EUROOPA KESKPANGA ARVAMUS,

11. aprill 2022,

seoses ettepanekuga võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Sissejuhatus ja õiguslik alus

16. detsembril 2020 esitas Euroopa Komisjon ettepaneku võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148 ([1]) (edaspidi „kavandatav direktiiv"). 3. detsembril 2021 leppis Euroopa Liidu Nõukogu kavandatava direktiivi suhtes kokku üldises lähenemisviisis ([2]). Euroopa Keskpanga (EKP) arvamuse andmise pädevus põhineb Euroopa Liidu toimimise lepingu artikli 127 lõike 4 teisel lõigul, kuna kavandatav direktiiv sisaldab EKP pädevusse kuuluvaid sätteid, mis puudutavad eelkõige maksesüsteemide tõrgeteta toimimise edendamist, finantsturgude süsteemi stabiilsusega seotud pädevate asutuste poliitika sujuvale elluviimisele kaasaaitamist ning EKP ülesandeid seoses krediidiasutuste usaldatavusnõuete täitmise järelevalvega vastavalt aluslepingu artikli 127 lõike 2 neljandale taandele, artikli 127 lõikele 5 ja artikli 127 lõikele 6. EKP nõukogu on käesoleva arvamuse vastu võtnud kooskõlas Euroopa Keskpanga kodukorra artikli 17.5 esimese lausega.

Üldised märkused

EKP toetab kindlalt kavandatava direktiivi eesmärki suurendada kübervastupidavusvõimet kõigis asjaomastes sektorites, vähendada ebaühtlust siseturul ning suurendada olukorrateadlikkust ja ühist valmisolekut ning reageerimissuutlikkust, tagades tõhusa koostöö liidus.

EKP mõistab, kui oluline on säilitada tugevad sidemed kavandatava direktiivi ja finantssektori vahel, mis peaks jääma võrgu- ja infosüsteemide ökosüsteemi osaks, et edendada info- ja kommunikatsioonitehnoloogiaga (IKT) seotud riskide järjepidevat hindamist kogu liidus ning toetada tõhusat valdkondadevahelist teabevahetust ja koostööd küberohtude käsitlemisel. Selleks peaks pädevatel asutustel olema võimalik kavandatava Euroopa Parlamendi ja nõukogu määruse (finantssektori digitaalse tegevuskerksuse kohta) ([3]) (edaspidi „DORA määrus") alusel osaleda strateegilistes poliitilistes aruteludes ja võrgu- ja infoturbe koostöörühma tehnilises töös ning vahetada teavet ja teha täiendavat koostööd kavandatavas direktiivis ([4]) osutatud ühtsete kontaktpunktide ja riiklike küberturbe intsidentide lahendamise üksustega.

1. Kavandatava direktiivi kohaldamisala

1.1 EKP arusaama kohaselt käsitatakse DORA määrust finantssektori ettevõtjate puhul valdkondliku õigusaktina, millega kehtestatakse küberturvalisuse riskijuhtimise ja intsidentidest teatamise nõuded, mis on vähemalt samaväärsed kavandatavas direktiivis sätestatud nõuetega ([5]). Seetõttu ei kohaldata kavandatava direktiivi sätteid, mis on seotud küberturvalisuse riskijuhtimise, aruandluskohustuse, teabe jagamise ning järelevalve ja jõustamisega, ühegi DORA määrusega hõlmatud finantssektori ettevõtja suhtes ([6]). Nagu on selgitatud kavandatava direktiivi põhjendustes, tuleks kavandatava direktiivi sätete asemel kohaldada DORA määruse sätteid, mis on seotud IKT

([1]) COM(2020) 823 final.
([2]) Avaldatud nõukogu veebilehel www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Vt Euroopa Keskpanga arvamus CON/2021/20, 4. juuni 2021, seoses ettepanekuga Euroopa Parlamendi ja nõukogu määruse kohta, mis käsitleb finantssektori digitaalset tegevuskerksust (ELT C 343, 26.8.2021, lk 1), punkt 1.5.. Kõik EKP arvamused on avaldatud EUR-Lexis. DORA määruse artikli 17 lõige 5 ja artikkel 42; kavandatava direktiivi artikkel 11.
([5]) Kavandatava direktiivi artikli 2 lõige 6.
([6]) Kavandatava direktiivi põhjendus 13 ja artikli 2 lõige 6.

riskijuhtimise meetmetega, IKTga seotud intsidentide haldamise ja intsidentidest teatamisega, digitaalse tegevuskerksuse testimisega, teabevahetuskorraga ja kolmandate isikutega seotud IKT-riskidega ([7]).

