõlas määruse (EL) nr 1093/2010, (EL) nr 1095/2010 või (EL) nr 1094/2010 artiklitega 10–14.

   Komisjonile antakse õigus võtta vastu esimese lõike 1 punktis b osutatud ühised rakenduslikud tehnilised standardid kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1095/2010 ja määruse (EL) nr 1094/2010 artikliga 15.

Artikkel 19

IKTga seotud olulistest intsidentidest teatamise tsentraliseerimine

1. Euroopa järelevalveasutused koostavad ühiskomitee kaudu ning EKP ja ENISAga konsulteerides ühisaruande, milles hinnatakse intsidentidest teatamise edasise tsentraliseerimise võimalikkust, milleks tuleks luua finantssektori ettevõtjate poolt IKTga seotud olulistest intsidentidest teatamiseks ühine ELi keskus. Aruandes analüüsitakse, kuidas hõlbustada IKTga seotud intsidentidest teatamist, vähendada sellega seotud kulusid ja toetada temaatilisi analüüse, et suurendada järelevalvealast ühtsust.

2. Lõikes 1 nimetatud aruandes tuleb käsitleda vähemalt järgmisi teemasid:

   (a) sellise ELi keskuse loomise eeltingimused;

   (b) kasu, takistused ja võimalikud riskid;

(c) tegevuse juhtimise elemendid;

(d) liikmesuse tingimused;

(e) finantssektori ettevõtjate ja riiklike pädevate asutuste ELi keskusele juurdepääsu üksikasjad;

(f) selliste finantskulude esialgne hinnang, mis kaasnevad ELi keskust toetava tegevusplatvormi loomisega (sealhulgas nõutavad eksperditeadmised).

3. Euroopa järelevalveasutused esitavad lõikes 1 osutatud aruande komisjonile, Euroopa Parlamendile ja nõukogule hiljemalt xx 202x [*ELT: palun lisada kuupäev: 3 aastat pärast jõustumist*].

Artikkel 20

Järelevalveasutuste tagasiside

1. Artikli 17 lõikes 1 osutatud aruande saamisel kinnitab pädev asutus teate kättesaamist ja esitab võimalikult kiiresti kogu vajaliku tagasiside või suunised finantssektori ettevõtjale, et eelkõige arutada parandusmeetmeid ettevõtja tasandil või viise kahjuliku mõju minimeerimiseks sektorite lõikes.

2. Euroopa järelevalveasutused esitavad ühiskomitee kaudu kord aastas anonüümitud koondaruande pädevatelt asutustelt saadud IKTga seotud intsidentide teadete kohta, milles esitatakse vähemalt IKTga seotud oluliste intsidentide arv, nende laad, mõju finantssektori ettevõtjate või klientide tegevusele, kulud ja võetud parandusmeetmed.

Euroopa järelevalveasutused annavad välja hoiatusi ja koostavad kvaliteetset statistikat, et toetada IKT-ohtude ja haavatavuse hindamist.

IV PEATÜKK

DIGITAALSE TEGEVUSKERKSUSE TESTIMINE

Artikkel 21

Digitaalse tegevuskerksuse testimise üldnõuded

1. Et hinnata valmisolekut IKTga seotud intsidentideks, tuvastada nõrgad kohad, puudused või lüngad digitaalses tegevuskerksuses ning rakendada viivitamata parandusmeetmeid, loovad finantssektori ettevõtjad artiklis 5 osutatud IKT-riski juhtimise raamistiku lahutamatu osana usaldusväärse ja tervikliku digitaalse tegevuskerksuse testimise programmi ning säilitavad ja vaatavad selle läbi, võttes nõuetekohaselt arvesse oma suurust ning äri- ja riskiprofiile.

2. Digitaalse tegevuskerksuse testimise programm peab hõlmama mitmesuguseid hindamisi, teste, meetodeid, tavasid ja vahendeid, mida kohaldatakse kooskõlas artiklitega 22 ja 23.

3. Finantssektori ettevõtjad järgivad lõikes 1 osutatud digitaalse tegevuskerksuse testimise programmi puhul riskipõhist lähenemisviisi, võttes arvesse IKT-riskide muutuvat laadi, spetsiifilisi riske, millele finantssektori ettevõtja on või võib olla avatud, teabevarade ja osutatud teenuste kriitilisust, aga ka kõiki muid tegureid, mida finantssektori ettevõtja peab asjakohaseks.

4. Finantssektori ettevõtjad tagavad, et teste teevad sõltumatud isikud – sisesed või välised.

5. Finantssektori ettevõtjad kehtestavad menetlused ja põhimõtted, et prioriseerida, liigitada ja kõrvaldada kõik testide käigus tuvastatud probleemid, ning kehtestavad sisemised valideerimismeetodid, et teha kindlaks, kas kõik tuvastatud nõrkused, puudused või lüngad on täielikult kõrvaldatud.

6. Finantssektori ettevõtjad testivad kõiki kriitilise tähtsusega IKT-süsteeme ja -rakendusi vähemalt kord aastas.

Artikkel 22

IKT-vahendite ja -süsteemide testimine

1. Artiklis 21 osutatud digitaalse tegevuskerksuse testimise programmiga nähakse ette kõik asjakohased testid, sealhulgas haavatavuse hindamised ja skaneerimised, avatud lähtekoodiga tarkvara analüüsid, võrguturvalisuse hindamised, lünkade analüüsid, füüsilise turvalisuse läbivaatamised, küsimustikud ja skaneerimistarkvara lahendused, võimaluse korral lähtekoodi ülevaatus, stsenaariumipõhised testid, ühilduvuse ja jõudlustestid ning läbiv- või läbistustestimine.

2. Artikli 2 lõike 1 punktides f ja g osutatud finantssektori ettevõtjad viivad haavatavuse hindamise läbi enne finantssektori ettevõtja kriitilise tähtsusega funktsioone, rakendusi ja taristukomponente toetavate uute või olemasolevate teenuste esmakordset või uuesti kasutusele võttu.

Artikkel 23

IKT-vahendite, -süsteemide ja -protsesside süvatestimine, mis tugineb ohuteabel põhinevale läbistustestimisele

1. Lõike 4 kohaselt kindlaks määratud finantssektori ettevõtjad viivad vähemalt iga kolme aasta järel läbi süvatestimise, kasutades selleks ohuteabel põhinevat läbistustestimist.

2. Ohuteabel põhinev läbistustestimine hõlmab vähemalt finantssektori ettevõtja kriitilise tähtsusega funktsioone ja teenuseid ning seda tehakse selliseid funktsioone toetavates toimivates süsteemides. Ohuteabel põhineva läbistustestimise täpse ulatuse määravad kriitilise tähtsusega funktsioonide ja teenuste hindamise alusel kindlaks finantssektori ettevõtjad ja selle kinnitavad pädevad asutused.

   Esimese lõigu kohaldamisel teevad finantssektori ettevõtjad kindlaks kõik olulised aluseks olevad IKT-protsessid, -süsteemid ja -tehnoloogiad, mis toetavad kriitilise tähtsusega funktsioone ja teenuseid, sealhulgas funktsioonid ja teenused, mis on edasi antud kolmandast isikust IKT-teenuste osutajatele või nendelt alltöövõtulepingu alusel ostetud.

   Kui kolmandast isikust IKT-teenuste osutajad on kaasatud ohuteabel põhinevasse läbistustestimisse, võtab finantssektori ettevõtja vajalikud meetmed, et tagada nende teenuseosutajate osalemine.

   Finantssektori ettevõtjad rakendavad tõhusat riskijuhtimiskontrolli, et vähendada riske, mis tulenevad võimalikust mõjust andmetele, vara kahjustamisest ja kriitilise tähtsusega teenuste või operatsioonide häiretest finantssektori ettevõtjas endas, selle vastaspooltes või finantssektoris.

Testi lõpus, pärast aruannete ja paranduskavade kokkuleppimist, esitavad finantssektori ettevõtja ja välistestijad pädevale asutusele dokumendid, mis kinnitavad, et ohuteabel põhinev läbistustestimine on läbi viidud vastavalt nõuetele. Pädevad asutused kinnitavad dokumendid ja annavad välja tõendi.

3. Finantssektori ettevõtjad sõlmivad ohuteabel põhineva läbistustestimise tegemiseks testijatega lepingu vastavalt artiklile 24.

Pädevad asutused määravad kindlaks finantssektori ettevõtjad, kes peavad tegema ohuteabel põhineva läbistustestimise viisil, mis on proportsionaalne finantssektori ettevõtja suuruse, tegevuse ulatuse, tegevusvaldkonna ja üldise riskiprofiiliga, hinnates järgmisi asjaolusid:

(a) mõjuga seotud tegurid, eelkõige finantssektori ettevõtja osutatavate teenuste ja tegevuste kriitilisus;

(b) võimalikud finantsstabiilsusega seotud probleemid, sealhulgas finantssektori ettevõtja süsteemne olulisus riigi või liidu tasandil, kui see on asjakohane;

(c) konkreetne IKT-riskide profiil, finantssektori ettevõtja IKT küpsus või hõlmatud tehnoloogilised omadused.

4. EBA, ESMA ja EIOPA töötavad pärast EKPga konsulteerimist ja võttes arvesse asjakohaseid liidu raamistikke, mida kohaldatakse teadmuspõhiste läbistustestide suhtes, välja regulatiivsete tehniliste standardite eelnõud, et täpsustada järgmist:

(a) käesoleva artikli lõike 6 kohaldamisel kasutatud kriteeriumid;

(b) nõuded, mis käsitlevad järgmist:

(a) käesoleva artikli lõikes 2 osutatud ohuteabel põhineva läbistustestimise ulatus;

(b) testimismetoodika ja meetodid, mida tuleb igas konkreetses testimisprotsessi etapis järgida;

(c) testimise tulemused, lõpetamise ja parandamise etapid;

(c) milline peab järelevalvealane koostöö olema ohuteabel põhineva läbistustestimise korral finantssektori ettevõtjate puhul, kes tegutsevad rohkem kui ühes liikmesriigis, et võimaldada piisavat järelevalvealast kaasatust ja paindlikku rakendamist, et võtta arvesse finantssektori allsektorite või kohalike finantsturgude eripära.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*ELT: palun lisada kuupäev: 2 kuud enne jõustumist*].

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu teises lõigus osutatud regulatiivsed tehnilised standardid kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1095/2010 ja määruse (EL) nr 1094/2010 artiklitega 10–14.

Artikkel 24

Testijatele esitatavad nõuded

1. Finantssektori ettevõtjad kasutavad ohuteabel põhinevaks läbistustestimiseks üksnes testijaid, kes:

(a) on kõige sobivamad ja parima mainega;

(b) omavad tehnilist ja organisatsioonilist suutlikkust ning tõendavad, et neil on eriteadmised ohuteadmuse, läbistustestimise või punase tiimi testimise alal;

(c) on sertifitseeritud liikmesriigi akrediteerimisasutuse poolt või järgivad ametlikke tegevusjuhendeid või eetikaraamistikke;

(d) juhul kui nad on välised testijad, esitavad sõltumatu kinnituse või auditiaruande ohuteabel põhineva läbistustestimisega seotud riskide usaldusväärse juhtimise kohta, sealhulgas finantssektori ettevõtja konfidentsiaalse teabe nõuetekohase kaitse kohta ja õiguskaitsevahendite kohta finantssektori ettevõtja äririskide puhul;

(e) juhul kui nad on välised testijad, on nõuetekohaselt ja täielikult kaetud asjakohase ametialase vastutuskindlustusega, sealhulgas väärkäitumise ja hooletuse riskide vastu.

2. Finantssektori ettevõtjad tagavad, et väliste testijatega sõlmitud lepingud eeldavad ohuteabel põhineva läbistustestimise tulemuste usaldusväärset haldamist ning et nende igasugune töötlemine, sealhulgas genereerimine, kirjapanek, salvestamine, koondamine, esitamine, edastamine või hävitamine, ei tekita finantssektori ettevõtjale riske.

V PEATÜKK

KOLMANDAST ISIKUST TULENEVA IKT-RISKI JUHTIMINE

I JAGU

KOLMANDAST ISIKUST TULENEVA IKT-RISKI USALDUSVÄÄRSE JUHTIMISE PEAMISED PÕHIMÕTTED

Artikkel 25

Üldpõhimõtted

Finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski oma IKT-riski juhtimise raamistikus IKT-riski lahutamatu osana ja kooskõlas järgmiste põhimõtetega.

1. Finantssektori ettevõtjad, kellel on lepingupõhised kokkulepped IKT-teenuste kasutamiseks oma äritegevuses, jäävad alati täielikult vastutavaks kõigi kohustuste järgimise ja täitmise eest, mis tulenevad käesolevast määrusest ja kohaldatavatest finantsteenuste õigusaktidest.

2. Finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski proportsionaalsuse põhimõtet järgides, võttes arvesse järgmist:

(a) IKTga seotud sõltuvuse ulatus, keerukus ja tähtsus;

(b) riskid, mis tulenevad IKT-teenuste kasutamise lepingupõhistest kokkulepetest, mis on sõlmitud kolmandast isikust IKT-teenuste osutajatega, võttes arvesse vastava teenuse, protsessi või funktsiooni kriitilisust või olulisust ning võimalikku mõju finantsteenuste ja -tegevuse järjepidevusele ja kvaliteedile nii individuaalsel kui ka grupi tasandil.

3. Finantssektori ettevõtjad võtavad IKT-riski juhtimise raamistiku osana vastu ja vaatavad korrapäraselt läbi kolmandast isikust tulenevat IKT-riski käsitleva strateegia, võttes arvesse artikli 5 lõike 9 punktis g osutatud mitme teenuseosutajaga strateegiat. See strateegia hõlmab kolmandast isikust IKT-teenuste osutajate pakutavate IKT-teenuste kasutamise poliitikat ning seda kohaldatakse individuaalselt või vajaduse korral allkonsolideeritud ja konsolideeritud alusel. Juhtorgan vaatab regulaarselt läbi kriitilise tähtsusega või oluliste funktsioonide edasiandmisega seoses tuvastatud riskid.

4. IKT-riski juhtimise raamistiku osana peavad ja ajakohastavad finantssektori ettevõtjad ettevõtja tasandil ning allkonsolideeritud ja konsolideeritud tasandil seoses kõigi lepingupõhiste kokkulepetega teaberegistrit kolmandast isikust IKT-teenuste osutajate osutatud IKT-teenuste kasutamise kohta.

   Esimeses lõigus osutatud lepingupõhised kokkulepped dokumenteeritakse nõuetekohaselt, eristades kriitilise tähtsusega või olulisi funktsioone käsitlevaid kokkuleppeid muudest kokkulepetest.

   Finantssektori ettevõtjad esitavad pädevatele asutustele vähemalt kord aastas teabe IKT-teenuste kasutamist käsitlevate uute kokkulepete arvu, kolmandast isikust IKT-teenuste osutajate kategooriate, lepingupõhiste kokkulepete liigi ning pakutavate teenuste ja funktsioonide kohta.

   Finantssektori ettevõtjad teevad taotluse korral pädevale asutusele kättesaadavaks kogu teaberegistri või vastavalt taotlusele selle teatavad osad koos teabega, mida peetakse finantssektori ettevõtja tõhusaks järelevalveks vajalikuks.

   Finantssektori ettevõtjad teavitavad pädevat asutust õigeaegselt kriitilise tähtsusega või oluliste funktsioonide täitmiseks kavandatud lepingute sõlmimisest ning sellest, kui funktsioon on muutunud kriitiliseks või oluliseks.

