Eesti Pangaliit

Rahandusministeerium
info@fin.ee

Koopia:
Kristiina.Kubja@fin.ee
Raavo.Palu@mkm.ee

Teie: 09.11.2023 nr 13-1.1/6798-1

Meie: 7.12.2023 nr 58

Pangaliidu kommentaarid finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse eelnõule

Austatud Mart Võrklaev

Käesolevaga esitame Pangaliidu kommentaarid finantskriisi ennetamise ja lahendamise seaduse ning teiste seaduste muutmise seaduse eelnõu (edaspidi Eelnõu) osas.

1. **Ettepanekud seoses CER direktiiviga**

   Eelnõu seletuskirjas on korrektselt viidatud, et lisaks NIS2 direktiivile mõjutab DORA ka CER direktiivi kehtivusala (vt SK p 2.5., lk 14-16). Samas ei ole aga eelnõus rakendussätteid, mis toetaks eelnimetatu rakendamist krediidiasutuste suhtes õigusaktide tasandil.

   Alltoodud ettepanekud põhinevad kättesaadaval informatsioonil, et nii hädaolukorra seaduse muudatused kui ka uue tsiviilkriisi ja riigikaitse seaduse eelnõu sätted ei näe krediidiasutustele ette erisusi võrreldes teiste elutähtsate teenuste osutajatega (ETO). Samuti, et Eesti Pank jätkab finantsteenuste osas elutähtsa teenuse korraldava asutuse (ETKA) rolli.

2. **Koostöö elutähtsate teenuste toimivuse valdkonnas**

   Teeme ettepaneku lisada Finantsinspektsiooni seadusesse koostöö kohta Eesti Panga ja Riigikantseleiga analoogne lisandus nagu Eelnõus pakutud § 47.11. Nimelt kehtiv ja meie andmetel ka jätkuv lahendus on, et finantsteenuste osas on ETKA-ks Eesti Pank ning üldiseks kriisideks valmistumise korraldajaks Riigikantselei, järelevalve teostajaks pankade üle aga Finantsinspektsioon. Koostöö nimetatud asutuste vahel, eelkõige aga ka info vahetamine, on sellise lahenduse efektiivse toimimise võtmeküsimus. Senine praktika on siinkohal näidanud vajakajäämisi, mis mh on krediidiasutustele kaasa toonud täiendava halduskoormuse sama teabe topelt esitamise kohustuse tõttu. Kindlasti võivad sellised vajakajäämised mõjutada ka üldist kriisijuhtimise kvaliteeti riigi tasandil.

3. **Krediidiasutuste seaduse nõuded operatsiooniriski juhtimisele**

   Teeme ettepaneku lisada krediidiasutuste seadusesse analoogne lisandus nagu Eelnõus pakutud § 82.4 lg 3, kuid seda seoses hädaolukorra seaduse / tsiviilkriisi ja riigikaitse seaduse teatud sätete mitterakendamisega ETO-pankadele.

Maakri 30, Tallinn 10145
T +372 611 6567
pangaliit@pangaliit.ee
pangaliit.ee

Ettepaneku ajendiks on CER põhjenduspunkt 21 ja artikkel 8 ning DORA preambula punktid 19, 22 ja 23 ning artikkel 1 p 2. Oleme esitanud analoogse ettepaneku ka Riigikantseleile, kelle vastutusalas on hädaolukorra seaduse / tsiviilkriisi ja riigikaitse seaduse kujundamine selliselt, et see vastaks CER direktiivi nõuetele.

Nõustume, et seoses kriisideks ettevalmistamise vajadusega on vajalik krediidiasutuste kaasamine ettevalmistustegevustesse. Kuid nagu ka CER-s ja DORA-s sätestatud, tuleks seda teha ebavajalikku halduskoormust vältides. Oleme valmis täiendavalt kaasa mõtlema, kuidas seda saavutada kõige efektiivsemal moel.

1. **Ettepanek VV määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (VVm) muutmiseks**

Täna kohaldub VVm nr 121 ka finantssektori ettevõtjatele. DORA ja VVm nr 121 koosmõjul kohalduks Eestis tegutsevatele finantssektori ettevõtjatele küberturvalisuse valdkonnas kaks vastavuskohustust ning kaks järelevalvet teostavat asutust.

Palun viia VVm kooskõlla Eelnõuga, määruse (EL) 2022/2554 ning direktiiviga (EL) 2022/2555) välistamaks finantssektorile kaasnevad riskid, tarbetu kordus ja täiendav halduskoormus.

Üheks võimalikuks lahenduseks võib olla VVm nr 121 täiendamine §-i 3 lõikega 4 järgmises sõnastuses:
„(4) määruse (EL) 2022/2554) kohaldamisalasse kuuluvatele ettevõtjatele ei kohaldata lõike 1 ja lõike 2 alusel kehtestatud nõudeid.“

1.1. Finantssektori ettevõtjatele kohalduvad eriseadusest tulenevad küberturvalisuse nõuded

VVm nr 121 näeb ette, et teenuse osutaja tõendab oma süsteemi turvameetmete vastavust järelevalveasutusele rakendades E-ITS-i või alternatiivselt ISO/IEC 27001 standardile vastavaid turvameetmeid ning esitab seejuures ka kehtiva ISO/IEC 27001 vastavussertifikaadi. VVm nr 121 on kehtestatud küberturvalisuse seaduse (KüTS) alusel, mis omakorda kehtestab NIS ja NIS2-s nõutud turvameetmete rakendamise ja küberintsidentidest teavitamise nõuded olulise teenuse ja digitaalse teenuse osutajatele.

Määrus (EL) 2022/2554 (DORA) on finantssektori ettevõtjatele kohalduv eriseadus, mis kehtestab spetsiifilised küberturvalisuse nõuded. Direktiivi (EL) 2022/2555 (NIS2) ei kohaldata finantssektori ettevõtjate suhtes ulatuses, mida reguleerib DORA.

NIS2 põhjenduspunkti 28 kohaselt tuleb DORA-t käsitada finantssektori ettevõtjate suhtes valdkondliku liidu õigusaktina. NIS2 artikli 4 kohaselt ei tuleks kohaldada finantssektori ettevõtjate suhtes NIS2-st tulenevaid sätteid (sh nt järelevalve- ja täitmise tagamise sätteid), kuna need nähakse ette valdkondlikes õigusaktides.

DORA põhjenduspunkti 16 kohaselt kehtestatakse DORA-ga finantssektori ettevõtjate suhtes rangemad nõuded võrreldes NIS2-ga. Seega tuleb DORA-t käsitleda finantssektori ettevõtjate suhtes valdkondliku liidu õigusaktina ning mitte kohaldada finantssektori ettevõtjate suhtes NIS2-e.

Eelnõu peatükk 2.5 möönab, et liikmesriigid ei tohiks kohaldada NIS2 direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist DORA määruse kohaldamisalasse jäävate finantssektori ettevõtjate suhtes. Eelnõu märgib, et Finantsinspektsioon (FI) ja Euroopa Keskpank (EKP) on pädevateks asutusteks teostamaks krediidiasutuse ja finantsturutaristu järelevalvet. Tõsistest IKT-intsidentidest teavitatakse ka RIA-t. Koostöösätetega tagatakse, et FI teeb RIA-ga koostööd, mh seoses finantsasutuste ohuteabel põhinevate läbistustestimistega.

Eesti naaberriigid (Läti, Leedu, Soome ja Rootsi) käsitlevad DORA't finantssektori ettevõtjate suhtes kehtiva valdkondliku liidu õigusaktina. Naaberriigid ei näe ette finantssektori ettevõtjatele kohustust vastata, lisaks DORA-le siseriiklikule või rahvusvahelisele infoturbestandardile, kuna DORA sätestab rangemad ja ühtsed valdkondlikud reeglid. Ühtlasi ei ole naaberriikides audiitorid ega sertifitseerimisasutused pädevad kontrollima finantssektori ettevõtjate vastavust DORA nõuetele vaid on üheselt täheldanud, et selliste ettevõtjate üle teostab järelevalvet DORA's sätestatud pädev asutus.

1.2. Täiendus välistab kaasuvad riskid, tarbetu korduse ja halduskoormuse

DORA kohaldamisalasse jäävate finantssektori ettevõtjate suhtes teostab järelevalvet vaid artikli 31 alusel määratud järelevalveasutus vastavalt kehtestatud korrale. Eestis on selliseks pädevaks asutuseks FI ja oluliste krediidiasutuste osas EKP. Seevastu E-ITS-i ja ISO/IEC 27001 kohaselt teostaks järelevalvet RIA ja audiitor vastavalt E-ITS-is või ISO/IEC kohaselt kehtestatud nõuetele. Siseriikliku või rahvusvahelise infoturbestandardi audiitor või sertifitseerimisasutus ei ole pädev teostama järelevalvet finantssektori ettevõtjate üle küberturvalisuse valdkonnas.

Kohaldades E-ITS-i või alternatiivselt ISO/IEC 27001 nõudeid DORA kohaldamisalasse jäävate finantssektori ettevõtjate suhtes, on finantssektori ettevõtjad kohustatud üheaegselt ning ühest ja samast küberturvalisuse aspektist lähtuvalt:

1.3. täitma valdkondliku liidu õigusakti DORA ja samaaegselt ka E-ITS-i või ISO/IEC 27001 nõudeid;
1.4. osalema nii valdkondliku liidu õigusakti DORA alusel kui ka E-ITS-i või ISO/IEC 27001 standardi alusel teostatavatel audititel;
1.5. esitama auditite järeldusotsuseid nii valdkondliku liidu õigusakti DORA alusel määratud juhtivale järelevalveüksusele kui ka RIA-le.

Täiendavate nõuete ja järelevalve kohaldamine ei taga tõhusamat nõuete täitmist, järelevalvet ega vastutuse jaotust. See võib kaasa tuua täiendavad riskid digitaalse tegevuskerksuse ja küberturvalisuse tagamisel finantssektoris. Dubleerivad nõuded pole kooskõlas hea halduse põhimõttega. Teised Euroopa Liidu liikmesriigid ei näe finantssektori ettevõtjatele ette sarnaseid dubleerivaid nõudeid.

Pangaliit on valmis andma täiendavaid selgitusi esitatud ettepanekutele.

Lugupidamisega,

/allkirjastatud digitaalselt/

Katrin Talihärm
Juhatuse liige