1.2 Samuti märgib EKP, et nõukogu on oma üldises lähenemisviisis kavandatava direktiivi suhtes esitanud muudatusettepaneku jätta kavandatava direktiivi kohaldamisalast välja „üksused, kelle tegevus on seotud kohtusüsteemiga, parlamentide või keskpankadega“ ([8]). EKP arusaama kohaselt hõlmaks kavandatav muudatus kõiki Euroopa Keskpankade Süsteemi (EKPS) põhiülesandeid ja pädevusi, mis on sätestatud aluslepingu artikli 127 lõikes 2 ning Euroopa Keskpankade Süsteemi ja Euroopa Keskpanga põhikirja (edaspidi „EKPSi põhikiri“) artiklis 3.1, nagu näiteks maksesüsteemide tõrgeteta toimimise edendamine. Sellisel juhul oleksid eurosüsteemile kuuluvad ja eurosüsteemi hallatavad finantsturutaristud, nt TARGET2 ja TARGET2-Securities, hõlmatud nõukogu ettepanekuga jätta keskpangad kavandatava direktiivi kohaldamisalast välja.

2. **EKPSi ja eurosüsteemi järelevaatamispädevus**

2.1 Lisaks EKPSi peamisele eesmärgile säilitada hindade stabiilsus ning kooskõlas aluslepingu artikli 127 lõikega 2 on üks EKPSi kaudu täidetavatest põhiülesannetest edendada maksesüsteemide tõrgeteta toimimist ([9]). Selle põhiülesande täitmiseks võivad „EKP ja riikide keskpangad anda vahendeid ja EKP võib kehtestada eeskirju efektiivsete ja usaldatavate arveldus- ja maksesüsteemide tagamiseks liidu piires ja teiste riikidega“ ([10]). Oma järelevaatamisülesannete täitmise raames võttis EKP vastu Euroopa Keskpanga määruse (EL) nr 795/2014 (EKP/2014/28) ([11]) (edaspidi „süsteemselt oluliste maksesüsteemide määrus“), millega muudetakse CPSS-IOSCO finantsturutaristute põhimõtted ([12]) vahetult kohaldatavaks õiguseks. Süsteemselt oluliste maksesüsteemide määrusega sätestatakse nõuded nii riigi kui eraomandis olevatele suurmaksete süsteemidele ja süsteemselt olulistele jaemaksete süsteemidele. Süsteemselt oluliste maksesüsteemide määruse nõuded juba hõlmavad muu hulgas operatsiooniriski juhtimist ja küberkerksuse raamistiku loomist ([13]).

2.2 Lisaks süsteemselt olulistele maksesüsteemidele kuuluvad eurosüsteemi järelevaatamise alla ka süsteemselt mitteolulised maksesüsteemid, elektroonilised maksevahendid, -skeemid ja -kord ning muud taristud ja elutähtsate teenuste osutajaid, nagu on sätestatud eurosüsteemi järelevaatamispoliitika raamistikus ([14]). Maksesüsteemid ja muud eurosüsteemi järelevaatamise alla kuuluvad süsteemid ei ole kavandatava direktiiviga selgesõnaliselt hõlmatud ([15]). Arvestades, et kavandatav direktiiv on minimaalse ühtlustamise vahend ([16]), võivad liikmesriikide vastu võetud rakendusaktid lõpuks kattuda eurosüsteemi järelevaatamispädevusega. Selle vältimiseks tuleks kavandatava direktiivi põhjendustes selgesõnaliselt tunnustada asutamislepingust ja EKPSi põhikirjast tulenevat EKPSi pädevust ning süsteemselt oluliste maksesüsteemide määrusest ja üldisemalt eurosüsteemi järelevaatamispoliitika raamistikust tulenevat eurosüsteemi pädevust.