5. Enne IKT-teenuste kasutamist käsitlevate lepingupõhiste kokkulepete sõlmimist teevad finantssektori ettevõtjad järgmist:

   (a) hindavad, kas lepingupõhine kokkulepe hõlmab kriitilise tähtsusega või olulist funktsiooni;

   (b) hindavad, kas lepingu sõlmimise järelevalvealased tingimused on täidetud;

   (c) teevad kindlaks ja hindavad kõiki lepingupõhise kokkuleppega seotud asjakohaseid riske, sealhulgas võimalust, et sellised lepingupõhised kokkulepped võivad suurendada IKT kontsentratsiooniriski;

   (d) võtavad kõik hoolsusmeetmed võimalike kolmandast isikust IKT-teenuste osutajate suhtes ning tagavad kogu valiku- ja hindamisprotsessi jooksul, et kolmandast isikust IKT-teenuste osutaja oleks sobiv;

   (e) tuvastavad ja hindavad huvide konflikte, mida lepingupõhine kokkulepe võib põhjustada.

6. Finantssektori ettevõtjad võivad sõlmida lepingupõhiseid kokkuleppeid ainult selliste kolmandast isikust IKT-teenuste osutajatega, kes vastavad rangetele, asjakohastele ja uusimatele infoturbestandarditele.

7. Rakendades kolmandast isikust IKT-teenuste osutaja suhtes pääsu-, kontrolli- ja auditeerimisõigusi, määravad finantssektori ettevõtjad eelnevalt riskipõhiselt kindlaks auditite ja kontrollide sageduse ning auditeeritavad valdkonnad, järgides

üldtunnustatud auditeerimisstandardeid kooskõlas järelevalvejuhistega selliste auditeerimisstandardite kasutamise ja inkorporeerimise kohta.

Tehnoloogiliselt väga keerukate lepingupõhiste kokkulepete puhul kontrollib finantssektori ettevõtja, kas audiitoritel (siseaudiitorid, audiitorite rühmad või välisaudiitorid) on piisavad oskused ja teadmised asjaomaste auditite ja hindamiste tõhusaks läbiviimiseks.

8. Finantssektori ettevõtjad tagavad, et IKT-teenuste kasutamise lepingupõhiste kokkulepete rakendamine lõpetatakse vähemalt järgmistel asjaoludel:

(a) kolmandast isikust IKT-teenuste osutaja rikub kohaldatavaid õigus- ja haldusnorme või lepingutingimusi;

(b) kolmandast isikust tuleneva IKT-riski jälgimise käigus on tuvastatud asjaolud, mis võivad muuta lepingupõhiste kokkulepetega reguleeritud funktsioonide täitmist, sealhulgas olulised muutused, mis mõjutavad kolmandast isikust IKT-teenuste osutaja töökorraldust või olukorda;

(c) kolmandast isikust IKT-teenuste osutaja puhul on tõendatud puudused üldises IKT-riski juhtimises ja eelkõige selles, kuidas ta tagab konfidentsiaalsete, isiku- või muude tundlike andmete või isikustamata teabe turvalisuse ja tervikluse;

(d) asjaolud, mille korral pädev asutus ei saa asjaomase lepingupõhise kokkuleppe tõttu enam finantssektori ettevõtja üle tõhusat järelevalvet teha.

9. Finantssektori ettevõtjad kehtestavad väljumisstrateegiad, et võtta arvesse riske, mis võivad tekkida kolmandast isikust IKT-teenuste osutaja tasandil, eelkõige viimase võimalik maksejõuetuks muutumine, pakutavate funktsioonide kvaliteedi halvenemine, teenuste sobimatust või ebaõnnestunud osutamisest tingitud äritegevuse häired või oluline risk, mis tekib seoses funktsiooni asjakohase ja pideva rakendamisega.

Finantssektori ettevõtjad tagavad, et neil on võimalik loobuda lepingupõhistest kokkulepetest:

(a) oma äritegevust häirimata,

(b) takistamata õigusnormide järgimist,

(c) kahjustamata klientidele teenuste osutamise järjepidevust ja kvaliteeti.

Väljumiskavad peavad olema põhjalikud, dokumenteeritud ja vajaduse korral piisavalt testitud.

Finantssektori ettevõtjad määravad kindlaks alternatiivsed lahendused ja töötavad välja üleminekukavad, mis võimaldavad neil võtta ära lepingupõhised funktsioonid ja asjaomased andmed kolmandast isikust IKT-teenuste osutajalt ning kanda need turvaliselt ja terviklikult üle alternatiivsetele teenuseosutajatele või inkorporeerida need uuesti ettevõttesiseselt.

Finantssektori ettevõtjad võtavad asjakohaseid erandolukorra meetmeid, et säilitada talitluspidevus kõigi esimeses lõigus osutatud asjaolude korral.

10. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja rakenduslike tehniliste standardite eelnõud, et kehtestada lõikes 4 osutatud teaberegistri standardvormid.

Euroopa järelevalveasutused esitavad kõnealused rakenduslike tehniliste standardite eelnõud komisjonile hiljemalt [*ELT: [palun lisada kuupäev: 1 aasta pärast käesoleva määruse jõustumist]*.

Komisjonile antakse õigus võtta vastu esimeses lõigus osutatud rakenduslikud tehnilised standardid kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1095/2010 ja määruse (EL) nr 1094/2010 artikliga 15.

11. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete standardite eelnõu, et täpsustada:

(a) lõikes 3 osutatud poliitika üksikasjalikku sisu seoses kolmandast isikust IKT-teenuste osutajate pakutavate IKT-teenuste kasutamise lepingupõhiste kokkulepetega, kirjeldades nende kokkulepete peamisi etappe;

(b) lõikes 4 osutatud teaberegistrisse kantava teabe liigid.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*väljaannete talitus: palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu teises lõigus osutatud regulatiivsed tehnilised standardid kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1095/2010 ja määruse (EL) nr 1094/2010 artiklitega 10–14.

Artikkel 26

IKT kontsentratsiooniriski esialgne hindamine ja edasiantud tegevuse edasiandmise kord

1. Artikli 25 lõike 5 punktis c osutatud IKT kontsentratsiooniriski kindlakstegemisel ja hindamisel võtavad finantssektori ettevõtjad arvesse, kas IKT-teenustega seotud lepingupõhise kokkuleppe sõlmimine tooks kaasa mõne järgmise asjaolu:

(a) lepingu sõlmimine kolmandast isikust IKT-teenuste osutajaga, keda ei saa hõlpsasti asendada, või

(b) mitu lepingupõhist kokkulepet IKT-teenuste osutamise kohta sama kolmandast isikust IKT-teenuste osutajaga või omavahel tihedalt seotud kolmandast isikust IKT-teenuste osutajatega.

Finantssektori ettevõtjad kaaluvad alternatiivsete lahenduste, näiteks erinevate kolmandast isikust IKT-teenuste osutajate kasutamise eeliseid ja kulusid, võttes arvesse seda, kas ja kuidas kavandatud lahendused vastavad nende digitaalse kerksuse strateegias sätestatud ärivajadustele ja -eesmärkidele.

2. Kui IKT-teenuste kasutamist käsitlev lepingupõhine kokkulepe hõlmab võimalust, et kolmandast isikust IKT-teenuste osutaja sõlmib kriitilise tähtsusega või olulise funktsiooni alltöövõtulepingu mõne muu kolmandast isikust IKT-teenuste osutajaga, kaaluvad finantssektori ettevõtjad kasu ja riske, mis võivad tekkida seoses tegevuse sellise võimaliku edasiandmisega, eriti juhul, kui IKT alltöövõtja on asutatud kolmandas riigis.

Kui IKT-teenuste kasutamist käsitlevad lepingupõhised kokkulepped sõlmitakse kolmandast isikust IKT-teenuste osutajaga, kes on asutatud kolmandas riigis, võtavad finantssektori ettevõtjad arvesse vähemalt järgmisi asjakohaseid tegureid:

(a) andmekaitse põhimõtete austamine;

(b) seaduse tulemuslik jõustamine;

(c) maksejõuetusõiguse sätted, mida kohaldataks kolmandast isikust IKT-teenuste osutaja pankroti korral;

(d) mis tahes takistused, mis võivad tekkida seoses finantssektori ettevõtja andmete kiire taastamisega.

Finantssektori ettevõtjad hindavad, kas ja kuidas pikad või keerukad alltöövõtuahelad võivad mõjutada nende võimet täielikult jälgida lepingupõhiseid funktsioone ja pädeva asutuse suutlikkust teha selles osas finantssektori ettevõtja üle tulemuslikku järelevalvet.

Artikkel 27

Peamised lepingusätted

1. Finantssektori ettevõtja ja kolmandast isikust IKT-teenuste osutaja õigused ja kohustused jaotatakse selgelt ja sätestatakse kirjalikult. Täisleping, mis sisaldab teenustaseme kokkuleppeid, dokumenteeritakse ühes kirjalikus dokumendis, mis on pooltele kättesaadav paberil või allalaaditavas ja kättesaadavas vormingus.

2. IKT-teenuste kasutamist käsitlevad lepingupõhised kokkulepped sisaldavad vähemalt järgmist:

(a) kolmandast isikust IKT-teenuste osutaja kõikide funktsioonide ja teenuste selge ja täielik kirjeldus, märkides ära, kas kriitilise tähtsusega või olulise funktsiooni või selle oluliste osade edasiandmine on lubatud, ja kui on, siis sellise alltöövõtu suhtes kohaldatavad tingimused;

(b) kus täidetakse või pakutakse lepingupõhiseid või alltöövõtu korras osutatavaid funktsioone ja teenuseid ning kus andmeid töödeldakse, sealhulgas andmete talletamise asukoht, ning nõue, et kolmandast isikust IKT-teenuste osutaja teavitaks finantssektori ettevõtjat, kui ta kavatseb vastavat kohta muuta;

(c) sätted, mis käsitlevad ligipääsu isikuandmetele, nende kättesaadavust, terviklust, turvalisust ja kaitset, ning sätted, mis käsitlevad ligipääsu finantssektori ettevõtja poolt töödeldavatele kergesti kättesaadavas vormis isikuandmetele ja isikustamata andmetele, samuti nende taastamist ja tagastamist kolmandast isikust IKT-teenuste osutaja maksejõuetuse, kriisilahenduse või äritegevuse lõpetamise korral;

(d) täielikud teenustasemete kirjeldused, sealhulgas nende muutmised ja läbivaatamised, ning täpsed kvantitatiivsed ja kvalitatiivsed tulemuseesmärgid kokkulepitud teenustasemete piires, et finantssektori ettevõtja saaks teha tõhusat järelevalvet ja võtta põhjendamatu viivituseta asjakohaseid parandusmeetmeid, kui kokkulepitud teenustasemeid ei saavutata;

(e) kolmandast isikust IKT-teenuste osutaja tähtajad ja kohustused seoses finantssektori ettevõtja teavitamisega, sealhulgas teavitamine kõigist muutustest, mis võivad oluliselt mõjutada kolmandast isikust IKT-teenuste osutaja suutlikkust tulemuslikult täita kriitilise tähtsusega või olulisi funktsioone kooskõlas kokkulepitud teenustasemetega;

(f) kolmandast isikust IKT-teenuste osutaja kohustus pakkuda IKTga seotud intsidendi korral abi ilma lisakuludeta või eelnevalt kindlaksmääratud hinnaga;

(g) kolmandast isikust IKT-teenuste osutajale esitatavad nõuded rakendada ja testida ettevõtte erandolukorrakavu ning kehtestada IKT-turvameetmed, -vahendid ja -põhimõtted, mis piisavalt tagavad, et finantssektori ettevõtja osutab teenuseid turvaliselt kooskõlas õigusraamistikuga;

(h) õigus pidevalt jälgida kolmandast isikust IKT-teenuste osutaja tegevust, mis hõlmab järgmist:

i) finantssektori ettevõtja või määratud kolmanda isiku pääsu-, kontrollimis- ja auditeerimisõigused ning õigus teha koopiaid asjaomastest dokumentidest, mille tulemuslikku kasutamist ei takista ega piira muud lepingupõhised kokkulepped või rakenduspõhimõtted;

ii) õigus leppida kokku alternatiivsed usaldusväärsuse tasemed, kui teiste klientide õigused on mõjutatud;

iii) kohustus teha täielikku koostööd finantssektori ettevõtja tehtavate kohapealsete kontrollide ajal ning kaugauditite ulatuse, viiside ja sageduse üksikasjad;

(i) kolmandast isikust IKT-teenuste osutaja kohustus teha täielikku koostööd finantssektori ettevõtja pädevate asutuste ja kriisilahendusasutustega, sealhulgas nende määratud isikutega;

(j) lepingu lõpetamise õigused ja sellega seotud minimaalne lepingu lõpetamisest etteteatamise aeg, vastavalt pädevate asutuste ootustele;

(k) väljumisstrateegiad, eelkõige piisava kohustusliku üleminekuperioodi kehtestamine:

(a) mille jooksul kolmandast isikust IKT-teenuste osutaja jätkab vastavate funktsioonide täitmist või teenuste osutamist, et vähendada häirete riski finantssektori ettevõtjas;

(b) mis võimaldab finantssektori ettevõtjal minna üle teisele kolmandast isikust IKT-teenuste osutajale või kasutada kohapealseid lahendusi, mis on kooskõlas osutatud teenuse keerukusega.

3. Lepingupõhiste kokkulepete üle läbi rääkides kaaluvad finantssektori ettevõtjad ja kolmandast isikust IKT-teenuste osutajad, kas kasutada konkreetsete teenuste jaoks välja töötatud lepingu tüüptingimusi.

4. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete tehniliste standardite eelnõud, et täpsustada elemente, mida finantssektori ettevõtja peab kriitilise tähtsusega või oluliste funktsioonide alltöövõtu korral kindlaks määrama ja hindama, et nõuetekohaselt jõustada lõike 2 punkti a sätteid.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*ELT: palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1095/2010 ja määruse (EL) nr 1094/2010 artiklitega 10–14.

II JAGU

KRIITILISE TÄHTSUSEGA KOLMANDAST ISIKUST IKT-TEENUSTE OSUTAJATE JÄRELEVALVERAAMISTIK

Artikkel 28

Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kindlaksmääramine

1. Euroopa järelevalveasutused teevad ühiskomitee kaudu ja artikli 29 lõike 1 kohaselt loodud järelevalvefoorumi soovitusel järgmist:

   (a) määravad kindlaks finantssektori ettevõtjate jaoks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad, võttes arvesse lõikes 2 sätestatud kriteeriume;

   (b) määravad igale kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale juhtivaks järelevalveasutuseks kas EBA, ESMA või EIOPA sõltuvalt sellest, kas selliste finantssektori ettevõtjate varade koguväärtus, kes kasutavad selle kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teenuseid ja kuuluvad kas määruse (EL) nr 1093/2010, (EL) nr 1094/2010 või (EL) nr 1095/2010 kohaldamisalasse, moodustab üle poole kõigi selliste finantssektori ettevõtjate varade koguväärtusest, kes kasutavad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teenuseid, lähtudes nende finantssektori ettevõtjate konsolideeritud bilansist või individuaalsest bilansist (juhul kui bilansid ei ole konsolideeritud).

