RAHANDUSMINISTEERIUM

Kilvar Kessler
Finantsinspektsioon
info@fi.ee

Meie 05.10.2020 nr 1.1-10/6769-1

KONSULTATSIOONIDOKUMENT
finantsteenuste digitaalse operatsioonilise resilientsuse akti (DORA) kohta

24. septembril 2020 avaldas Euroopa Komisjon **digirahanduse** (ingl Digital Finance) **paketi**, mis sisaldab digirahanduse ja jaemaksete strateegiaid ning seadusandlike ettepanekuid krüptovarade (MiCA) ja finantsteenuste digitaalse operatsioonilise resilientsuse (DORA) kohta. Digirahanduse pakett on leitav järgmiselt lingilt: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

Käesolev konsultatsioonidokument puudutab viimati nimetatud seadusandlikku ettepanekut eesmärgiga koondada seotud osapoolte, sh ministeeriumide, pädevate asutuste, finantsjärelevalve ja turuosaliste esmased arvamused **DORA** (määruse eelnõu) ja sellega kaasneva direktiivi eelnõu kohta.

Nimetatud õigusaktide eelnõude peamiseks eesmärgiks on ennetada ja maandada finantssektoris esinevaid digitaalseid riske, sh küberriske. Euroopa Komisjoni hinnangul tähendab finantssektori järjest suurem sõltuvus tarkvarast ja digitaalsetest protsessidest ka info- ja kommunikatsioonitehnoloogiaga (IKT) seotud riskide tõusu. Seetõttu teeb komisjon suurele hulgale ettevõtjatele ettepaneku tagada, et nad suudaksid vastu pidada igat tüüpi IKT-ga seotud häiretele ja ohtudele. Pangad, börsid, arvelduskojad ja ka finantstehnoloogia ettevõtjad peavad IKT-ga seotud juhtumite ennetamiseks ja riskide maandamiseks järgima seega rangeid standardeid. Samuti kehtestab komisjon järelevalveraamistiku teenusepakkujatele (näiteks kõrgtehnoloogia ettevõtjad ehk *Big Techs*), kes pakuvad finantsasutustele pilvandmetöötlust või mõnda muud olulist teenust.

DORA määruse ettepanekuga seotud dokumentide lingid:

- **DORA määruse ettepanek**;
- Esialgne mõjuhinnang DORA määruse juurde;
- Lühikokkuvõte kaasnevatest mõjudest;
- **DORA ja MiCA ettepanekutega kaasnev direktiiv**;
- Mõjuhinnang eelviidatud direktiivi juurde;
- Mõjude lühikokkuvõte.

Selleks, et saaksime Eesti poolt aktiivselt mõjutada eeltoodud ettepanekute menetlemist EL tasandil, palub Rahandusministeerium huvirühmade arvamusi DORA-ga seotud õigusaktide kohta. Teiepoolse sisendi koostamise toetamiseks oleme omalt poolt käesoleva kirja lisades

esitanud mõned küsimused üldise seisukoha kujundamiseks ja võimalike mõjude hindamiseks. Küsimused on jagatud vastavalt DORA määruse eelnõu ja direktiivi eelnõu ettepaneku struktuurile teemablokkidesse.

Palume Teie tagasisidet hiljemalt 16. oktoobriks 2020.

Lugupidamisega

/allkirjastatud digitaalselt/

Märten Ross
finantspoliitika ja välissuhete asekantsler

Lisa 1: Küsimused DORA määruse kohta
Lisa 2: Küsimused DORA ja MiCA määrustega kaasneva direktiivi, millega muudetakse järgmiseid õigusakte: 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, kohta

Paula Etti 6113502, paula.etti@fin.ee
Kristiina Kubja 6113658, kristiina.kubja@fin.ee