([7]) Kavandatava direktiivi põhjendus 13.
([8]) Kavandatavat direktiivi käsitleva nõukogu üldise lähenemisviisi artikli 2 lõike 3a esimese lõigu punkt b.
([9]) Euroopa Liidu toimimise lepingu artikli 127 lõige 2, nagu on sätestatud ka EKPSi põhikirja artiklis 3.1.
([10]) EKPSi põhikirja artikkel 22.
([11]) Euroopa Keskpanga määrus (EL) nr 795/2014, 3. juuli 2014, süsteemselt oluliste maksesüsteemide järelevaatamise kohta (EKP/2014/28) (ELT L 217, 23.7.2014, lk 16).
([12]) Vt makse- ja arveldussüsteemide komitee (CPSS) ja Rahvusvahelise Väärtpaberijärelevalve Organisatsiooni (IOSCO) tehnilise komitee finantsturutaristute põhimõtted, aprill 2012, avaldatud Rahvusvaheliste Arvelduste Panga veebilehel www.bis.org. Kohustus D näeb ette, et kõik CPSSi ja IOSCO liikmed peavad neid põhimõtteid kohaldama oma jurisdiktsioonis tegutsevate asjaomaste finantsturutaristute suhtes maksimaalses ulatuses, mis on nende jurisdiktsiooni õigusraamistikuga lubatud.
([13]) Määruse (EL) nr 795/2014 (EKP/2014/28) artikkel 15.
([14]) Eurosüsteemi järelevaatamispoliitika raamistik, läbivaadatud redaktsioon (juuli 2016), avaldatud EKP veebilehel www.ecb.europa.eu.
([15]) Kavandatava direktiivi artikkel 2 ning I ja II lisa.
([16]) Kavandatava direktiivi artikkel 3.

3. **Kolmandate isikutega seotud IKT-risk, ulatuslike intsidentide ja kriiside ohjamine, teabe jagamine ja riiklik küberturvalisuse strateegia**

3.1 *Kolmandate isikutega seotud IKT-riski juhtimine*

3.1.1 Kavandatava direktiiviga antakse pädevatele asutustele täitmise tagamise volituste rakendamisel õigus anda siduvaid juhiseid või korraldusi, millega nõutakse, et kõnealused üksused kõrvaldaksid tuvastatud puudused või heastaksid kavandatavas direktiivis sätestatud kohustuste rikkumised ([17]). Samal ajal võib DORA määruse alusel määratud „juhtiv järelevalveasutus“ anda kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele soovitusi võimalike süsteemsete riskide juhtimiseks, mis kaasnevad tegevuse edasiandmise ja kolmandast isikust IKT-teenuste osutajate kontsentratsiooniga ([18]).

3.1.2 Arvestades asjaolu, et kavandatavas direktiivis käsitletud elutähtsa üksuse võib määrata ka kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaks DORA määruse alusel, soovib EKP rõhutada ([19]), et vastuoluliste soovituste ja siduvate juhiste andmist tuleb vältida. EKP toetab selles osas nõukogu üldist lähenemisviisi kavandatava direktiivi suhtes. Selle lähenemisviisi kohaselt peavad pädevad asutused teavitama DORA määruse alusel loodud järelevalvefoorumit järelevalve- ja täitmise tagamise volituste kasutamisest seoses elutähtsa üksusega, mis on DORA määruse kohaselt määratletud kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja ([20]).

3.2 *Ulatuslike intsidentide ja kriiside ohjamine*

3.2.1 Kavandatava direktiivi kohaselt ([21]) peavad liikmesriigid määrama ühe või mitu pädevat asutust, kes vastutavad ulatuslike intsidentide ja kriiside ohjamise eest. Nagu kavandatava direktiivi põhjendustes on selgitatud, tuleks ulatusliku intsidendina mõista intsidenti, millel on märkimisväärne mõju vähemalt kahele liikmesriigile või mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa. Ulatuslikud intsidendid võivad muutuda täieulatuslikuks kriisiks, mis takistab siseturu nõuetekohast toimimist ([22]).

3.2.2 Kui DORA määruse kohaselt määratud pädevad asutused vastutavad finantssektori ettevõtjatega seotud küberturbe intsidentide haldamise eest, on koostöö kavandatava direktiivi kohaselt loodud struktuuride ja ametiasutustega äärmiselt oluline, et tagada koordineeritud reageerimisvõime kogu liidus. Seetõttu toetaks EKP DORA määruse kohaselt määratud pädevate asutuste, sealhulgas EKP, osalemist Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikus (EU-CyCLONe) ([23]) finantssektorit mõjutavate ulatuslike küberturbe intsidentide ja kriiside korral.