2. Lõike 1 punktis a osutatud kindlaksmääramine põhineb järgmistel kriteeriumidel:

   (a) süsteemne mõju finantsteenuste osutamise stabiilsusele, järjepidevusele või kvaliteedile juhul, kui asjaomast kolmandast isikust IKT-teenuste osutajat tabaks laiaulatuslik teenuste osutamise katkemine, võttes arvesse nende finantssektori ettevõtjate arvu, kellele asjaomane kolmandast isikust IKT-teenuste osutaja teenuseid osutab;

   (b) asjaomasest kolmandast isikust IKT-teenuste osutajast sõltuvate finantssektori ettevõtjate süsteemne olemus või olulisus, mida hinnatakse järgmiste parameetrite alusel:

      i) nende globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate arv, kes sõltuvad asjaomasest kolmandast isikust IKT-teenuste osutajast;

      ii) punktis i osutatud globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate ja muude finantssektori ettevõtjate vastastikune sõltuvus, sealhulgas olukorrad, kus globaalsed või muud süsteemselt olulised ettevõtjad osutavad finantstaristu teenuseid teistele finantssektori ettevõtjatele;

   (c) finantssektori ettevõtjate tuginemine teenustele, mida osutab asjaomane kolmandast isikust IKT-teenuste osutaja seoses finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonidega, mis lõpuks hõlmavad sama kolmandast isikust IKT-teenuste osutajat, olenemata sellest, kas finantssektori ettevõtjad sõltuvad nendest teenustest otseselt või kaudselt alltöövõtukokkulepete abil või kaudu;

(d) kolmandast isikust IKT-teenuste osutaja asendatavus, võttes arvesse järgmisi parameetreid:

i) tõeliste alternatiivide (isegi osaliselt) puudumine, mis on tingitud konkreetsel turul tegutsevate kolmandast isikust IKT-teenuste osutajate vähesusest või asjaomase kolmandast isikust IKT-teenuste osutaja turuosast või tegevuse tehnilisest keerukusest (sealhulgas seoses patenditud tehnoloogiaga) või kolmandast isikust IKT-teenuste osutaja organisatsiooni või tegevuse eripärast;

ii) raskused asjaomaste andmete ja töökoormuse osalisel või täielikul migreerimisel ühelt kolmandast isikust IKT-teenuste osutajalt teisele, mis on tingitud kas märkimisväärsetest rahalistest kuludest, kuluvast ajast või muud liiki ressurssidest, mida migratsioon võib hõlmata, või suurenenud IKT-riskidest või muudest operatsiooniriskidest, millega finantssektori ettevõtja võib sellise migratsiooni tõttu kokku puutuda;

(e) liikmesriikide arv, kus asjaomane kolmandast isikust IKT-teenuste osutaja teenuseid osutab;

(f) liikmesriikide arv, kus tegutsevad asjaomast kolmandast isikust IKT-teenuste osutajat kasutavad finantssektori ettevõtjad.

3. Komisjonil on artikli 50 kohaselt õigus vastu võtta delegeeritud õigusakte, millega täiendatakse lõikes 2 osutatud kriteeriume.

4. Lõike 1 punktis a osutatud kindlaksmääramise mehhanismi ei kasutata enne, kui komisjon on võtnud kooskõlas lõikega 3 vastu delegeeritud õigusakti.

5. Lõike 1 punktis a osutatud kindlaksmääramise mehhanismi ei kohaldata seoses kolmandast isikust IKT-teenuste osutajatega, kelle suhtes kohaldatakse järelevalveraamistikke, mis on kehtestatud Euroopa Liidu toimimise lepingu artikli 127 lõikes 2 osutatud ülesannete täitmise toetamiseks.

6. Euroopa järelevalveasutused koostavad, avaldavad ja ajakohastavad igal aastal ühiskomitee kaudu liidu tasandil kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate loetelu.

7. Lõike 1 punkti a kohaldamisel edastavad pädevad asutused igal aastal artikli 25 lõikes 4 osutatud koondaruanded artikli 29 kohaselt loodud järelevalvefoorumile. Järelevalvefoorum hindab finantssektori ettevõtjate sõltuvust kolmandast isikust IKT-teenuste osutajatest pädevatelt asutustelt saadud teabe põhjal.

8. Kolmandast isikust IKT-teenuste osutajad, kes ei ole kantud lõikes 6 osutatud loetellu, võivad taotleda enda sinna lisamist.

Esimese lõigu kohaldamisel esitab kolmandast isikust IKT-teenuste osutaja põhjendatud taotluse EBA-le, ESMA-le või EIOPA-le, kes otsustab ühiskomitee kaudu, kas kanda see kolmandast isikust IKT-teenuste osutaja kõnealusesse loetellu vastavalt lõike 1 punktile a.

Teises lõigus osutatud otsus võetakse vastu ja sellest teatatakse kolmandast isikust IKT-teenuste osutajale kuue kuu jooksul alates taotluse saamisest.

9. Finantssektori ettevõtjad ei kasuta kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajat, kes oleks määratud kriitilise tähtsusega ettevõtjaks vastavalt lõike 1 punktile a, kui ta oleks asutatud liidus.

Artikkel 29

Järelevalveraamistiku struktuur

1. Ühiskomitee asutab kooskõlas vastavalt määruse (EL) nr 1093/2010, määruse (EL) nr 1094/2010 ja määruse (EL) nr 1095/2010 artikliga 57 allkomiteena järelevalvefoorumi, et toetada ühiskomitee ja artikli 28 lõike 1 punktis b osutatud juhtiva järelevalveasutuse tööd, mis on seotud kolmandast isikust tuleneva IKT-riskiga finantssektoris. Järelevalvefoorum valmistab ette ühiskomitee selle valdkonna ühisseisukohtade ja -aktide eelnõud.

   Järelevalvefoorum arutab korrapäraselt IKT-riskide ja haavatavustega seotud muutusi ning edendab kolmandast isikust tulenevate IKT-riskide järjepidevat jälgimist liidu tasandil.

2. Järelevalvefoorum hindab igal aastal ühiselt kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalve tulemusi ja leide ning edendab koordineerimismeetmeid, et suurendada finantssektori ettevõtjate digitaalset tegevuskerksust, edendada IKT kontsentratsiooniriski käsitlemise parimaid tavasid ja uurida riskide valdkonnaülest ülekandumist leevendavaid tegureid.

3. Järelevalvefoorum esitab kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate põhjalikud võrdlusalused, mille ühiskomitee võtab vastu Euroopa järelevalveasutuste ühiste seisukohtadena kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikli 56 lõikega 1.

4. Järelevalvefoorumi moodustavad Euroopa järelevalveasutuste eesistujad ja iga liikmesriigi ajaomases pädevas asutuses töötavate töötajate üks kõrgetasemeline esindaja. Vaatlejatena osalevad järelevalvefoorumis kõigi Euroopa järelevalveasutuste tegevdirektorid ning üks Euroopa Komisjoni, Euroopa Süsteemsete Riskide Nõukogu, EKP ja ENISA esindaja.

5. Euroopa järelevalveasutused annavad kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 16 välja suunised, milles käsitletakse Euroopa järelevalveasutuste ja pädevate asutuste vahelist koostööd käesoleva jao kohaldamisel, pädevate asutuste ja Euroopa järelevalveasutuste vaheliste ülesannete täitmise üksikasjalikke protseduure ja tingimusi ning pädevatele asutustele vajaliku teabevahetuse üksikasju, et tagada artikli 31 lõike 1 punkti d kohaselt juhtivate järelevalveasutuste poolt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele esitatud soovituste järgimine.

6. Käesolevas jaos sätestatud nõuded ei piira direktiivi (EL) 2016/1148 ega pilvandmetöötlusteenuste osutajate suhtes kohaldatavate muude liidu järelevalve-eeskirjade kohaldamist.

7. Euroopa järelevalveasutused esitavad igal aastal ühiskomitee kaudu ja järelevalvefoorumi eeltöö põhjal Euroopa Parlamendile, nõukogule ja komisjonile aruande käesoleva jao kohaldamise kohta.

Artikkel 30

Juhtiva järelevalveasutuse ülesanded

1. Juhtiv järelevalveasutus hindab, kas kõik kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad on kehtestanud põhjalikud, usaldusväärsed ja tulemuslikud

eeskirjad, menetlused, mehhanismid ja korra, et juhtida IKT-riske, mida ta võib tekitada finantssektori ettevõtjatele.

2. Lõikes 1 osutatud hindamine hõlmab järgmist:

(a) IKT-nõuded, et tagada eelkõige selliste teenuste turvalisus, kättesaadavus, järjepidevus, skaleeritavus ja kvaliteet, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja osutab finantssektori ettevõtjatele, samuti suutlikkus säilitada igal ajal kõrgel tasemel andmete turvalisus, konfidentsiaalsus ja terviklus;

(b) füüsiline julgeolek, mis aitab tagada IKT turvalisust, sealhulgas ruumide, rajatiste ja andmekeskuste turvalisus;

(c) riskijuhtimisprotsessid, sealhulgas IKT-riskide juhtimise põhimõtted, IKT talitluspidevuse ja taastekavad;

(d) juhtimiskord, sealhulgas organisatsiooniline struktuur, millel on selged, läbipaistvad ja järjepidevad vastutusliinid, ning IKT-riske tõhusalt juhtida võimaldavad vastutuseeskirjad;

(e) IKTga seotud intsidentide tuvastamine, jälgimine ja neist finantssektori ettevõtjatele kiire teatamine ning selliste intsidentide, eelkõige küberrünnete juhtimine ja lahendamine;

(f) andmete ja rakenduste porditavuse ja koostalitlusvõime mehhanismid, mis tagavad lõpetamisõiguste tulemusliku kasutamise finantssektori ettevõtjate poolt;

(g) IKT-süsteemide, -taristu ja -kontrollide testimine;

(h) IKT-auditid;

(i) selliste asjakohaste riiklike ja rahvusvaheliste standardite kasutamine, mida kohaldatakse IKT-teenuste osutamisel finantssektori ettevõtjatele.

3. Lõikes 1 osutatud hindamise alusel võtab juhtiv järelevalveasutus vastu selge, üksikasjaliku ja põhjendatud individuaalse järelevalvekava iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja kohta. See kava edastatakse igal aastal kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale.

4. Kui lõikes 3 osutatud iga-aastased järelevalvekavad on kokku lepitud ja neist on teatatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele, võivad pädevad asutused võtta meetmeid seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega üksnes kokkuleppel juhtiva järelevalveasutusega.

Artikkel 31

Juhtiva järelevalveasutuse volitused

1. Käesolevas jaos sätestatud ülesannete täitmiseks on juhtival järelevalveasutusel järgmised volitused:

(a) nõuda vastavalt artiklile 32 kogu asjakohast teavet ja dokumentatsiooni;

(b) viia vastavalt artiklitele 33 ja 34 läbi üldisi uurimisi ja kontrolle;

(c) nõuda pärast järelevalvetoimingute lõpuleviimist aruandeid, milles täpsustatakse võetud või parandusmeetmeid, mida kriitilise tähtsusega

kolmandast isikust IKT-teenuste osutajad on võtnud seoses käesoleva lõike punktis d osutatud soovitustega;

(d) anda soovitusi artikli 30 lõikes 2 osutatud valdkondades, eelkõige seoses järgmisega:

i) konkreetsete IKT turva- ja kvaliteedinõuete või -protsesside kasutamine, eelkõige seoses paikade, uuenduste, krüpteerimise ja muude turvameetmete kasutuselevõtuga, mida juhtiv järelevalveasutus peab vajalikuks, et tagada finantssektori ettevõtjatele osutatavate IKT-teenuste turvalisus;

ii) nende tingimuste kasutamine (sealhulgas tehniline rakendamine), mille alusel kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad osutavad teenuseid finantssektori ettevõtjatele, mida juhtiv järelevalveasutus peab oluliseks, et hoida ära nõrkade lülide tekitamist või nende võimendamist või et minimeerida võimalikku süsteemset mõju kogu liidu finantssektoris IKT kontsentratsiooniriski korral;

iii) vastavalt alltöövõttu käsitlevate kokkulepete kontrollile, mis on tehtud vastavalt artiklitele 32 ja 33 ja mis hõlmab ka edasiantud tegevuse edasiandmise kokkuleppeid, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad kavatsevad sõlmida muude kolmandast isikust IKT-teenuste osutajatega või kolmandas riigis asutatud IKT alltöövõtjatega, mis tahes kavandatud alltöövõtt, sealhulgas edasiantud tegevuse edasiandmine, kui juhtiv järelevalveasutus leiab, et tegevuse täiendav edasiandmine võib põhjustada riske finantssektori ettevõtja teenuste osutamisel või ohustada finantsstabiilsust;

iv) täiendavate alltöövõtukokkulepete sõlmimisest hoidumine, kui on täidetud järgmised kumulatiivsed tingimused:

– kavandatav alltöövõtja on kolmandast isikust IKT-teenuste osutaja või kolmandas riigis asutatud IKT alltöövõtja;

– alltöövõtt on seotud finantssektori ettevõtja kriitilise tähtsusega või olulise funktsiooniga.

2. Juhtiv järelevalveasutus konsulteerib enne lõikes 1 osutatud volituste kasutamist järelevalvefoorumiga.

3. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad teevad heas usus koostööd juhtiva järelevalveasutusega ja abistavad teda tema ülesannete täitmisel.

4. Juhtiv järelevalveasutus võib määrata perioodilisi karistusmakseid, et sundida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajat täitma lõike 1 punktides a, b ja c sätestatud nõudeid.

5. Lõikes 4 osutatud perioodiline karistusmakse määratakse iga päeva kohta kuni nõuete täitmise saavutamiseni ja mitte kauemaks kui kuueks kuuks pärast kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teavitamist.

6. Perioodilise karistusmakse summa, mis arvutatakse alates perioodilise karistusmakse määramise otsuses sätestatud kuupäevast, on 1 % kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja eelmise majandusaasta ülemaailmsest keskmisest päevakäibest.

7. Karistusmaksed on haldusõiguslikud ja täitmisele pööratavad. Täitmist reguleerivad selles liikmesriigis kehtivad tsiviilmenetluse normid, mille territooriumil kontrollid aset leiavad ja kus on juurdepääs. Kaebused, mis on seotud täitmise eeskirjade eiramisega, kuuluvad asjaomase liikmesriigi kohtute pädevusse. Karistusmaksete summad kantakse Euroopa Liidu üldeelarvesse.

8. Euroopa järelevalveasutused avalikustavad kõik määratud perioodilised karistusmaksed, välja arvatud juhul, kui selline avalikustamine ohustaks tõsiselt finantsturge või tekitaks asjaomastele isikutele ebaproportsionaalset kahju.

9. Enne lõike 4 alusel perioodilise karistusmakse määramist annab juhtiv järelevalveasutus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esindajatele, kelle suhtes on algatatud menetlus, võimaluse esitada järelduste kohta oma seisukoht, ning teeb oma otsused üksnes nende järelduste põhjal, mille kohta kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal, kelle suhtes on algatatud menetlus, on olnud võimalus oma seisukoht esitada. Menetluse käigus tagatakse täielikult uurimisaluste isikute õigus kaitsele. Neil on õigus tutvuda toimikuga tingimusel, et võetakse arvesse teiste isikute õigustatud huvi kaitsta oma ärisaladusi. Toimikuga tutvumise õigus ei hõlma konfidentsiaalset teavet ega juhtiva järelevalveasutuse asutusesiseseks kasutuseks ette nähtud ettevalmistavaid dokumente.

Artikkel 32
Teabenõue

1. Juhtiv järelevalveasutus võib lihtteabenõude või otsusega nõuda, et kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad esitaksid kogu teabe, mida on juhtival järelevalveasutusel vaja käesolevast määrusest tulenevate ülesannete täitmiseks, sealhulgas kõik asjakohased äri- või tegevusdokumendid, lepingud, poliitikadokumendid, IKT turvalisuse auditiaruanded ja IKTga seotud intsidentide aruanded, samuti kogu teabe, mis on seotud isikutega, kellele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja on funktsioonid või tegevuse edasi andnud.

2. Kui juhtiv järelevalveasutus saadab lõike 1 kohase lihtteabenõude, peab ta:

   (a) viitama nõude õigusliku alusena käesolevale artiklile;

   (b) nimetama teabenõude eesmärgi;

   (c) täpsustama, millise teabe esitamist nõutakse;

   (d) määrama tähtaja, mille jooksul teave tuleb esitada;

   (e) teavitama kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esindajat, kellelt teavet taotletakse, et teabe andmine ei ole kohustuslik, kuid et teabenõude alusel vabatahtlikult esitatav teave ei tohi olla ebaõige ega eksitav.

3. Kui juhtiv järelevalveasutus nõuab teabe esitamist vastavalt lõikele 1, peab ta:

   (a) viitama nõude õigusliku alusena käesolevale artiklile;

   (b) nimetama teabenõude eesmärgi;

   (c) täpsustama, millise teabe esitamist nõutakse;

   (d) määrama tähtaja, mille jooksul teave tuleb esitada;

   (e) märkima artikli 31 lõikes 4 ettenähtud perioodilised karistusmaksed, mida kohaldatakse, kui nõutav teave esitatakse mittetäielikult;

(f) viitama õigusele kaevata otsus edasi Euroopa järelevalveasutuse apellatsiooninõukogule ja õigusele vaidlustada otsus Euroopa Liidu Kohtus (edaspidi „Euroopa Kohus“) vastavalt määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitele 60 ja 61.

4. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate esindajad esitavad nõutud teabe. Nõuetekohaselt volitatud juristid võivad teavet esitada oma klientide nimel. Kui esitatud teave on ebatäielik, ebaõige või eksitav, jääb täielikult vastutavaks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja.

5. Juhtiv järelevalveasutus saadab teabeesitamise otsuse koopia viivitamata nende finantssektori ettevõtjate pädevatele asutustele, kes kasutavad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate teenuseid.

Artikkel 33
Üldised uurimised

1. Käesolevast määrusest tulenevate ülesannete täitmiseks võib juhtiv järelevalveasutus, keda abistab artikli 34 lõikes 1 osutatud kontrollirühm, korraldada kolmandast isikust IKT-teenuste osutajate suhtes vajalikke uurimisi.

2. Juhtival järelevalveasutusel on õigus:

(a) kontrollida dokumente, andmeid, protseduure ja muid tema ülesannete täitmisega seonduvaid materjale, sõltumata nende salvestamiseks kasutatud andmekandjast;

(b) teha või saada nendest dokumentidest, andmetest, protseduuridest ja muudest materjalidest tõendatud koopiaid või väljavõtteid;

(c) kutsuda kolmandast isikust IKT-teenuste osutaja esindajaid välja ja paluda neil anda suulisi või kirjalikke selgitusi uurimise sisu ja eesmärgiga seotud asjaolude või dokumentide kohta ning salvestada vastuseid;

(d) küsitleda teisi küsitlemisega nõustuvaid füüsilisi või juriidilisi isikuid, et koguda teavet uurimise sisu kohta;

(e) nõuda andmeid telefonikõnede ja andmeedastuse kohta.

3. Juhtiva järelevalveasutuse poolt lõikes 1 osutatud uurimiseks volitatud ametnikud ja muud isikud teostavad oma õigusi, esitades kirjaliku volituse, milles on täpsustatud uurimise sisu ja eesmärk.

Nimetatud volitusse märgitakse ka artikli 31 lõikes 4 sätestatud perioodilised karistusmaksed, mida kohaldatakse juhul, kui nõutud dokumente, andmeid, teavet protseduuride kohta ja muid materjale või vastuseid kolmandast isikust IKT-teenuste osutaja esindajatele esitatud küsimustele ei esitata või kui need esitatakse mittetäielikult.

4. Kolmandast isikust IKT-teenuste osutajate esindajad peavad alluma juhtiva järelevalveasutuse otsuse alusel algatatud uurimisele. Otsuses märgitakse uurimise sisu ja eesmärk, artikli 31 lõikes 4 sätestatud perioodilised karistusmaksed, määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 kohased õiguskaitsevahendid ja samuti õigus otsuse läbivaatamisele Euroopa Kohtu poolt.

5. Aegsasti enne uurimist teavitavad juhtivad järelevalveasutused seda kolmandast isikust IKT-teenuste osutajat kasutavate finantssektori ettevõtjate pädevaid asutusi uurimisest ja volitatud isikutest.

Artikkel 34

Kohapealsed kontrollid

1. Käesolevast määrusest tulenevate ülesannete täitmiseks võib juhtiv järelevalveasutus, keda abistavad artikli 35 lõikes 1 osutatud kontrollirühmad, siseneda kolmandast isikust IKT-teenuste osutajate äriruumidesse, maale või kinnisasjale, näiteks peakontoritesse, tegevuskeskustesse ja varuruumidesse, ning viia läbi kõik vajalikud kohapealsed kontrollid, aga teha ka *offline*-kontrolle.

2. Ametnikud ja muud isikud, keda juhtiv järelevalveasutus on volitanud tegema kohapealset kontrolli, võivad siseneda sellistesse äriruumidesse, maale või kinnisasjale ning neil on kõik volitused pitseerida äriruume ning raamatupidamis- ja muid dokumente selliseks ajavahemikuks ja sellises ulatuses, mida on vaja kontrolli läbiviimiseks.

   Nad teostavad oma õigusi, esitades kirjaliku volituse, milles täpsustatakse kontrolli sisu ja eesmärk ning artikli 31 lõikes 4 sätestatud perioodilised karistusmaksed, mida kohaldatakse juhul, kui asjaomaste kolmandast isikust IKT teenuste osutajate esindajad ei allu kontrollile.

3. Aegsasti enne kontrolli teavitavad juhtivad järelevalveasutused seda kolmandast isikust IKT-teenuste osutajat kasutavate finantssektori ettevõtjate pädevaid asutusi.

4. Kontrollid hõlmavad kõiki asjakohaseid IKT-süsteeme,-võrke,-seadmeid, -teavet ja -andmeid, mida kasutatakse teenuste osutamisel finantssektori ettevõtjatele või mis aitavad sellele kaasa.

5. Enne kavandatud kohapealset kontrollkäiku teavitavad juhtivad järelevalevasutused mõistliku aja jooksul kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaid, välja arvatud juhul, kui selline teatamine ei ole võimalik häda- või kriisiolukorra tõttu või kui see viiks olukorrani, kus kontroll või audit ei oleks enam tulemuslik.

6. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja peab alluma juhtiva järelevalveasutuse otsuse alusel korraldatud kohapealsele kontrollile. Otsuses määratakse kindlaks kontrolli sisu ja eesmärk ning selle alustamise kuupäev ning sellesse märgitakse artikli 31 lõikes 4 sätestatud perioodilisted karistusmaksed ja määrustega (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 tagatud õiguskaitsevahendid, samuti õigus otsuse läbivaatamisele Euroopa Kohtu poolt.

7. Kui juhtiva järelevalveasutuse volitatud ametnikud ja muud isikud leiavad, et kriitilise tähtsusega kolmandast isikust IKT-teenuse osutaja ei nõustu käesoleva artikli kohaselt otsusega ette nähtud kontrolliga, teavitab juhtiv järelevalveasutus kriitilise tähtsusega IKT-teenuste osutajat sellise vastuseisu tagajärgedest, sealhulgas asjaomaste finantssektori ettevõtjate pädevate asutuste võimalusest lõpetada lepingulised kokkulepped, mis on sõlmitud kõnealuse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga.

Artikkel 35

Jooksev järelevalve

1. Üldiste uurimiste või kohapealsete kontrollide läbiviimisel abistab juhtivaid järelevalveasutusi ühine kontrollirühm, mis on moodustatud iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja jaoks.

2. Lõikes 1 osutatud ühine kontrollirühm koosneb kuni kümnest juhtiva järelevalveasutuse ja selliste asjaomaste pädevate asutuste töötajast, kes teevad järelevalvet nende finantssektori ettevõtjate üle, kellele kriitilise tähtsusega

kolmandast isikust IKT-teenuste osutaja osutab teenuseid, ning kes osalevad järelevalvealase tegevuse ettevalmistamises ja läbiviimises. Kõigil ühise kontrollirühma liikmetel peavad olema IKT- ja operatsiooniriskialased teadmised. Ühine kontrollirühm töötab Euroopa järelevalveasutuse määratud töötaja („juhtiv järelevalvekoordinaator“) koordineerimisel.

3. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja ühiste regulatiivsete tehniliste standardite eelnõud, et täpsustada asjaomaste pädevate asutuste ühise kontrollirühma liikmete määramist ning kontrollirühma ülesandeid ja töökorraldust. Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt [*ELT: palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus võtta vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas vastavalt määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10 kuni 14.

4. Kolme kuu jooksul pärast uurimise või kohapealse kontrolli lõpetamist võtab juhtiv järelevalveasutus pärast järelevalvefoorumiga konsulteerimist vastu soovitused, mille juhtiv järelevalveasutus esitab vastavalt artiklis 31 osutatud volitustele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale.

5. Lõikes 4 osutatud soovitused edastatakse viivitamata kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale ja nende finantssektori ettevõtjate pädevatele asutustele, kellele ta teenuseid osutab.

Järelevalve tegemiseks võivad juhtivad järelevalveasutused võtta arvesse mis tahes asjakohaseid kolmandate isikute sertifikaate ning kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja kättesaadavaks tehtud sise- või välisauditi aruandeid.

Artikkel 36

Järelevalve tegemist võimaldavate tingimuste ühtlustamine

1. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete standardite eelnõud, et määrata kindlaks:

(a) teave, mille kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja peab esitama, kui ta soovib artikli 28 lõike 8 kohaselt taotleda vabatahtlikku järelevalves osalemist;

(b) selliste aruannete sisu ja vorm, mida võidakse nõuda artikli 31 lõike 1 punkti c kohaldamiseks;

(c) see, kuidas peab olema esitatud teave, mille kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad peavad artikli 31 lõike 1 kohaselt esitama või avalikustama või mida nad peavad aruannetes käsitlema (sealhulgas struktuur, vorming ja meetodid);

(d) pädevate asutuste üksikasjalik hinnang meetmetele, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad on võtnud juhtivate järelevalveasutuste artikli 37 lõike 2 kohaste soovituste alusel.

2. Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 1. jaanuariks 20xx [*ELT: palun lisada kuupäev: 1 aasta pärast jõustumist*].

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid vastavalt menetlusele, mis on sätestatud määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklites 10–14.

Artikkel 37

Pädevate asutuste järelmeetmed

1. 30 kalendripäeva jooksul pärast juhtivate järelevalveasutuste poolt artikli 31 lõike 1 punkti d kohaselt antud soovituste kättesaamist teatavad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad juhtivale järelevalveasutusele, kas nad kavatsevad neid soovitusi järgida. Juhtivad järelevalveasutused edastavad selle teabe viivitamata pädevatele asutustele.

2. Pädevad asutused jälgivad, kas finantssektori ettevõtjad võtavad arvesse riske, mis on nimetatud soovitustes, mille juhtiv järelevalveasutus on esitanud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele vastavalt artikli 31 lõike 1 punktile d.

3. Pädevad asutused võivad kooskõlas artikliga 44 nõuda, et finantssektori ettevõtjad peataksid ajutiselt osaliselt või täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja pakutava teenuse kasutamise või kasutuselevõtu, kuni kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele suunatud soovitustes nimetatud riskid on kõrvaldatud. Vajaduse korral võivad nad nõuda, et finantssektori ettevõtjad lõpetaksid osaliselt või täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingupõhised kokkulepped.

4. Lõikes 3 osutatud otsuste tegemisel võtavad pädevad asutused arvesse riski liiki ja ulatust, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja ei käsitle, ning mittejärgimise tõsidust, võttes arvesse järgmisi kriteeriume:

   (a) mittejärgimise raskus ja kestus;

   (b) kas mittejärgimine on paljastanud tõsiseid puudusi kolmandast isikust IKT-teenuste osutaja menetlustes, juhtimissüsteemides, riskijuhtimises ja sisekontrollis;

   (c) kas mittejärgimine hõlbustas finantskuritegu, põhjustas selle või on muul viisil sellega seostatav;

   (d) kas mittejärgimine pandi toime tahtlikult või hooletuse tõttu.

5. Pädevad asutused teavitavad juhtivaid järelevalveasutusi korrapäraselt finantssektori ettevõtjatega seotud järelevalveülesannete täitmisel kasutatud lähenemisviisidest ja meetmetest ning finantssektori ettevõtjate võetud lepingupõhistest meetmetest, kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja ei ole juhtiva järelevalveasutusi soovitusi osaliselt või täielikult heaks kiitnud.

Artikkel 38

Järelevalvetasud

1. Euroopa järelevalveasutused nõuavad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt tasu, mis katab täielikult Euroopa järelevalveasutuste kulud, mis on vajalikud käesoleva määruse kohaste järelevalveülesannete täitmiseks, sealhulgas kõigi selliste kulude hüvitamine, mis võivad tekkida seoses pädevate asutuste tööga, mis ühinevad artikli 35 kohase järelevalvetegevusega.

   Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajalt võetav tasu katab kõik halduskulud ja on proportsionaalne tema käibega.

2. Komisjonil on õigus võtta kooskõlas artikliga 50 vastu delegeeritud õigusakt käesoleva määruse täiendamiseks ning määrata kindlaks tasude suuruse ja nende maksmise viisi.

Artikkel 39

Rahvusvaheline koostöö

1. EBA, ESMA ja EIOPA võivad vastavalt määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklile 33 sõlmida halduskokkuleppeid kolmandate riikide reguleerivate ja järelevalveasutustega, et edendada rahvusvahelist koostööd seoses kolmandast isikust tuleneva IKT-riskiga eri finantssektorites ning eelkõige töötada välja IKT-riskide juhtimise ja kontrolli, leevendusmeetmete ja intsidentidele reageerimise parimad tavad.

2. Euroopa järelevalveasutused esitavad ühiskomitee kaudu iga viie aasta järel Euroopa Parlamendile, nõukogule ja komisjonile ühise konfidentsiaalse aruande, milles võetakse kokku lõikes 1 osutatud kolmandate riikide ametiasutustega peetud asjakohaste arutelude tulemused, keskendudes kolmandast isikust tuleneva IKT-riski muutusele ja selle mõjule finantsstabiilsusele, turu usaldusväärsusele, investorite kaitsele või ühtse turu toimimisele.

VI PEATÜKK

TEABEJAGAMISE KOKKULEPPED

Artikkel 40

Küberohte käsitleva teabe ja teadmuse jagamise kokkulepped

1. Finantssektori ettevõtjad võivad omavahel vahetada küberohte käsitlevat teavet ja teadmust, sealhulgas ohunäitajaid, taktikaid, tehnikaid ja menetlusi, küberturbehoiatusi ja konfigureerimisvahendeid, kui sellise teabe ja teadmuse jagamine:

   (a) aitab suurendada finantssektori ettevõtjate digitaalset tegevuskerksust ning eelkõige suurendab küberohtudest teadlikkust, piirab või takistab küberohtude levikut, toetab finantssektori ettevõtjate erinevaid kaitsevõimeid, ohu avastamise meetodeid, leevendusstrateegiaid või reageerimis- ja taastamisetappe;

   (b) toimub finantssektori ettevõtjate usaldusväärses kogukonnas;

   (c) toimub selliste teabejagamise kokkulepete alusel, mis kaitsevad jagatava teabe potentsiaalselt tundlikku laadi ning mille suhtes kohaldatakse tegevuseeskirju,

austades täielikult ärisaladuse ja isikuandmete kaitse põhimõtteid[48] ning konkurentsipoliitika suuniseid[49].

2. Lõike 1 punkti c kohaldamisel määratakse teabejagamise kokkulepetes kindlaks osalemistingimused ning vajaduse korral sätestatakse üksikasjad avaliku sektori asutuste osalemise ja ulatuse kohta, milles neid võib teabejagamise kokkulepetesse kaasata, samuti tegevuse elemendid, sealhulgas spetsiaalsete IT-platvormide kasutamine.

3. Finantssektori ettevõtjad teavitavad pädevaid asutusi oma osalemisest lõikes 1 osutatud teabevahetuse kokkulepetes pärast oma liikmesuse kinnitamist, või kui see on asjakohane, oma liikmesuse lõpetamisest pärast viimase jõustumist.

VII PEATÜKK

PÄDEVAD ASUTUSED

Artikkel 41

Pädevad asutused

Ilma et see piiraks käesoleva määruse V peatüki II jaos osutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalveraamistikku käsitlevate sätete kohaldamist, tagavad käesolevas määruses sätestatud kohustuste täitmise kooskõlas vastavates õigusaktides sätestatud volitustega järgmised pädevad asutused:

(a) krediidiasutuste puhul direktiivi 2013/36/EL artikli 4 kohaselt määratud pädev asutus, ilma et see piiraks EKP-le määrusega (EL) nr 1024/2013 antud eriülesandeid;

(b) makseteenuste pakkujate puhul direktiivi (EL) 2015/2366 artikli 22 kohaselt määratud pädev asutus;

(c) e-raha asutuste puhul direktiivi 2009/110/EÜ artikli 37 kohaselt määratud pädev asutus;

(d) investeerimisühingute puhul direktiivi (EL) 2019/2034 artikli 4 kohaselt määratud pädev asutus;

(e) krüptovarateenuse osutajate, krüptovarade emitentide, varapõhiste tokenite emitentide ja oluliste varapõhiste tokenite emitentide puhul määruse [*(EL) 20xx MICA määrus*] artikli 3 lõike 1 punkti ee esimese taande kohaselt määratud pädev asutus;

(f) väärtpaberite keskdepositooriumide puhul määruse (EL) nr 909/2014 artikli 11 kohaselt määratud pädev asutus;

(g) kesksete vastaspoolte puhul määruse (EL) nr 648/2012 artikli 22 kohaselt määratud pädev asutus;

---

[48] Kooskõlas Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrusega (EL) 2016/679 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).

[49] Komisjoni teatis „Suunised Euroopa Liidu toimimise lepingu artikli 101 kohaldatavuse kohta horisontaalkoostöö kokkulepete suhtes“ (2011/C 11/01).

(h) kauplemiskohtade ja aruandlusteenuse pakkujate puhul direktiivi 2014/65/EÜ artikli 67 kohaselt määratud pädev asutus;

(i) kauplemisteabehoidlate puhul määruse (EL) nr 648/2012 artikli 55 kohaselt määratud pädev asutus;

(j) alternatiivsete investeerimisfondide valitsejate puhul direktiivi 2011/61/EL artikli 44 kohaselt määratud pädev asutus;

(k) fondivalitsejate puhul direktiivi 2009/65/EÜ artikli 97 kohaselt määratud pädev asutus;

(l) kindlustus- ja edasikindlustusandjate puhul direktiivi 2009/138/EÜ artikli 30 kohaselt määratud pädev asutus;

(m) kindlustus- ja edasikindlustusvahendajate ja kõrvaltegevusena pakutava kindlustuse vahendajate puhul direktiivi (EL) 2016/97 artikli 12 kohaselt määratud pädev asutus;

(n) tööandja kogumispensioni asutuste puhul direktiivi (EL) 2016/2341 artikli 47 kohaselt määratud pädev asutus;

(o) reitinguagentuuride puhul määruse (EÜ) nr 1060/2009 artikli 21 kohaselt määratud pädev asutus;

(p) vannutatud audiitorite ja audiitorühingute puhul direktiivi 2006/43/EÜ artikli 3 lõike 2 ja artikli 32 kohaselt määratud pädev asutus;

(q) kriitilise tähtsusega võrdlusaluste haldurite puhul *määruse xx/202x* artiklite 40 ja 41 kohaselt määratud pädev asutus;

(r) ühisrahastusteenuse osutajate puhul *määruse xx/202x artikli x* kohaselt määratud pädev asutus;

(s) väärtpaberistamise registrite puhul määruse (EL) 2017/2402 artikli 10 ja artikli 14 lõike 1 kohaselt määratud pädev asutus.

Artikkel 42

Koostöö direktiiviga (EL) 2016/1148 loodud struktuuride ja asutustega

1. Koostöö edendamiseks ja järelevalvealase teabevahetuse võimaldamiseks käesoleva määruse kohaselt määratud pädevate asutuste ning direktiivi (EL) 2016/1148 artikli 11 alusel loodud koostöörühma vahel võivad Euroopa järelevalveasutused ja pädevad asutused taotleda koostöörühma töös osalemist.

2. Pädevad asutused võivad vajaduse korral konsulteerida ühtse kontaktpunktiga ja riiklike küberturbe intsidentide lahendamise üksustega, millele on osutatud vastavalt direktiivi (EL) 2016/1148 artiklites 8 ja 9.

Artikkel 43

Finantssektoriteülesed simulatsioonid, teabevahetus ja koostöö

1. Et suurendada teadlikkust olukorrast ning teha kindlaks sektorite ühised küberhaavatavused ja -riskid, võivad Euroopa järelevalveasutused ühiskomitee kaudu ning koostöös pädevate asutuste, EKP ja Euroopa Süsteemsete Riskide Nõukoguga luua mehhanisme, mis võimaldavad jagada finantssektorite vahel tõhusaid tavasid.

Nad võivad välja töötada kriisijuhtimis- ja erandolukorra simulatsioone, mis hõlmavad küberrünnete stsenaariume, et töötada välja sidekanalid ja võimaldada järk-järgult tõhusat koordineeritud reageerimist ELi tasandil IKTga seotud olulise piiriülese intsidendi või seonduva ohu korral, millel on süsteemne mõju liidu finantssektorile tervikuna.

Nende õppuste käigus võib vajaduse korral testida ka finantssektori sõltuvust muudest majandussektoritest.

2. Pädevad asutused, EBA, ESMA või EIOPA ja EKP teevad omavahel tihedat koostööd ja vahetavad teavet, et täita oma artiklite 42–48 kohaseid ülesandeid. Nad kooskõlastavad tihedalt oma järelevalvetegevust, et teha kindlaks ja likvideerida käesoleva määruse rikkumised, töötada välja ja edendada parimaid tavasid, hõlbustada koostööd, edendada tõlgendamise ühtsust ning anda lahkhelide korral jurisdiktsiooniüleseid hinnanguid.

Artikkel 44

Halduskaristused ja parandusmeetmed

1. Pädevatel asutustel on kõik käesoleva määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused.

2. Lõikes 1 osutatud volitused hõlmavad vähemalt õigust:

   (a) tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis pädeva asutuse arvates võiksid olla tema ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid;

   (b) teha kohapeal kontrolle või uurimisi;

   (c) nõuda käesoleva määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

3. Ilma et see piiraks liikmesriikide õigust määrata kriminaalkaristusi vastavalt artiklile 46, kehtestavad liikmesriigid eeskirjad, millega sätestatakse asjakohased halduskaristused ja parandusmeetmed käesoleva määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise.

   Sellised karistused ja meetmed peavad olema tulemuslikud, proportsionaalsed ja heidutavad.

4. Liikmesriigid annavad pädevatele asutustele õiguse kohaldada käesoleva määruse rikkumise korral vähemalt järgmisi halduskaristusi või parandusmeetmeid:

   (a) teha ettekirjutus, et füüsiline või juriidiline isik lõpetaks teatava tegevuse ja hoiduks selle tegevuse kordamisest;

   (b) nõuda sellise tegevuse või tava ajutist või alalist peatamist, mis pädeva asutuse arvates on vastuolus käesoleva määruse sätetega, ning hoida ära sellise tegevuse või tava kordumine;

   (c) võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist;

   (d) nõuda siseriikliku õigusega lubatud ulatuses sideoperaatorite valduses olevaid andmeliiklusandmeid, kui on piisav alus kahtlustada käesoleva määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised käesoleva määruse rikkumiste uurimisel, ning

(e) väljastada avalikke teadaandeid, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

5. Juhul kui lõike 2 punkti c ja lõike 4 sätteid kohaldatakse juriidiliste isikute suhtes, annavad liikmesriigid pädevatele asutustele õiguse kohaldada halduskaristusi ja parandusmeetmeid vastavalt siseriiklikus õiguses sätestatud tingimustele juhtorgani liikmete ja teiste isikute suhtes, kes vastutavad siseriikliku õiguse alusel asjaomase rikkumise eest.

6. Liikmesriigid tagavad, et iga otsus, millega määratakse lõike 2 punktis c sätestatud halduskaristused või parandusmeetmed, on nõuetekohaselt põhjendatud ja et selle võib edasi kaevata.

Artikkel 45

Halduskaristuste ja parandusmeetmete määramise õiguse kasutamine

1. Olenevalt asjaoludest kasutavad pädevad asutused oma volitusi artiklis 44 osutatud halduskaristuste ja parandusmeetmete määramisel kooskõlas oma riigi õigusraamistikuga kas

(a) otse;

(b) koostöös teiste ametiasutustega;

(c) omal vastutusel, delegeerides küsimuse teistele asutustele;

(d) suunates küsimuse pädevatele õigusasutustele.

2. Kui pädevad asutused määravad kindlaks artikli 44 kohase halduskaristuse või parandusmeetme liiki ja ulatust, võtavad nad seejuures arvesse, mil määral on rikkumine tahtlik või tuleneb hooletusest, ja kõiki muid asjakohaseid asjaolusid, sealhulgas vajaduse korral järgmist:

(a) rikkumise olulisus, raskusaste ja kestus;

(b) rikkumise toime pannud füüsilise või juriidilise isiku vastutuse ulatus;

(c) vastutava füüsilise või juriidilise isiku finantsseisundi tugevus;

(d) vastutava füüsilise või juriidilise isiku saadud kasu või välditud kahju suurus, kui seda on võimalik kindlaks määrata;

(e) kolmandate isikute kahju, mis tulenes rikkumisest, kui seda on võimalik kindlaks määrata;

(f) vastutava füüsilise või juriidilise isiku ja pädeva asutuse koostöö tase, ilma et see piiraks vajadust tagada kõnealuse isiku saadud kasumi tagastamine või välditud kahjumi sissenõudmine;

(g) vastutava füüsilise või juriidilise isiku varasemad rikkumised.

Artikkel 46

Kriminaalkaristused

1. Liikmesriigid võivad otsustada mitte kehtestada halduskaristusi või parandusmeetmeid käsitlevaid õigusnorme selliste rikkumiste suhtes, mille suhtes kohaldatakse siseriiklikus õiguses kriminaalkaristusi.

2. Kui liikmesriigid on otsustanud kehtestada kriminaalkaristused käesoleva määruse rikkumise eest, tagavad nad asjakohaste abinõude kasutuselevõtu, nii et pädevatel asutustel oleksid kõik vajalikud volitused suhelda oma jurisdiktsiooni piires kohtute, prokuratuuri või kriminaalõigusasutustega, et saada konkreetset teavet käesolevas määruses osutatud rikkumiste asjus algatatud kriminaaluurimiste või menetluste kohta, ning anda sama teavet teistele pädevatele asutustele ja EBA-le, ESMA-le või EIOPA-le, et täita käesoleva määruse kohast koostöökohustust.

Artikkel 47

Teatamiskohustus

Liikmesriigid teavitavad komisjoni, ESMAt, EBAt ja EIOPAt oma õigus- ja haldusnormidest, millega võetakse üle käesolev peatükk, sealhulgas asjaomastest kriminaalõiguse sätetest hiljemalt [*ELT: palun lisada kuupäev: 1 aasta pärast jõustumist*]. Liikmesriigid teatavad komisjonile, ESMA-le, EBA-le ja EIOPA-le kõikidest nende õigusnormide hilisematest muudatustest ilma põhjendamatu viivituseta.

Artikkel 48

Halduskaristuste avaldamine

1. Pädevad asutused avaldavad oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud.

2. Lõike 1 kohasel karistuste avaldamisel tuleb avaldada teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused.

3. Kui pädev asutus leiab pärast juhtumipõhist hindamist, et juriidilise isiku identiteedi või füüsilise isiku identiteedi ja isikuandmete avaldamine oleks ebaproportsionaalne, ohustaks finantsturgude stabiilsust või käimasolevat kriminaaluurimist või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju, niivõrd kui seda on võimalik kindlaks teha, võtab ta halduskaristuse määramise otsuse suhtes vastu ühe järgmistest võimalustest:

   (a) lükata otsuse avaldamine edasi seni, kuni kõik mitteavaldamise põhjused langevad ära;

   (b) avaldada see anonüümselt kooskõlas siseriikliku õigusega või

   (c) hoiduda selle avaldamisest, kui punktides a ja b sätestatud võimalusi peetakse kas ebapiisavaks, et tagada ohtude puudumine finantsturgude stabiilsusele, või kui selline avaldamine ei oleks proportsionaalne määratud karistuse leebema kohtlemisega.

4. Kui halduskaristuse määramise otsus otsustatakse avaldada kooskõlas lõike 3 punktiga b anonüümselt, võib asjaomaste andmete avaldamise edasi lükata.

5. Kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtu otsus, millega tühistatakse halduskaristuse määramise otsus.

6. Pädevad asutused tagavad, et lõigete 1–4 kohaselt avaldatud andmed jäävad nende ametlikule veebisaidile vähemalt viieks aastaks alates nende avaldamisest. Avaldatud

isikuandmeid hoitakse pädeva asutuse veebisaidil ainult nii kaua, kui see on vajalik vastavalt kohaldatavatele andmekaitsenormidele.

Artikkel 49

Ametisaladus

1. Käesoleva määruse kohaselt saadud, vahetatud või edastatud konfidentsiaalse teabe suhtes kehtib lõikes 2 sätestatud ametisaladuse hoidmise kohustus.
2. Ametisaladuse hoidmise kohustus kehtib kõigile isikutele, kes töötavad või on töötanud käesoleva määruse alusel pädeva asutuse heaks või mõne ametiasutuse või turul tegutseva ettevõtja või füüsilise või juriidilise isiku heaks, kellele need pädevad asutused on ülesandeid delegeerinud, sealhulgas pädevate asutuste lepingulised audiitorid ja eksperdid.
3. Ametisaladuse alla kuuluvat teavet ei tohi avalikustada ühelegi teisele isikule ega ametiasutusele, välja arvatud juhul, kui avalikustamise kohustus tuleneb liidu või liikmesriigi õigusest.
4. Kogu käesoleva määruse kohaselt pädevate asutuste vahel vahetatavat teavet, mis puudutab äri- või töötingimusi ja muid majanduslikke või isiklikke küsimusi, peetakse konfidentsiaalseks ja selle suhtes kohaldatakse ametisaladuse nõudeid, välja arvatud juhul, kui pädev asutus märgib teavet edastades, et seda võib avaldada, või kui avalikustamine on vajalik tulenevalt kohtumenetlusest.

VIII PEATÜKK

DELEGEERITUD ÕIGUSAKTID

Artikkel 50

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.
2. Komisjonile antakse õigus võtta vastu artikli 28 lõikes 3 ja artikli 38 lõikes 2 osutatud delegeeritud õigusakte viieks aastaks alates *[väljaannete talitus: palun lisada kuupäev: 5 aastat pärast käesoleva määruse jõustumist]*.
3. Euroopa Parlament ja nõukogu võivad artikli 28 lõikes 3 ja artikli 38 lõikes 2 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse selles otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.
4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetega iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle samal ajal teatavaks Euroopa Parlamendile ja nõukogule.

6. Artikli 28 lõike 3 ja artikli 38 lõike 2 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kahe kuu võrra.

IX PEATÜKK

ÜLEMINEKU- JA LÕPPSÄTTED

I JAGU

Artikkel 51

Läbivaatamisklausel

Komisjon teeb hiljemalt [*väljaannete talitus: palun lisada kuupäev: 5 aastat pärast käesoleva määruse jõustumist*] ning pärast konsulteerimist vastavalt EBA, ESMA, EIOPA ja Euroopa Süsteemsete Riskide Nõukoguga läbivaatamise ning esitab Euroopa Parlamendile ja nõukogule aruande, millele lisatakse vajaduse korral seadusandlik ettepanek, milles käsitletakse artikli 28 lõikes 2 sätestatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kindlaksmääramise kriteeriume.

II JAGU

MUUDATUSED

Artikkel 52

Määruse (EÜ) nr 1060/2009 muutmine

Määruse (EÜ) nr 1060/2009 I lisa A jao lõike 4 esimene lõik asendatakse järgmisega:

„Reitinguagentuuril on usaldusväärne haldus- ja arvestuskord, sisekontrollimehhanismid, tulemuslikud riskianalüüsi menetlused ning tulemuslik kontrolli- ja kaitsekord IKT-süsteemide haldamiseks vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2021/xx* [DORA].

* Euroopa Parlamendi ja nõukogu […] määrus (EL) 2021/xx (ELT L XX, PP.KK.AAAA, lk. X).“

Artikkel 53

Määruse (EL) nr 648/2012 muutmine

Määrust (EL) nr 648/2012 muudetakse järgmiselt.

(1) Artiklit 26 muudetakse järgmiselt:

(a) lõige 3 asendatakse järgmisega:

„3. Keskse vastaspoole organisatsiooniline struktuur peab olema selline, millega tagatakse, et teenuseid osutatakse ja tegevusi sooritatakse järjepidevalt ja korrektselt. Ta kasutab asjakohaseid ja proportsionaalseid süsteeme, ressursse ja protseduure, sealhulgas IKT-süsteeme, mida hallatakse vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2021/xx* [DORA].

* Euroopa Parlamendi ja nõukogu […] määrus (EL) 2021/xx (ELT L XX, PP.KK.AAAA, lk. X).“;

(b) lõige 6 jäetakse välja.

(2) Artiklit 34 muudetakse järgmiselt:

(a) lõige 1 asendatakse järgmisega:

„1. Keskne vastaspool kehtestab asjakohase talitluspidevuse kava ja avariitaastekava, mis hõlmab vastavalt määrusele (EL) 2021/XX [DORA] koostatud IKT talitluspidevuse ja taastekavu, ning rakendab ja säilitab neid, et tagada keskse vastaspoole funktsioonide säilitamine, tema tegevuste kiire taastamine ja kohustuste täitmine.“;

(b) lõike 3 esimene lõik asendatakse järgmisega:

„Selleks et tagada käesoleva artikli ühetaoline kohaldamine, töötab ESMA pärast EKPSi liikmetega konsulteerimist välja regulatiivsete tehniliste standardite eelnõu, milles täpsustatakse talitluspidevuse poliitika ja avariitaastekava (v.a IKT talitluspidevuse ja taastekavad) minimaalne sisu ning neile esitatavad nõuded.“

(3) Artikli 56 lõike 3 esimene lõik asendatakse järgmisega:

„3. Selleks et tagada käesoleva artikli ühetaoline kohaldamine, töötab ESMA välja regulatiivse tehnilise standardi eelnõu, milles täpsustatakse lõikes 1 osutatud registreerimistaotluse üksikasjad, v.a IKT-riski juhtimisega seotud nõuded.“

(4) Artikli 79 lõiked 1 ja 2 asendatakse järgmistega:

„1. Kauplemisteabehoidla tuvastab operatsiooniriski allikad ja töötab nende minimeerimiseks välja asjakohased süsteemid, kontrollid ja menetlused, sealhulgas vastavalt määrusele (EL) 2021/xx *[DORA]* hallatavad IKT-süsteemid.

2. Kauplemisteabehoidla kehtestab asjakohase talitluspidevuse poliitika ja avariitaastekava (sealhulgas vastavalt määrusele (EL) 2021/XX [DORA] koostatud IKT talitluspidevuse ja taastekavad) ning rakendab ja säilitab neid, et tagada kauplemisteabehoidla funktsioonide säilitamine, tema tegevuste kiire taastamine ja kohustuste täitmine.“

(5) Artikli 80 lõige 1 jäetakse välja.

Artikkel 54

Määruse (EL) nr 909/2014 muutmine

Määruse (EL) nr 909/2014 artiklit 45 muudetakse järgmiselt:

(1) lõige 1 asendatakse järgmisega:

„1. Keskdepositoorium tuvastab nii sisemised kui ka välised operatsiooniriski allikad ning minimeerib nende mõju asjakohaste IT-vahendite, -protsesside ja -põhimõtete rakendamise kaudu, mis on kehtestatud ja mida hallatakse vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) 2021/xx* [DORA], ning kõigi muud liiki operatsiooniriskide seisukohast asjakohaste vahendite, kontrollide ja menetluste kaudu, sealhulgas tema korraldatavate väärtpaberiarveldussüsteemide puhul.

* Euroopa Parlamendi ja nõukogu […] määrus (EL) 2021/xx (ELT L XX, PP.KK.AAAA, lk. X).“;

(2) lõige 2 jäetakse välja;

(3) lõiked 3 ja 4 asendatakse järgmisega:

„3. Keskdepositoorium kehtestab osutatavate teenuste ja iga korraldatava väärtpaberiarveldussüsteemi jaoks asjakohase talitluspidevuse kava ja avariitaastekava (sealhulgas vastavalt määrusele (EL) 2021/XX [DORA] koostatud IKT talitluspidevuse ja taastekavad) ning rakendab ja säilitab neid, et tagada teenuste jätkuv osutamine, tegevuste kiire taastamine ja keskdepositooriumi kohustuste täitmine sündmuste korral, mille puhul on märkimisväärne tegevuse katkemise oht.

4. Lõikes 3 osutatud kava võimaldab katkestuse korral taastada kõik tehingud ja liikmete positsioonid, et võimaldada keskdepositooriumi liikmetel jätkata kindlalt tegevust ja viia arveldus lõpule kavandatud kuupäeval, sealhulgas tagades, et kriitilise tähtsusega IT-süsteemid saaksid katkestuse korral kiiresti uuesti tööle hakata, nagu sätestatud määruse (EL) 2021/xx [DORA] artikli 11 lõigetes 5 ja 7.“;

(4) lõike 6 esimene lõik asendatakse järgmisega:

„Keskdepositoorium tuvastab, jälgib ja juhib riske, mille võivad tema tegevusele kaasa tuua tema korraldatavate väärtpaberiarveldussüsteemide peamised liikmed, samuti teenuste pakkujad ning muud keskdepositooriumid või muud turuinfrastruktuurid. Pädeva asutuse ja asjaomaste asutuste taotluse korral esitab ta neile teabe tuvastatud riskide kohta. Samuti teavitab ta pädevat asutust ja asjaomaseid asutusi viivitamata kõigist operatsioonidega seotud intsidentidest (v.a IKT-riskiga seotud intsidendid), mis tulenesid kõnealustest riskidest.“;

(5) lõike 7 esimene lõik asendatakse järgmisega:

„Euroopa Väärtpaberiturujärelevalve töötab tihedas koostöös EKPSi liikmetega välja regulatiivsete tehniliste standardite eelnõu, et täpsustada lõigetes 1 ja 6 osutatud operatsiooniriske (v.a IKT-riske), kõnealuste riskide testimise, kõrvaldamise või minimeerimise meetodeid, sealhulgas lõigetes 3 ja 4 osutatud talitluspidevuse strateegiat ja avariitaastekava ning nende hindamise meetodeid.“

Artikkel 55

Määruse (EL) nr 600/2014 muutmine

Määrust (EL) nr 600/2014 muudetakse järgmiselt.

(1) Artiklit 27g muudetakse järgmiselt:

(a) lõige 4 jäetakse välja;

(b) lõike 8 punkt c asendatakse järgmisega:

(c) „c) lõigetes 3 ja 5 sätestatud konkreetsed organisatsioonilised nõuded.“

(2) Artiklit 27h muudetakse järgmiselt:

(a) lõige 5 jäetakse välja;

(b) lõike 8 punkt e asendatakse järgmisega:

„e) lõikes 4 sätestatud konkreetsed organisatsioonilised nõuded.“

(3) Artiklit 27i muudetakse järgmiselt:

(a) lõige 3 jäetakse välja;

(b) lõike 5 punkt b asendatakse järgmisega:

„b) lõigetes 2 ja 4 sätestatud konkreetsed organisatsioonilised nõuded.“

Artikkel 56

Jõustumine ja kohaldamine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates [*väljaannete talitus*: *lisada kuupäev: 12 kuud pärast jõustumist*].

Artikleid 23 ja 24 kohaldatakse siiski alates *[väljaannete talitus: palun lisada kuupäev: 36 kuud pärast käesoleva määruse jõustumist]*.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Brüssel,

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*

FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad

1.3. Ettepaneku/algatuse liik

1.4. Eesmärgid

1.5. Ettepaneku/algatuse põhjendused

1.6. Ettepaneku/algatuse kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

2.2. Haldus- ja kontrollisüsteem(id)

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

3.2. Hinnanguline mõju assigneeringutele

3.2.1. Hinnanguline mõju assigneeringutele – ülevaade

3.2.2. Hinnanguline mõju assigneeringutele

3.2.3. Hinnanguline mõju inimressurssidele

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline osalus

3,3. Hinnanguline mõju tuludele

Lisa

Üldised eeldused

Järelevalvevolitused

FINANTSSELGITUS – ASUTUSED

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Ettepanek: Euroopa Parlamendi ja nõukogu määrus finantssektori digitaalse tegevuskerksuse kohta.

1.2. Asjaomased poliitikavaldkonnad

Poliitikavaldkond: finantsstabiilsus, finantsteenused ja kapitaliturgude liit

Tegevus: digitaalne tegevuskerksus

1.3. Ettepanek käsitleb:

☑ **uut meedet**

☐ **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[50]

☐ **olemasoleva meetme pikendamist**

☐ **ühe või mitme meetme ühendamist teise või uue meetmega**

1.4. Eesmärgid

1.4.1. Üldeesmärgid

Algatuse üldeesmärk on tugevdada ELi finantssektori ettevõtjate digitaalset tegevuskerksust, ühtlustada ja ajakohastada kehtivaid eeskirju ning lisada lünkade korral uusi nõudeid. See muudaks ka ühtse reeglistiku digitaalse mõõtme tõhusamaks.

Üldeesmärk koosneb laias laastus kolmest eesmärgist: 1) vähendada finantshäirete ja ebastabiilsuse ohtu, 2) vähendada halduskoormust ja suurendada järelevalve tulemuslikkust ning 3) suurendada tarbijate ja investorite kaitset.

1.4.2. Erieesmärgid

Ettepaneku erieesmärgid on järgmised:

käsitleda info- ja kommunikatsioonitehnoloogia (edaspidi „IKT“) riske terviklikumalt ja tugevdada finantssektori üldist digitaalset kerksust;

ühtlustada IKTga seotud intsidentidest teatamist ja vähendada aruandlusnõuete kattumist;

anda finantsjärelevalveasutustele juurdepääs teabele IKTga seotud intsidentide kohta;

tagada, et käesoleva ettepanekuga hõlmatud finantssektori ettevõtjad hindavad oma ennetus- ja kerksusmeetmete tulemuslikkust ning teevad kindlaks IKTga seotud haavatavused;

vähendada ühtse turu killustatust ja võimaldada testimistulemuste piiriülest tunnustamist;

tugevdada finantssektori ettevõtjate lepingupõhiseid kaitsemeetmeid IKT-teenuste kasutamisel, sealhulgas tegevuse edasiandmise eeskirjade puhul (reguleerides kolmandast isikust IKT-teenuste osutajate järelevalvet);

[50] Vastavalt finantsmääruse artikli 58 lõike 2 punktile a või b.

võimaldada järelevalvet kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate tegevuse üle; soodustada ohuteadmuse vahetamist finantssektoris.

1.4.3. Oodatavad tulemused ja mõju

Märkige, milline peaks olema ettepaneku/algatuse oodatav mõju toetusesaajatele/sihtrühmale.

Finantssektori digitaalset tegevuskerksust käsitlev õigusakt tagaks tervikliku raamistiku, mis hõlmab kõiki digitaalse tegevuskerksuse aspekte, ning oleks tõhus finantssektori üldise tegevuskerksuse parandamisel. See tagaks ühtse reeglistiku selguse ja ühtsuse.

Samuti muudaks see koostoime küberturvalisuse direktiivi ja selle läbivaatamisega selgemaks ja sidusamaks. See parandaks finantssektori ettevõtjate jaoks nende suhtes kehtivate digitaalset tegevuskerksust käsitlevate erinevate eeskirjade selgust, seda eelkõige nende finantssektori ettevõtjate jaoks, kellel on mitu tegevusluba ja kes tegutsevad ELi eri turgudel.

1.4.4. Tulemusnäitajad

Märkige, milliste näitajate abil jälgitakse edusamme ja saavutusi.

Võimalikud näitajad:

IKTga seotud intsidentide arv ELi finantssektoris ja nende mõju

Oluliste IKTga seotud intsidentide arv, millest on teatatud usaldatavusnõuete täitmise järelevalvet tegevatele asutustele

Nende finantssektori ettevõtjate arv, kellelt nõutaks ohuteabel põhinevate läbistustestide tegemist

Nende finantssektori ettevõtjate arv, kes kasutavad lepingu tüüptingimusi lepingupõhiste kokkulepete sõlmimiseks kolmandast isikust IKT-teenuste osutajatega

Euroopa järelevalveasutuste või usaldatavusnõuete täitmise järelevalvet tegevate asutuste järelevalve all olevate kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate arv

Ohuteadmuse jagamise lahendustes osalevate finantssektori ettevõtjate arv

Ametiasutuste arv, kes saavad aruandeid sama IKTga seotud intsidendi kohta

Piiriüleste ohuteabel põhinevate läbistustestide arv

1.5. Ettepaneku/algatuse põhjendused

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise üksikasjalik ajakava

Finantssektor sõltub suurel määral info- ja kommunikatsioonitehnoloogiast (IKT). Hoolimata märkimisväärsetest edusammudest, mis on tehtud tänu sihipärasele riiklikule ja Euroopa poliitikale ja seadusandlikele algatustele, on IKT-riskid jätkuvalt probleem liidu finantssüsteemi tegevuskerksuse, toimimise ja stabiilsuse jaoks. 2008. aasta finantskriisile järgnenud reformiga tugevdati peamiselt ELi finantssektori finantskerksust ja sooviti kaitsta ELi konkurentsivõimet ja stabiilsust majanduslikust, usaldatavusnõuete ja turukäitumise seisukohast. Kuigi IKT turvalisus ja üldine digitaalne tegevuskerksus on osa operatsiooniriskist, on kriisijärgses regulatiivses tegevuskavas pööratud nendele vähem tähelepanu ning neid on edasi arendatud ainult mõnes liidu finantsturgude poliitika ja regulatiivses valdkonnas või ainult üksikutes liikmesriikides. See toob kaasa järgmised probleemid, mida tuleks ettepanekus käsitleda.

