MAJANDUS- JA
KOMMUNIKATSIOONI-
MINISTEERIUM

Rahandusministeerium
info@rahandusministeerium.ee

Teie 09.11.2023 nr 13-1.1/6798-1,
RAM/23-1460/-1K

Meie 29.12.2023 nr 2-7/2023/4744

Eelnõu kooskõlastamine märkustega

Austatud rahandusminister

Täname võimaluse eest esitada tagasisidet finantskriisi ennetamise ja lahendamise seaduse ning teise seaduste muutmise seaduse eelnõule (edaspidi eelnõu). Kooskõlastame eelnõu järgnevate märkustega arvestamisel.

1. Kübervaldkonnas järelevalve korraldus

Eelnõu kohaselt määratakse Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 ehk DORA määruse artikkel 46 mõttes pädevaks asutuseks Finantsinspektsioon (FI), millest tulenevalt hakkab finantssektori küberturvalisuse nõuete üle järelevalvet teostama samuti FI. Leiame, et eelnõu seletuskirjas ei ole ammendavalt põhjendatud, miks ei oleks võimalik järelevalve pädevust DORA määrusest tulenevate IKT riskijuhtimise nõuete täitmise üle anda Riigi Infosüsteemi Ametile (RIA) ning näeme valitud lahenduses mitmeid olulisi puuduseid.

Seetõttu esitame **ettepaneku** kaaluda täiendavalt DORA määruses ettenähtud IKT-riski juhtimise meetmete alase järelevalve pädevuse andmist RIAle ja sellest tulenevalt:

1) sätestada küberturvalisuse seaduses (edaspidi: KüTS), et DORA määruses kehtestatud IKT-riski juhtimise nõuete üle teostab järelevalvet RIA;
2) muuta eelnõu § 2 punkti 1, millega muudetakse finantsinspektsiooni seadust (edaspidi: FIS) ja millega täiendatakse paragrahvi 6 lõiget 1 punktiga 7^5 ja §-i 4, millega lisatakse §-ga 47^{11} vastavalt ettepanekule, et DORA määruses kehtestatud IKT-riski juhtimise nõuete täitmise järelevalve jääb RIAle;
3) sätestada investeerimisfondide seaduses, kindlustustegevuse seaduses, krediidiasutuste seaduses (KAS), makseasutuste ja e-raha asutuste seaduses ning väärtpaberite registri pidamise seaduses (EVKS), et RIAl on õigus teostada järelevalvet DORA määruses sätestatu täitmise üle, sealhulgas teha DORA määruse artiklis 50 sätestatud järelevalvetoiminguid ning rakendada karistusi ja muid meetmeid (ehk muuta eelnõus ettenähtud sarnase sõnastusega sätteid, mis annavad vastava pädevuse FIle);
4) muuta teisi asjasse puutuvaid eelnõu sätteid.

Seletuskirjas on välja toodud, et selleks, et anda DORA pädeva asutuse roll osaliselt RIA-le, tuleb RIA määratleda (kaas)pädeva asutusena ka kõikide DORA määruse artiklis 46 loetletud finantssektori Euroopa Liidu direktiivide ja määruste tähenduses ning selline lähenemine tooks mh kaasa nt osamaksete tasumise kohustuse. Sellega kogu põhjendus piirdub ning ei ole välja toodud, millised olid need arutluskäigud, millega taoline variant pädevuse jagamiseks kõrvale jäeti, millised on need „rida kohustusi“ ja kas need ka konkreetselt DORA määrusest tuleneva pädevuse degeleerimisel kindlasti RIAle kohalduksid. RIA on väljendanud varasemaltki soovi jääda riigis küberpädevust omavaks

asutuseks ning teinud ettepaneku pädevuse jagamiseks. Puudub põhjendus, mis välistab osaliselt järelevalve pädevuse edasi delegeerimist.

Muudatus eeldab küberturbe kompetentsi tagamist FIs. Siinkohal tuleb arvesse võtta, et vastava kompetentsiga isikute hulk Eesti töörutul on piiratud. Küberturbe järelevalve võimekuse loomine mitmesse asutusse tähendab täiendavat konkurentsi tööjõu suhtes erasektori kõrval.

Eestis on seni küberturbe tagamisel lähtutud tsentraliseeritud mudelist, vastava suuna on heaks kiitnud ka Vabariigi Valitsuse Julgeolekukomisjoni Küberjulgeoleku Nõukogu. Kuigi mitmetes Euroopa Liidu riikides on küberturbe tagamine ja järelevalve jaotatud sektoriaalsete asutuste vahel, ei ole see Eesti väiksust ja ressursi piiratust arvestades asjakohane. Samuti ei ole selline tegevus kooskõlas null-eelarve põhimõtetega, mille raames otsitakse võimalusi ülesannete dubleerimise vältimiseks avalikus sektoris.

Laiahaardelise ja efektiivse küberturvalisuse tagamiseks on oluline, et RIAl oleks terviklik pilt kõikidest küberturbe riskidest üle sektorite. Arvestades finantsasutuste vastu suunatud intsidentide rohkust ning mõju, on tegemist eriti olulise sektoriga riigi üldise küberturvalisuse tagamisel. Eelnõuga ettenähtud koostöö RIAga ning finantsasutuste teavitamine olulistest küberintsidentidest ei taga piisavat ülevaadet, et efektiivselt läbi viia nii ennetus- ja analüüsitegevusi kui operatiivselt toetada intsidentide lahendamist.

Lisaks tuleb arvestada, et DORA määrus sätestab erinormid vaid teatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ehk NIS2 direktiiviga üle võetavate kohustuste osas ning samuti rakenduksid vähemalt osadele finantsasutustele ka Eesti-spetsiifilised nõuded (vt siinse kooskõlastuse punkte 3 ja 9). Nende nõuete osas jääks järelevalvepädevus siiski RIAle. Seega oleks otstarbekas jätta pädevus ühte asutusse, kes saab kõikehõlmavalt teha järelevalvet nii DORA määruse nõuete kui ka sealt väljajäävate, kuid muudes õigusaktides (peamiselt KüTSis) sätestatud nõuete täitmise üle.

Oleme koos RIAga valmis siinset ettepanekut täiendavalt arutama ning mainime, et järgnevad ettepanekud on tehtud sõltumata siinse ettepaneku sisust.

2. DORA määruse valikukoht nr 3

Seletuskirja lk 11 (DORA määruse valikukoht nr 3 selgitus, viimane tekstilõik) on märgitud:

Eelnõu väljatöötamisel oli kaalumisel ka variant, et kui hoiu-laenuühistud jätta DORA määruse kohaldamisalast välja, siis alternatiivina oleks võimalik neile ka KüTS küberturvalisuse nõudeid kohaldada ja RIA oleks sellisel juhul pädevaks asutuseks. Kuna hoiu-laenuühistute seaduseelnõu menetlus on hetkel veel pooleli, siis hetkel on võetud lähenemine, et sõltuvalt menetluse seisust ja tulemusest seoses viidatud eelnõuga, tehakse otsused ka selles osas, mis puudutab hoiu-laenuühistutele küberturvalisuse nõuete kohaldamist.

Siin juhime tähelepanu NIS2 direktiivi artikli 2 lõikele 10, mis sätestab:

Käesolevat direktiivi ei kohaldata üksuste suhtes, mille liikmesriigid on kooskõlas määruse (EL) 2022/2554 artikli 2 lõikega 4 kõnealuse määruse kohaldamisalast välja jätnud.

Sisuliselt on NIS2 direktiivi kohaldamisalast välistatud Eesti puhul hoiu-laenuühistud. Seetõttu soovitame üle hinnata, kas DORA määruse valikukoht nr 3 tulemus jääb samaks või mitte. Kui valikukoht muutub, siis tuleb ka seletuskirja muud osad üle vaadata (nt seletuskirja lk 13 olev tabel ja eelnõu § 3 sisu ning selgitus).

3. NIS2 direktiivi järgimine

Seletuskirja lk 15 on tabel, mille üks tulp on ka NIS2 direktiivi kohta. Tabelis on krediidiasutuste ja finantsturutaristute real märgitud NIS2 direktiivi artikli 4 lõigete 1 ja 2 sisu ehk loetelu teemadest, mida need isikud ei pea NIS2 direktiivi puhul järgima.

Samas ei ole seal välja toodud, millised võivad olla NIS2 direktiivi sätted, mida peaksid need ettevõtjad NIS2 direktiivi artiklite 2 ja 3, koosmõjus NIS2 direktiivi artikli 4 lõigete 1 ning 2, tõttu järgima.

Esmasel analüüsil tundub, et nendeks säteteks võivad olla NIS2 direktiivi artikkel 9, artikkel 14 lõige 3, artikkel 16, artikli 24 lõige 1, artikkel 29 ja artikkel 30. Kaudselt on kohaldamisala mõttes siin seotud ka NIS2 direktiivi artiklid 7, 9, 10 ja 16. Lisaks on liikmesriikidel võimalik (mitte kohustus) kohaldada nende isikute suhtes ka NIS2 direktiivi artikli 3 lõike 3 tõttu ka artiklit 27.

Siin soovitame tutvuda ka Euroopa Komisjoni 18.9.2023 teatisega „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta 2023/C 328/02“, mis on leitav siit: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52023XC0918(01).

Eeltoodu tõttu palume seletuskirja täiendada eelmainitud sätetega.

4. RIA teavitamine tõsisest info- ja kommunikatsioonitehnoloogiaga seotud intsidendist ning olulisest küberohust

Eelnõu tekitab mitmes seaduses kohustuse teavitada tõsisest info- ja kommunikatsioonitehnoloogiaga seotud intsidendist ning olulisest küberohust muu hulgas ka RIAt. Nendeks muudatusteks on eelnõu § 4 punkt 7, eelnõu § 5 punktid 6, 8 ja 9, eelnõu § 7 punkt 5, eelnõu § 8 punkt 16, eelnõu § 9 punkt 3, eelnõu § 10 punktid 11, 13, 19 ning 20.

Enamus isikutest, kes neid kohustusi eelnõu tulemusena peavad hakkama täitma, pole varasemalt pidanud RIA-le neid teavitusi kohustuslikus korras tegema. Sellest hoolimata toetame nende muudatuste tegemist (isegi juhul, kui siinse kirja punktis 1 olevat ettepanekut ei täideta), kuna samad või sarnased küberintsidendid ja -ohud võivad aset leida või ilmneda ka muudes valdkondades ning RIA saab sel juhul aegsasti tegeleda nende ennetamise ja lahendamisega.

5. Planeeritava finantskriisi ennetamise ja lahendamise seaduse (edaspidi: FELS) § 29 lg 1 punkti 8 osas **soovitame** hinnata, kas eelnõuga planeeritava FELS § 29 lg 1 punkti 8 muudatuses peaks DORA määruse asemel olema viide KüTSile. Seda ennekõike seetõttu, et NIS2 direktiiviga ei muutu „võrgu- ja infosüsteemi“ mõiste ning hetkel on selle mõiste sisu üle võetud KüTS § 2 punktis 1.

6. Planeeritav FIS § 47^{11}

FIS § 47^{11} lg 1 punkti 2 kohaselt hõlmab FI ja RIA vaheline koostöö muu hulgas RIA-lt tehnilise nõu ja abi küsimine ning FI-le selle andmine […].

Me pole üldiselt vastu selles punktis raamistatud koostööle, kuid tekib küsitavus, kas FI kohta käivas seaduses on võimalik tekitada RIA-le kohustusi (vt allajoonitud osa) kui FIS ei reguleeri RIA ülesandeid ja toimimist.

7. Planeeritav FIS § 54 lg 4 punkt 12

Toetame FIS § 54 lõike 4 täiendamist punktiga 12 ning selgitame, et NIS2 direktiivi üle võtvasse eelnõusse kavandatakse koostöösäte DORA määruse pädevate asutustega.

Täiendavalt soovitame hinnata, kas FIS § 54 lõiget 4 tuleks täiendada ka kontrollimisandmete edastamisega Andmekaitse Inspektsioonile.

8. Ebatäpsused FIS §-ga 54^2

Juhime tähelepanu, et eelnõu § 2 punktiga 6 täiendatakse FIS § 54^2 lõikega 4, kuid seletuskirjas ei ole selle lõike kohta selgitusi esitatud. Samuti on seletuskirjas (lk 20) toodud selgitus FIS § 54^4 täiendamise kohta lõikega 4^1, kuid eelnõus sellist lõiget pole.

9. KüTS-i nõuete kohaldumine krediidiasutustele

Eelnõu § 7 punktiga 4 lisandub KASi § 82^4, mille lõike 3 kavandatava sõnastuse kohaselt ei kohaldata krediidiasutustele KüTS-i 2. peatükis sätestatud küberturvalisuse tagamise nõudeid. Eelnõus on ka märkus, et õige viide selgub kooskõlas NIS2 direktiivi üle võtmisega, millised KüTS-i sätted pankadele ei kohaldu.

Nõustume põhjendusega selles osas, et DORA määrus toimib NIS2 direktiivi suhtes *lex specialis'*ena ja sealsed nõuded katavad ära NIS2 direktiivis esitatavad nõuded küberturvalisuse riskijuhtimisele ja küberintsidentidest teavitamisele. Samas näiteks sisaldab KüTS-i alusel kinnitatud Eesti infoturbestandard ehk E-ITS tingimusi ja nõudeid, mis on Eesti spetsiifilised ning mida ei kata ei NIS2 direktiiv ega DORA määrus – näiteks eID ja X-tee. Seetõttu peaks tulevikus olema olukord, kus finantsvaldkonna ettevõtjad üldiselt peavad järgima vaid DORA määruse nõudeid, kuid kui mingis osas DORA määrus (sh selle alusel kehtestatud rakendusaktid) KüTS-i alusel kehtestatud Eesti spetsiifilisi nõudeid ära ei kata, siis tuleb täita ka neid.

Nõustume sellega, et NIS2 direktiivi üle võtvas eelnõus saab täpsustada, millised KüTS-i 2. peatüki sätted kohalduvad või ei kohaldu. Selle käigus selgub ka, millised NIS2 sätted kohalduvad ka DORA määruse subjektidele – vt siin eespool olevat märkust nr 3. NIS2 direktiivi üle võtvas eelnõus saab ka määratleda, millal KüTS-is sätestatud erisused hakkavad kehtima (vt siin ka eelnõu seletuskirja lk 30 alguses olevat selgitust).

Siinse muudatusega seonduvalt on Pangaliit enda 07.12.2023 tagasisides eelnõule esitanud ka ettepaneku Vabariigi Valitsuse 9.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 3 täiendamisega lõikega 4, mis välistaks E-ITSi ja selle vabatahtliku alternatiivi (rahvusvahelise standardi ISO/IEC 27001) kohaldumise ettevõtjatele, kes on DORA määruse kohaldamisalas. Leiame, et see ettepanek on asjakohane, kuid kavandatava KAS § 82^4 lõike 3 sõnastusest sõltub, kas on vaja teha Pangaliidu ettepanekus tehtud muudatust eelnimetaud Vabariigi Valitsuse määruses. Seda ennekõike seetõttu, et kui KAS § 82^4 lõike 3 tõttu välistatakse muuhulgas DORA määruse subjektide puhul KüTS § 7 lõige 5, siis sellise välistuse korral puudub vajadus teha Vabariigi Valitsuse määrusesse KAS-i tehtud nõuet kordav õigusnorm.

10. Eelnõu § 7 punkti 10 puhul pole otseselt selge eelnõust ega seletuskirjas, millisesse KAS-i peatükki soovitakse taaskehtestada eelnõu § 7 punktiga 9 kehtetuks tunnistatavate paragrahvide sisu. Eelduslikult on tegemist 12. peatükiga.

11. Info- ja kommunikatsioonitehnoloogia süsteem

Eelnõu § 8 punkti 13 ning eelnõu § 10 punkti 7 osas soovitame hinnata, kas siin on võimalik sõnade „info- ja kommunikatsioonitehnoloogia süsteem“ asemel kasutada KüTS § 2 punktis 1 olevat terminit „võrgu- ja infosüsteem“. Eelnõu § 8 punktis 13 soovitakse neid sõnu kasutada sõna „infosüsteem“ asemel.

Palume ka üle vaadata seletuskirja terminoloogia osa (lk 45), kuna seal on viidatud „võrgu- ja infosüsteemi“ mõiste puhul ainult NIS2 direktiivis sätestatud mõistele. Siin vt ka eespool olevat märkust nr 5.

12. Eelnõu § 9 punktis 1 ehk EVKS § 7^1 lõike 5 esimese lause muudatuses on RIA nimetus nurksulgudes.

13. Pensioniregister

EVKS reguleerib penisoniregistri pidamist ning eelnõu seletuskirja lk 37 (lõpus) kohaselt kohaldub registripidajale „DORA määruse turvastandard“. Eelnõu seletuskirjas on EVKS § 30^2 lõike 2

selgitustes mainitud, miks registripidajale ei kohaldu KüTS-i 2. peatükk.

EVKS § 1^3 lõike 1 kohaselt on pensioniregister riigi infosüsteemi kuuluv andmekogu kogumispensionide seaduses sätestatud kohustuslike ja vabatahtlike pensionifondide osakute ning nendega tehtavate toimingute registreerimiseks. Seetõttu on pensioniregister praegu KüTS-i kohaldamisalas sama seaduse § 3 lg 4 punkti 1 tõttu. Samas saame aru, et eelnõuga soovitakse tekitada olukord, kus pensioniregistri pidaja (vastutav töötleja ja volitatud töötleja) kohaldaks DORA määruse nõudeid.

Seetõttu soovitame hinnata, kas eelnõu § 9 punkt 3 (EVKS täiendamine §-ga 30^2) on piisav, et seletuskirjas toodud olukord saavutada. Ehk tuleb hinnata, kas eelnõud tuleb siin täiendada, tehes EVKS-is täiendavad sätted või kas alternatiivina tuleks teha täiendav säte KüTS §-s 3. Oleme valmis arutama, et kas see muudatus võiks olla NIS2 direktiivi üle võtvas eelnõus – selleks palume ühendust võtta siinse vastuse koostajaga.

Kui leiate, et eelnõuga kavandatavad sätted on piisavad, siis palume EVKS § 30^2 lõike 2 sõnastamisel lähtuda kavandatava KAS § 82^4 lõike 3 sõnastusest, sh vt ka eespool olevat märkust nr 8.

14. Väärtpaberituru seaduse muudatused

NIS2 direktiivi subjektide hulka on hõlmatud finantsturutaristust Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL artikli 4 punktis 24 määratletud kauplemiskohtade korraldajad ning Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 artikli 2 punktis 1 määratletud kesksed vastaspooled (vt NIS2 direktiivi lisa I punkti 4).

Väärtpaberituru seadus reguleerib muu hulgas ka kauplemiskohtade korraldajate ning kesksete vastaspoolte tegevust. Eeldame, et tegemist on samade ettevõtjatega/isikutega, mis on nimetatud eelmises alapunktis.

Eeltoodu tõttu soovitame hinnata, kas eelnõud on vaja täiendada sättega nagu on planeeritud KAS §-i 82^4. Siin vt ka eespool olevat märkust nr 9.

Lugupidamisega

(allkirjastatud digitaalselt)
Tiit Riisalo
majandus- ja infotehnoloogiaminister

Raavo Palu
raavo.palu@mkm.ee
Liina Lumiste
liina.lumiste@ria.ee