3.3 *Teabe jagamine*

3.3.1 Nagu eespool märgitud, toetab EKP kindlalt DORA määruse kohaselt määratud pädevate asutuste koostööd kavandatava direktiivi alusel loodavate struktuuride ja ametiasutustega. Eelkõige toetab ametiasutuste vaheline teabevahetus valdkondadeülese teadmuse omandamist, küberrünnakute ennetamist ja tõhusat ohjamist ning edendab IKTga seotud riskide järjepidevat hindamist kogu liidus. Siiski soovib EKP rõhutada, et teabevahetus peaks toimuma ainult juhul, kui on olemas selgelt määratletud klassifitseerimis- ja teabejagamise mehhanismid koos piisavate kaitsemeetmetega konfidentsiaalsuse tagamiseks ([24]). EKP toetab nõukogu üldist lähenemisviisi kavandatava direktiivi suhtes, milles tehakse ettepanek asjaomase teabe korrapäraseks vahetamiseks ametiasutuste

([17]) Vt kavandatava direktiivi artikli 29 lõike 4 punkt b.
([18]) DORA määruse artikkel 31.
([19]) Vt arvamuse CON/2021/20 punkt 1.2.
([20]) Kavandatavat direktiivi käsitleva nõukogu üldise lähenemisviisi artikli 29 lõige 10.
([21]) Kavandatava direktiivi artikli 7 lõige 1.
([22]) Kavandatava direktiivi põhjendus 27.
([23]) Kavandatava direktiivi artikkel 14.
([24]) Vt arvamuse CON/2021/20 punkt 1.5.

vahel ([25]), koostöökorra kehtestamiseks, et määrata kindlaks teabevahetuse mehhanism ([26]), ning automaatseks ja otseseks intsidentidest teatamiseks ([27]). Sellega seoses tuleks tagada, et DORA määruse ametisaladuse sätete ([28]) või asjakohaste valdkondlike õigusaktide ([29]) kohaselt konfidentsiaalsena käsitletavat teavet saab vahetada kavandatavas direktiivis osutatud pädevate asutustega ainult juhul, kui selline teabevahetus on vajalik selleks, et pädevad asutused kohaldaksid kavandatava direktiivi sätteid ([30]).

3.4 *Riiklik küberturvalisuse strateegia*

3.4.1 Kavandatava direktiivi kohaselt peavad liikmesriigid võtma vastu riiklikud küberturvalisuse strateegiad, milles määratakse kindlaks strateegilised eesmärgid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada ja säilitada kõrgel tasemel küberturvalisus ([31]). Nagu on selgitatud kavandatava direktiivi põhjendustes, peaksid liikmesriigid jätkuvalt hõlmama finantssektori oma küberturvalisuse strateegiatesse ([32]). Liikmesriigid peaksid oma riiklike küberturvalisuse strateegiate raames kujundama poliitikameetmed, mis käsitlevad küberturvalisust IKT-toodete ja IKT-teenuste tarneahelas, mida ettevõtjad kasutavad oma teenuste osutamiseks. Finantssektori puhul peaksid riiklikud küberturvalisuse strateegiad olema kooskõlas DORA määrusest tuleneva õigusraamistikuga. Sellega seoses leiab EKP, et on vaja täiendavalt selgitada, kuidas tagada riiklike küberturvalisuse strateegiate kooskõla valdkondlike õigusaktidega.

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

Frankfurt Maini ääres, 11. aprill 2022

EKP president
Christine LAGARDE

([25]) Kavandatavat direktiivi käsitleva nõukogu üldise lähenemisviisi artikli 11 lõige 5.
([26]) Kavandatavat direktiivi käsitleva nõukogu üldise lähenemisviisi põhjendus 23a.
([27]) Kavandatavat direktiivi käsitleva nõukogu üldise lähenemisviisi põhjendus 13.
([28]) DORA määruse artikkel 49.
([29]) Euroopa Parlamendi ja nõukogu direktiiv 2013/36/EL, 26. juuni 2013, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ (ELT L 176, 27.6.2013, lk 338), artiklid 53 kuni 62.
([30]) Kavandatava direktiivi artikli 2 lõige 5 ja artikli 11 lõige 4.
([31]) Kavandatava direktiivi artikkel 5.
([32]) Kavandatava direktiivi põhjendus 13.