Kogu finantssektori IKT-riski ja tegevuskerksust hõlmav ELi õigusraamistik on killustunud ega ole täielikult järjepidev.

Kuna IKTga seotud intsidentidest teatamise nõuded ei ole järjepidevad, ei ole järelevalveasutustel täielikku ülevaadet intsidentide laadist, sagedusest, tähtsusest ja mõjust.

Mõned finantssektori ettevõtjad seisavad sama IKTga seotud intsidendi puhul silmitsi keerukate, kattuvate ja potentsiaalselt vastuoluliste aruandlusnõuetega.

Ebapiisav teabevahetus ja koostöö küberohte käsitleva teadmuse valdkonnas strateegilisel, taktikalisel ja tegevustasandil ei lase üksikutel finantssektori ettevõtjatel küberohtusid asjakohaselt hinnata, jälgida, end nende eest kaitsta ega neile reageerida.

Mõnes finantssektori allsektoris võib olla mitmeid ja omavahel kooskõlastamata läbistus- ja kerksustestimise raamistikke, millele lisandub tulemuste piiriülese tunnustamise puudumine, ning mõningates allsektorites ei olegi selliseid testimisraamistikke.

Järelevalveasutuste ülevaate puudumine sellisest finantssektori ettevõtjate tegevusest, mis on edasi antud kolmandast isikust IKT-teenuste osutajale, avab finantssektori ettevõtjad eraldi ja kogu finantssüsteemi tervikuna operatsiooniriskidele.

Finantsjärelevalveasutustel ei ole piisavaid volitusi ega vahendeid, et jälgida ja juhtida kontsentratsiooni- ja süsteemseid riske, mis tulenevad finantssektori ettevõtjate tuginemisest kolmandast isikust IKT-teenuste osutajatele.

1.5.2. ELi meetme lisaväärtus (see võib tuleneda erinevatest teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus“ väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid muidu üksi loonud.

ELi tasandi meetme põhjused (ex ante):

Digitaalne tegevuskerksus on ELi finantsturgudele ühist huvi pakkuv küsimus. ELi tasandil võetavad meetmed annaksid riigiti võetavatest meetmetest rohkem kasu ja neil oleks suurem väärtus. Ilma IKT-riski käsitlevate tegevussätete lisamiseta pakuks ühtne reeglistik vahendeid kõigi muude riskidega tegelemiseks Euroopa tasandil, kuid jätaks välja digitaalse tegevuskerksuse aspektid või jätaks need reguleerida riikliku tasandi algatustele, mis on killustatud ja kooskõlastamata. Ettepanek annaks õigusselguse selle kohta, kas ja kuidas kohaldatakse digitaalse tegevuse sätteid, eelkõige piiriüleste finantssektori ettevõtjate suhtes, ning kaotaks vajaduse, et iga liikmesriik eraldi parandaks tegevuskerksust ja küberturvalisust käsitlevaid eeskirju, standardeid ja eeldusi, et reageerida ELi eeskirjade praegusele piiratud ulatusele ja küberturvalisuse direktiivi üldisele olemusele.

Oodatav tekkiv liidu lisaväärtus (ex post):

Liidu sekkumine suurendaks märkimisväärselt poliitika tulemuslikkust, vähendades samal ajal keerukust ning kõikide finantssektori ettevõtjate finants- ja halduskoormust. Sellega ühtlustataks majandusvaldkonda, mis on nii tihedalt seotud ja integreeritud ning mille suhtes juba kohaldatakse ühtseid eeskirju ja järelevalvet. Mis puutub IKTga seotud intsidentidest teatamisse, siis ettepanek vähendaks erinevatele ELi ja/või riiklikele asutustele samast IKTga seotud intsidendist teatamise koormust ja kaudseid kulusid. Samuti hõlbustab see piiriüleselt tegutsevate ettevõtjate puhul, kelle suhtes kohaldatakse eri liikmesriikides eri testimisraamistikke, testimistulemuste vastastikust tunnustamist/aktsepteerimist.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Uus algatus

1.5.4. Kooskõla mitmeaastase finantsraamistikuga ja võimalik koostoime muude asjaomaste meetmetega

Käesoleva ettepaneku eesmärk on kooskõlas mitme muu ELi poliitika ja käimasoleva algatusega, eelkõige küberturvalisuse direktiivi ning Euroopa elutähtsate infrastruktuuride direktiiviga. Ettepanekuga säilitataks küberturvalisuse horisontaalse raamistikuga seonduv kasu, jättes kolm finantssektori allsektorit küberturvalisuse direktiivi kohaldamisalasse. Jäädes küberturvalisuse ökosüsteemiga seotuks, saaksid finantsjärelevalveasutused vahetada asjakohast teavet selle valdkonna ametiasutustega ning osaleda võrgu- ja infoturbe koostöörühmas. Ettepanek ei mõjutaks küberturvalisuse direktiivi, vaid pigem tugineks sellele ja käsitleks võimalikke kattumisi *lex specialis*'e alusel. Finantsteenuste määruse ja küberturvalisuse direktiivi koostoimet reguleeriks jätkuvalt *lex specialis*, mis vabastaks finantssektori ettevõtjad küberturvalisuse direktiivi sisulistest nõuetest ning väldiks nende kahe õigusakti kattumist. Lisaks on ettepanek kooskõlas Euroopa elutähtsate infrastruktuuride direktiiviga, mida vaadatakse praegu läbi, et suurendada elutähtsate infrastruktuuride kaitset ja vastupidavust mitteküberohtudele.

Käesolev ettepanek ei mõjutaks mitmeaastast finantsraamistikku. Esiteks rahastatakse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalveraamistikku täielikult nendelt teenuseosutajatelt võetavatest tasudest; teiseks tagatakse Euroopa järelevalveasutustele usaldatud nende täiendavate regulatiivsete ülesannete täitmine, mis on seotud digitaalse tegevuskerksusega, olemasolevate töötajate sisemise ümberpaigutamisega.

Sellest lähtudes tehakse ettepanek suurendada tulevase iga-aastase eelarvemenetluse käigus ameti volitatud töötajate arvu. Amet jätkab tööd selle nimel, et maksimeerida (muu hulgas IT-süsteemide kaudu) sünergia ja tõhusus, ning jälgib tähelepanelikult käesoleva ettepanekuga seotud täiendavat töökoormust, mis kajastub ameti poolt iga-aastase eelarvemenetluse käigus taotletavas volitatud töötajate arvus.

1.5.5. Erinevate kasutada olevate rahastamisvõimaluste, sealhulgas vahendite ümberpaigutamise võimaluste hinnang

Kaaluti mitut rahastamisvõimalust.

Esiteks saaks lisakulusid rahastada Euroopa järelevalveasutuste tavapärase rahastamismehhanismi kaudu. See tooks aga kaasa märkimisväärselt suurema ELi panuse Euroopa järelevalveasutuste rahalistesse vahenditesse.

See võimalus on valitud käesoleva ettepanekuga seotud regulatiivsete ülesannetega seonduvate kulude jaoks. Euroopa järelevalveasutustel palutakse seega paigutada ümber olemasolevad töötajad, et töötada välja mitu tehnilist standardit. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevalvega seotud lisakulusid ei oleks siiski võimalik katta vahendite ümberpaigutamise teel Euroopa järelevalveasutustes, kellel on lisaks käesolevas ettepanekus ja muudes liidu õigusaktides kavandatud ülesannetele ka muid ülesandeid. Lisaks nõuavad digitaalse tegevuskerksusega seotud järelevalveülesanded spetsiifilisi tehnilisi teadmisi ja oskusteavet. Kuna selliste ressursside praegune tase Euroopa järelevalveasutustes ei ole piisav, on vaja lisavahendeid.

Ettepaneku kohaselt nõutakse tasu järelevalve alla kuuluvatelt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt. Need peaksid katma kõik täiendavad ressursid, mida Euroopa järelevalveasutused vajavad oma uute ülesannete ja volituste täitmiseks.

1.6. Ettepaneku/algatuse kestus ja finantsmõju

☐ **Piiratud kestusega**

☐ Ettepanek/algatus hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

☐ Finantsmõju avaldub ajavahemikul AAAA–AAAA

☑ **Piiramatu kestusega**

Rakendamise käivitumisperiood hõlmab ajavahemikku alates 2021. aastast,

millele järgneb täieulatuslik rakendamine.

1.7. Ettenähtud eelarve täitmise viisid[51]

Eelarve otsene täitmine komisjoni poolt

☐ täitevasutuste kaudu

☐ **Eelarve jagatud täitmine** koostöös liikmesriikidega

☑ **Eelarve kaudne täitmine**, mille puhul eelarve täitmise ülesanded on delegeeritud:

☐ rahvusvahelistele organisatsioonidele ja nende allasutustele (nimetage);

☐ Euroopa Investeerimispangale ja Euroopa Investeerimisfondile;

☑ finantsmääruse artiklites 70 ja 71 osutatud asutustele;

☐ avalik-õiguslikele asutustele;

☐ avalikke teenuseid osutavatele eraõiguslikele asutustele, kuivõrd nad esitavad piisavad finantstagatised;

☐ liikmesriigi eraõigusega reguleeritud asutustele, kellele on delegeeritud avaliku ja erasektori partnerluse rakendamine ja kes esitavad piisavad finantstagatised;

☐ isikutele, kellele on delegeeritud Euroopa Liidu lepingu V jaotise kohaste ÜVJP erimeetmete rakendamine ja kes on kindlaks määratud asjaomases alusaktis.

Märkused

Ei kohaldata.

[51] Eelarve täitmise viise koos viidetega finantsmäärusele on selgitatud veebisaidil https://myintracomm.ec.europa.eu/budgweb/ET/man/budgmanag/Pages/budgmanag.aspx.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Märkige sagedus ja tingimused.

Kooskõlas kehtiva korraga koostavad Euroopa järelevalveasutused korrapäraselt oma tegevuse kohta aruandeid (sealhulgas sisearuanded kõrgemale juhtkonnale, aruanded juhatusele ja aastaaruande koostamine) ning kontrollikoda ja komisjoni siseauditi talitus korraldavad auditid nende vahendite kasutamise ja tegevuse tulemuslikkuse kohta. Ettepanekuga hõlmatud meetmete üle tehakse järelevalvet ja nende kohta esitatakse aruandeid kooskõlas juba kehtivate nõuetega, aga ka käesolevast ettepanekust tulenevate uute nõuetega.

2.2. Haldus- ja kontrollisüsteem(id)

2.2.1. Eelarve täitmise viisi(de), rahastamise rakendamise mehhanismi(de), maksete tegemise korra ja kavandatava kontrollistrateegia selgitus.

Haldamine toimub kaudselt Euroopa järelevalveasutuste kaudu. Rahastamismehhanismi rakendataks asjaomastelt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt võetavate tasude kaudu.

2.2.2. Teave kindlakstehtud riskide ja nende vähendamiseks kasutusele võetud sisekontrollisüsteemi(de) kohta

Eeldatakse, et käesoleva ettepanekuga ette nähtud assigneeringute kasutamisel ei kaasne õiguspärasuse, säästlikkuse, tõhususe ja tulemuslikkuse seisukohast uusi olulisi riske, mis ei ole kaetud olemasoleva sisekontrolli raamistikuga. Uus probleem võib aga olla seotud selle tagamisega, et tasud kogutakse asjaomastelt kriitilise tähtsusega kolmandast isiksust IKT-teenuste osutajatelt õigeaegselt.

2.2.3. Kontrollide kulutõhususe (kontrollikulude suhe hallatavate vahendite väärtusse) hinnang ja põhjendus ning prognoositav veariski tase (maksete tegemise ja sulgemise ajal).

Euroopa järelevalveasutuste määrustega ette nähtud juhtimis- ja kontrollisüsteemid on juba rakendatud. Euroopa järelevalveasutused teevad tihedalt koostööd komisjoni siseauditi talitusega, et tagada asjakohaste nõuete täitmine kõigis sisekontrolli raamistiku valdkondades. Seda korda kohaldatakse Euroopa järelevalveasutuste suhtes ka seoses rolliga, mis on neile käesoleva ettepanekuga antud. Lisaks sellele annab Euroopa Parlament igal eelarveaastal nõukogu soovituse põhjal kinnituse iga Euroopa järelevalveasutuse tegevusele asjaomase eelarve täitmisel.

2.3. Pettuse ja eeskirjade eiramise ärahoidmise meetmed

Nimetage rakendatavad või kavandatud ennetus- ja kaitsemeetmed, nt pettustevastase võitluse strateegias esitatud meetmed.

Pettuse, korruptsiooni ja muu ebaseadusliku tegevuse vastu võitlemiseks kohaldatakse Euroopa järelevalveasutuste suhtes piiranguteta Euroopa Parlamendi ja nõukogu 11. septembri 2013. aasta määrust (EL, Euratom) nr 883/2013 Euroopa Pettustevastase Ameti (OLAF) juurdluste kohta.

Euroopa järelevalveasutustel on spetsiaalne pettustevastase võitluse strateegia ja sellest tulenev tegevuskava. Euroopa järelevalveasutuste tugevdatud meetmed pettustevastase võitluse valdkonnas on kooskõlas finantsmääruses sätestatud eeskirjade ja suunistega (pettusevastased meetmed usaldusväärse finantsjuhtimise osana), OLAFi pettuste ärahoidmise põhimõtetega ning komisjoni pettustevastase võitluse strateegia (COM(2011) 376) ja ELi detsentraliseeritud asutusi käsitleva ühise lähenemisviisi (juuli 2012) ning asjaomase tegevuskava põhimõtetega.

Lisaks sellele sisaldavad nii Euroopa järelevalveasutuste asutamismäärused kui ka Euroopa järelevalveasutuste finantsmäärused sätteid Euroopa järelevalveasutuste eelarvete täitmise ja kontrolli kohta ning kohaldatavaid finantseeskirju, sealhulgas neid, mille eesmärk on pettuste ja eeskirjade eiramise ärahoidmine.

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata[52]	EFTA riigid[53]	kandidaatriigid[54]	kolmanda riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses

Uued eelarveread, mille loomist taotletakse

Järjestage mitmeaastase finantsraamistiku rubriigiti ja iga rubriigi sees eelarveridade kaupa

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr	Liigendatud/liigendamata	EFTA riigid	kandidaatriigid	kolmanda riigid	finantsmääruse artikli 21 lõike 2 punkti b tähenduses

[52] Liigendatud = liigendatud assigneeringud / liigendamata = liigendamata assigneeringud.

[53] EFTA: Euroopa Vabakaubanduse Assotsiatsioon.