Sama:
Majandus- ja Kommunikatsiooniministeerium
Siseministeerium
Justiitsministeerium
Eesti Pangaliit MTÜ
FinanceEstonia MTÜ
Riigi Infosüsteemi Amet
Audiitorkogu
Eesti Kindlustusseltside Liit
Eesti Kindlustusmaaklerite Liit
Admiral Markets AS
Aktsiaselts Cresco Väärtpaberid
Aktsiaselts KIT Finance Europe
Aktsiaselts KAWE KAPITAL
AS Redgate Capital
Nasdaq Tallinn AS
Eesti Infotehnoloogia ja Telekommunikatsiooni Liit
Eesti Advokatuur
Eesti Pank
Eesti Krüptoraha Liit

LISA 1. DORA määruse eelnõu

Määruse eelnõu (edaspidi määruse) eesmärk
Määrus kehtestab sektori-spetsiifilised ühetaolised nõuded IKT süsteemide turvalisusele, toetades seeläbi finantssektoris tegutsevate ettevõtjate majandustegevust ja tagades kõrgtasemelise digitaalse operatsioonilise resilientsuse. Määrus katab järgmisi valdkondi: • IKT riskijuhtimine; • suurtest IKT intsidentidest raporteerimine pädevale asutusele; • digitaalse operatsioonilise resilientsuse testimine; • küberohtudega ja haavatavustega seotud infojagamine; • kolmandatest osapooltest IKT teenuseosutajatega seotud riskide juhtimise ja maandamise meetmed; • finantsteenuse osutaja ja kolmandast osapoolest IKT teenuseosutaja vahelistele lepingutele kohalduvad printsiibid; • kolmandatest osapooltest IKT teenuseosutajate järelevaatamise raamistik; • pädevate asutuste koostöö ja järelevalve ning –vaatamise reeglid.
1. Milline on teie üldhinnang määruse eesmärkidele?
Vastus:
2. Muud tähelepanekud.
Vastus:
Määruse kohaldamisala ja proportsionaalsus
Määruse kohaldamisalasse (artikkel 2) kuulub 20 erinevat teenuseosutajat, kellest enamik on **finantsteenuse osutajad** (sh krediidiasutused, kindlustusandjad, -vahendajad, investeerimisühingud, fondivalitsejad, ühisrahastusteenuse osutajad jt), lisaks **audiitorid** ja **kolmandatest osapooltest IKT teenuseostajad (***edaspidi* **teenuseosutajad)**. Proportsionaalsuse põhimõtted võib jagada kolmeks: • regulatiivsed leevendused, mis on ette nähtud väikestele teenuseosutajatele; • eeskirjad, mis kohalduvad ainult olulistele teenuseosutajatele; • nõuded, mis on seotud teatud tegevuste olulisusega.
3. Kas määrus peaks kohalduma kõikidele ettepanekus määratletud teenuseosutajatele ?
Vastus:
4. Kas teie hinnangul ettepanekus esitatud proportsionaalsuse põhimõtted võtavad õiglaselt arvesse teenuseosutaja laadi, organisatsiooni struktuuri ja juhtimist, tegevuse mahtu jne? Kui ei, milliste teenuseosutajate või milliste tegevuste suhtes tuleks ette näha täiendavad leevendused või välistused?
Vastus:
5. Kas erisused määruse kohaldumisalas, nt maksesüsteemide välistamine, on teie hinnangul põhjendatud?
Vastus:
6. Üldine seisukoht ja muud tähelepanekud määruse kohaldamisala kohta.
Vastus:
IKT riskide juhtimine (art 4-14)