[54] Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

3.2. Hinnanguline mõju assigneeringutele

3.3. Hinnanguline mõju assigneeringutele – ülevaade

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik	Nr	Rubriik

<….> peadirektoraat			2020	2021	2022	2023	2024	2025	2026	2027	**KOKKU**
	Kulukohustused	(1)									
	Maksed	(2)									
<….> peadirektoraadi assigneeringud KOKKU	Kulukohustused										
	Maksed										

Mitmeaastase finantsraamistiku rubriik		

miljonites eurodes (kolm kohta pärast koma)

		2022	2023	2024	2025	2026	2027	**KOKKU**
Peadirektoraadid:								
• Personalikulud								
• Muud halduskulud <>								
Peadirektoraadid KOKKU	Assigneeringud							

Mitmeaastase finantsraamistiku **RUBRIIGI <….> assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)							

miljonites eurodes püsivhindades (kolm kohta pärast koma)

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIGI 1 assigneeringud KOKKU**	Kulukohustused							
	Maksed							

3.3.1. Hinnanguline mõju assigneeringutele

☑ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

☐ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

kulukohustuste assigneeringud miljonites eurodes püsivhindades (kolm kohta pärast koma)

Märkige eesmärgid ja väljundid ⇩			2022		2023		2024		2025		2026		2027		**KOKKU**	
	VÄLJUNDID															
	Liik[55]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[56]...																
- Väljund																
Erieesmärk nr 1 kokku																
ERIEESMÄRK nr 2																
- Väljund																
Erieesmärk nr 2 kokku																
KULUD KOKKU																

55 Väljunditena käsitatakse tarnitavaid tooteid ja osutatavaid teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

56 Vastavalt punktile 1.4.2. „Erieesmärk/erieesmärgid…“.

3.3.2. Hinnanguline mõju inimressurssidele

3.3.2.1. Kokkuvõte

☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

☑ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes püsivhindades (kolm kohta pärast koma)

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**KOKKU**
Ajutised töötajad (AD palgaastmed)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Ajutised töötajad (AST palgaastmed)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Lepingulised töötajad							
Riikide lähetatud eksperdid							
KOKKU	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Personalivajadused (täistööajale taandatud töötajad):

EBA, EIOPA ja ESMA	2022	2023	2024	2025	2026	2027	**KOKKU**
Ajutised töötajad (AD palgaastmed) EBA=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Ajutised töötajad (AST palgaastmed) EBA=1, EIOPA=1, ESMA=1	3	3	3	3	3	3	3
Lepingulised töötajad							
Riikide lähetatud eksperdid							
KOKKU	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. (Vastutava) peadirektoraadi hinnanguline personalivajadus

☑ Ettepanek/algatus ei hõlma personali kasutamist.

☐ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Hinnanguline väärtus täisarvuna (või maksimaalselt ühe kohaga pärast koma)

		2022	2023	2024	2025	2026	2027
• **Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)**							
• **Koosseisuväline personal (täistööajale taandatud töötajad)**[57]							
XX 01 02 01 (üldvahenditest rahastatavad lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud)							
XX 01 02 02 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored spetsialistid delegatsioonides)							
XX 01 04 ***yy***[58]	- peakorteris[59]						
	- delegatsioonides						
XX 01 05 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)							
10 01 05 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)							
Muud eelarveread (märkige)							
KOKKU							

XX tähistab asjaomast poliitikavaldkonda või eelarvejaotist.

Personalivajadused kaetakse juba meedet haldavate peadirektoraadi töötajatega ja/või töötajate peadirektoraadi sisese ümberpaigutamise teel. Vajaduse korral võidakse personali täiendada iga-aastase vahendite eraldamise menetluse käigus, arvestades olemasolevate eelarvepiirangutega.

Ülesannete kirjeldus:

[57] Lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud, noored spetsialistid delegatsioonides.

[58] Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised B..A read).

[59] Peamiselt struktuurifondid, Euroopa Maaelu Arengu Põllumajandusfond (EAFRD) ja Euroopa Kalandusfond (EFF).

Ametnikud ja ajutised töötajad	
Koosseisuvälised töötajad	

V lisa punktis 3 tuleks esitada täistööajale taandatud töötajate kulude arvutamise meetodi kirjeldus.

3.3.3. Kooskõla kehtiva mitmeaastase finantsraamistikuga

☑ Ettepanek/algatus on kooskõlas kehtiva mitmeaastase finantsraamistikuga.

☐ Ettepanekuga/algatusega kaasneb mitmeaastase finantsraamistiku asjaomase rubriigi ümberplaneerimine.

☐ Ettepanek/algatus eeldab paindlikkusinstrumendi kohaldamist või mitmeaastase finantsraamistiku muutmist[60].

Selgitage, millised toimingud on vajalikud, osutades asjaomastele rubriikidele, eelarveridadele ja summadele. [...]

3.3.4. Kolmandate isikute rahaline osalus

☐ Ettepanek/algatus ei hõlma kolmandate isikute poolset kaasrahastamist.

☑ Ettepanek/algatus hõlmab kaasrahastamist, mille hinnanguline summa on järgmine:

miljonites eurodes (kolm kohta pärast koma)

EBA

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kaasrahastatavad assigneeringud KOKKU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Kaasrahastatavad assigneeringud KOKKU	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Vt nõukogu määruse (EL, Euratom) nr 1311/2013 (millega määratakse kindlaks mitmeaastane finantsraamistik aastateks 2014–2020) artiklid 11 ja 17.

61 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.

62 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kaasrahastatavad assigneeringud KOKKU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Hinnanguline mõju tuludele

☑ Ettepanekul/algatusel puudub finantsmõju tuludele

☐ Ettepanekul/algatusel on järgmine finantsmõju:

☐ omavahenditele

☐ muudele tuludele

☐ palun märkige, kas see on kulude eelarveridasid mõjutav sihtotstarbeline tulu

miljonites eurodes (kolm kohta pärast koma)

Tulude eelarverida:	Jooksva aasta eelarves kättesaadavad assigneeringud	Ettepaneku/algatuse mõju[64]						
		Aasta **N**	Aasta **N+1**	Aasta **N+2**	Aasta **N+3**	Lisage vajalik arv aastaid, et kajastada kogu finantsmõju kestust (vt punkt 1.6)		
Artikkel …….								

Mitmesuguste sihtotstarbeliste tulude puhul täpsustage, milliseid kulude eelarveridasid ettepanek mõjutab.

[...]

Täpsustage tuludele avaldatava mõju arvutamise meetod.

[...]

63 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.

64 Traditsiooniliste omavahendite (tollimaksud ja suhkrumaksud) korral tuleb märkida netosummad, s.t brutosumma pärast 20 % sissenõudmiskulude mahaarvamist.

LISA

Üldised eeldused

I jaotis – Personalikulud

Personalikulude arvutamisel on kasutatud järgmisi konkreetseid eeldusi, mis põhinevad allpool selgitatud personalivajadustel.

- 2022. aastal tööle võetavate lisatöötajate kulud hõlmavad kuut kuud, võttes arvesse lisatöötajate töölevõtmiseks eeldatavalt kuluvat aega.
- Ajutise töötaja keskmine aastane kulu on 150 000 eurot, mis sisaldab 25 000 eurot ametiruumidega seotud kulusid (hooned, IT jne).
- Töötajate palkade suhtes kohaldatavad paranduskoefitsiendid Pariisis (EBA ja ESMA) ja Frankfurdis (EIOPA) on vastavalt 117,7 ja 99,4.
- Ajutiste töötajate tööandja pensionimaksed põhinevad standardsetel põhipalkadel, mis sisalduvad standardsetes keskmistes aastakuludes, milleks on 95 660 eurot.
- Täiendavad ajutised teenistujad on AD5 palgaastmel või tegevusüksuses AST.

II jaotis – Taristu- ja tegevuskulud

Kulude arvutamisel korrutatakse töötajate arv töötatud osaga aastast ja ametiruumidega seotud standardkuludega (25 000 eurot).

III jaotis – Tegevuskulud

Kulude hindamisel lähtutakse järgmistest eeldustest.

- Tõlkekuludeks on määratud 350 000 eurot aastas iga Euroopa järelevalveasutuse kohta.
- Eeldatakse, et ühekordseid IT-kulusid 500 000 eurot ESA kohta rakendatakse kahe aasta jooksul (aastatel 2022 ja 2023), jagades summa aastate vahel võrdselt. Iga-aastased hoolduskulud on alates 2024. aastast hinnanguliselt 50 000 eurot iga Euroopa järelevalveasutuse kohta.
- Iga-aastased kohapealse järelevalve kulud on hinnanguliselt 200 000 eurot iga Euroopa järelevalveasutuse kohta.

Eespool esitatud hinnangute põhjal on aastased kulud järgmised:

Mitmeaastase finantsraamistiku rubriik	Nr	

Püsivhinnad

EBA			2022	2023	2024	2025	2026	2027	**KOKKU**
Jaotis 1:	Kulukohustused	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Maksed	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Jaotis 2:	Kulukohustused	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksed	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Jaotis 3:	Kulukohustused	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksed	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
EBA assigneeringud KOKKU	Kulukohustused	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Maksed	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA			2022	2023	2024	2025	2026	2027	**KOKKU**
Jaotis 1:	Kulukohustused	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Maksed	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Jaotis 2:	Kulukohustused	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksed	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Jaotis 3:	Kulukohustused	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksed	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000

EIOPA assigneeringud KOKKU	Kulukohustused	=1+1a+3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Maksed	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA			2022	2023	2024	2025	2026	2027	**KOKKU**
Jaotis 1:	Kulukohustused	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Maksed	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Jaotis 2:	Kulukohustused	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Maksed	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Jaotis 3:	Kulukohustused	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Maksed	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
ESMA assigneeringud KOKKU	Kulukohustused	=1+1a+3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Maksed	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Ettepanek hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

kulukohustuste assigneeringud miljonites eurodes püsivhindades (kolm kohta pärast koma)

EBA

Märkige eesmärgid ja väljundid ⇩			2022		2023		2024		2025		2026		2027			
	VÄLJUNDID															
	Liik[65]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[66]: otsene järelevalve kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle																
- Väljund				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Erieesmärk nr 1 kokku																
ERIEESMÄRK nr 2																
- Väljund																
Erieesmärk nr 2 kokku																
KULUD KOKKU				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Märkige eesmärgid ja väljundid ⇩			2022		2023		2024		2025		2026		2027			
	VÄLJUNDID															
	Liik[67]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[68]: otsene järelevalve kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle																

[65] Väljunditena käsitatakse tarnitavaid tooteid ja osutatavaid teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

[66] Vastavalt punktile 1.4.2. „Erieesmärk/erieesmärgid…“.

[67] Väljunditena käsitatakse tarnitavaid tooteid ja osutatavaid teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

[68] Vastavalt punktile 1.4.2. „Erieesmärk/erieesmärgid…“.

- Väljund				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Erieesmärk nr 1 kokku																
ERIEESMÄRK nr 2																
- Väljund																
Erieesmärk nr 2 kokku																
KULUD KOKKU				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Märkige eesmärgid ja väljundid ⇩			2022		2023		2024		2025		2026		2027			
	VÄLJUNDID															
	Liik[69]	Keskmine kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 1[70]: otsene järelevalve kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle																
- Väljund				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Erieesmärk nr 1 kokku																
ERIEESMÄRK nr 2																
- Väljund																
Erieesmärk nr 2 kokku																
KULUD KOKKU				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Väljunditena käsitatakse tarnitavaid tooteid ja osutatavaid teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

[70] Vastavalt punktile 1.4.2. „Erieesmärk/erieesmärgid…“.

Järelevalvetegevuse kulud kaetakse täielikult järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest:

EBA

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kaasrahastatavad assigneeringud KOKKU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
Kaasrahastatavad assigneeringud KOKKU	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Kokku
Kulud kaetakse 100 % järelevalve alla kuuluvatelt ettevõtjatelt nõutavatest tasudest[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
Kaasrahastatavad assigneeringud KOKKU	1,373	1,948	1,748	1,748	1,748	1,748	10,313

SPETSIIFILINE TEAVE

Otsese järelevalve volitused

Sissejuhatuseks tuleks meenutada, et ESMA otsese järelevalve alla kuuluvad ettevõtjad peaksid maksma ESMA-le tasu (ühekordne registreerimiskulu ja korduv pideva järelevalve kulu). See puudutab

[71] 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.
[72] 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.
[73] 100 % hinnangulisest kogumaksumusest pluss tööandja täielikud pensionimaksed.

reitinguagentuure (vt komisjoni delegeeritud määrus (EL) nr 272/2012) ja kauplemisteabehoidlaid (komisjoni delegeeritud määrus (EL) nr 1003/2013).

Käesoleva seadusandliku ettepaneku kohaselt antakse Euroopa järelevalveasutustele uued ülesanded, mille eesmärk on ühtlustada finantssektoris kolmandast isikust tulenevat IKT-riski käsitlevaid järelevalvealaseid lähenemisviise, kohaldades kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes liidu järelevalveraamistikku.

Käesoleva ettepaneku kohane järelevalveraamistik toetub finantsteenuste valdkonna praegusele institutsioonilisele struktuurile, mis tähendab, et Euroopa järelevalveasutuste ühiskomitee tagab valdkondadevahelise koordineerimise kõigis IKT-riskiga seotud küsimustes kooskõlas oma küberturvalisust puudutavate ülesannetega ja teda toetab asjaomane allkomitee (järelevalvefoorum), mis valmistab ette kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele suunatud individuaalseid otsuseid ja ühissoovitusi.

Selle raamistiku kaudu saavad Euroopa järelevalveasutused, mis on määratud iga kõnealuse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja juhtivaks järelevalveasutuseks, õiguse tagada, et selliste tehnoloogiateenuse osutajate üle, mis mängivad finantssektori toimimises kriitilise tähtsusega rolli, tehakse üleeuroopaliselt piisavat järelevalvet. Järelevalveülesanded on sätestatud ettepanekus ja neid on täiendavalt selgitatud seletuskirjas. Need hõlmavad õigusi nõuda kogu asjakohast teavet ja dokumente, et viia läbi üldisi uurimisi ja kontrolle, esitada soovitusi ja seejärel aruandeid soovituste täitmiseks võetud meetmete või rakendatud parandusmeetmete kohta.

Käesoleva ettepanekuga kavandatud uute ülesannete täitmiseks võtavad Euroopa järelevalveasutused täiendavalt tööle töötajaid, kes on spetsialiseerunud IKT-riskidele ja keskenduvad kolmandatest isikutest sõltuvuse hindamisele.

Personalivajadus on hinnanguliselt 6 täistööajale taandatud töötajat iga asutuse kohta (5 AD ametikohta ja 1 AST ametikoht AD ametikohtade toetamiseks). Euroopa järelevalveasutused kannavad ka täiendavaid IT-kulusid, mis on hinnanguliselt 500 000 eurot ühekordseid kulusid ja 50 000 eurot aastas hoolduskulude katteks kõigil kolmel Euroopa järelevalveasutusel. Üks uute ülesannete oluline element on kohapealsed kontrollid ja auditid, mille kulud on hinnanguliselt 200 000 eurot aastas iga Euroopa järelevalveasutuse kohta. Selliste erinevate dokumentide tõlkimise kulud, mida Euroopa järelevalveasutused saaksid kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt, on samuti esitatud tegevuskulude real ja moodustavad 350 000 eurot aastas.

Kõik eespool nimetatud halduskulud kaetakse täielikult iga-aastastest tasudest, mida Euroopa järelevalveasutused nõuavad järelevalve alla kuuluvatelt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt (mõju ELi eelarvele puudub).