7. (**Ainult turuosalistele**) Kuidas on IKT riskide juhtimine korraldatud teie organisatsioonis täna ja kui palju ümberkorraldusi te peaksite tegema käesoleva ettepaneku valguses, sh seoses täiendava personali kaasamise ja investeeringutega IT lahendustesse?
Vastus:
8. Üldine seisukoht ja muud tähelepanekud IKT riskide juhtimise kohta.
Vastus:
IKT-ga seotud intsidentidest raporteerimine (art 15-20)
Ettepaneku kohaselt peab teenuseosutajal olema juhtimisprotsess IKT-ga seotud intsidentide monitoorimiseks ja säilitamiseks, misjärel tuleb need klassifitseerida ja olulisematest pädevat asutust teavitada.
9. Kas teie hinnangul on selline EL tasandil harmoniseeritud teavitamismudel asjakohane ning seda peaks kohaldama kõikide teenuseosutajate suhtes. Kui mitte, siis miks ja millised on teie ettepanekud eeskirjade parandamiseks?
Vastus:
10. Üldine seisukoht ja muud tähelepanekud IKT-ga seotud intsidentidest teavitamise kohta.
Vastus:
Digitaalse operatsioonilise resilientsuse testimine (art 21-24)
11. Kas DORA IV peatükis sätestatud testimisraamistik on arusaadav? Kui ei, mida tuleks täpsustada või muuta? Kas Eesti peaks implementeerima ka Tiber-EU[1] testimisraamistiku?
Vastus:
12. Üldine seisukoht artiklites 21-24 sätestatu kohta.
Vastus:
Kolmandatest osapooltest IKT teenuseosutajatega seonduvad riskid (art 25-39)
13. (Ainult turuosalistele) Kas te ostate sisse IKT teenuseid? Kas ettepanekus esitatud lahendused pigem lihtustavad kolmandate osapooltega suhtlemist/läbirääkimisi/lepingu sõlmimist või muudavad selle pigem keerulisemaks?
Vastus:
14. Mida te arvate sellest, et ettepaneku kohaselt teostatakse kriitilise tähtsusega kolmandate osapoolte üle järelevalvet EL tasandil?
Vastus:
Küberohtude ja haavatavustega seotud informatsiooni jagamine (art 40)
15. Millist lisaväärtust te näete selles, et artikli 40 kohaselt võiksid finantsteenuse osutajad omavahel küberohtude ja haavatavuste kohta (vabatahtlikult) teavet jagada?
Vastus:
16. Kas te näete sellises teavitamises ka ohte või üldisi takistusi?

[1] Vt täpsemalt: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html. Tiber-EU testimisraamistiku on implementeeriunud oma õigusesse juba Belgia, Saksamaa, Soome, Taani, Iirimaa, Itaalia, Norra, Rumeenia, Rootsi ja Holland.

Vastus:
17. Üldine seisukoht ja muud tähelepanekud teavitamise kohta.
Vastus:
Pädev asutus (artiklid 41-49)
18. Üldine seisukoht artiklites 41-49 sätestatu kohta.
Vastus:
Delegeeritud aktid, ülevaatusklausel, muudatused muudes õigusaktides ja jõustumisaeg (artiklid 50-56)
19. Üldine seisukoht artiklites 56-59 sätestatu kohta?
Vastus:
20. Kas artiklis 56 sätestatud üldine jõustumise tähtaeg 12 kuud on piisav muudatuste tegemiseks ja organisatsiooni vastavusse viimiseks kehtestatud nõuetega?
Vastus:
Muud teemad, mida eelnevalt ei käsitletud
21. Palume tagasisidet ja ettepanekuid teemade osas, mis eelnevalt kajastamist ei leidnud, kui teie hinnangul on neid nüansse oluline adresseerida.
Vastus:

LISA 2. DORA ja MiCA määrustega kaasnev direktiivi eelnõu, millega muudetakse järgmiseid õigusakte: 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341

Direktiivi eelnõu (edaspidi eelnõu) eesmärk
Direktiivi eesmärk on viia olemasolevad Euroopa Liidu õigusaktid kooskõlla DORA ja MiCA nõuetega.
1. Üldine seisukoht eelviidatud direktiiviga kavandatavate muudatuste kohta ja võimalikud muud tähelepanekud.
Vastus: