MÄRKUSTE TABEL

Justiitsministeerium	**Märkused 1–3**
Majandus- ja kommunikatsiooniministeerium	**Märkused 4–17**
Riigikantselei	**Märkused 18 ja 19**
Finantsinspektsioon	**Märkused 20–28**
Pangaliit	**Märkused 29–32**
FinanceEstonia	**Märkused 33–35**
Eesti Kaubandus- Tööstuskoda	**Märkused 36 ja 37**

Nr.	**Ettepaneku sisu**	**Arvestatu/ Mitte arvestatud/ Selgitatud**	**Rahandusministeeriumi seisukoht**
JUSTIITSMINISTEERIUM			
1. JuM	1. Eelnõu § 7 punktiga 11 ja § 9 punktiga 9 muudetakse olemasolevate sätete asukohta. Viidatud sätete sisuks on väärteo aegumise erisus üldisest aegumise tähtajast (mis on karistusseadustiku § 81 lõike 3 kohaselt kaks aastat). Justiitsministeerium ei toeta eraldi aegumise paragrahvi sätestamist. Aegumise erand tuleb sätestada menetluse paragrahvis. Sel juhul on see kooskõlas teistes eriseadustes ettenähtud regulatsiooniga, nt riigihangete seaduse § 216 lõikega 2, maksukorralduse seaduse §-ga 162. Samuti puuduvad seletuskirjas täpsemad selgitused, miks peab olema kooskõlastamiseks esitatud eelnõus olevate väärtegude aegumistähtaeg kolm aastat. Palume seletuskirja lisada vastav põhjendus.	Arvestatud/ Selgitatud	Eelnõusse on lisatud muudatused, mille kohaselt väärtegude aegumissätted on tõstetud menetluse paragrahvi. Samas juhime tähelepanu, et eelnõuga ei nähta ette ühetegi uut väärtegude aegumist reguleerivat normi ja kõik aegumistähtajaga seotud muudatused eelnõus on normitehnilised, st nii KAS-is, EVKS-is kui ka VpTS-is on juba kehtiva õiguse kohaselt aegumistähtaeg kolm aastat. Finantssektori väärtegude aegumistähtajad nähti ette finantsvaldkonna väärteokaristuste reformi raames ning vastavate õigusnormide kohta on esitatud selgitused vastava eelnõu seletuskirjas[1]. Samuti on JuM juhtinud karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse[2] teise lugemise seletuskirjas juhtinud tähelepanu asjaolule, et ***„Arvestades siiski teatud valdkondade eripära, võib senisest suuremate trahvide korral olla põhjendatud ka pikemate aegumistähtaegade sätestamine****. Nii näiteks on EL määruse (EU) 468/2014 artikli 130 kohaselt Euroopa Keskpanga poolt kohaldatavate trahvide korral aegumistähtajaks 5 aastat. Kui krediidiasutus ei allu Euroopa Keskpanga järelevalvele, oleks Eestis sama rikkumise korral aegumistähtaeg põhjendamatult lühem. Kehtiv KarS § 81 lg 3 näeb ette, et üldreeglina on väärteo aegumistähtaeg 2 aastat ning seaduses sätestatud juhtudel võib ette näha kolmeaastase aegumistähtaja. Ettepaneku kohaselt jääks KarS § 81 lg 3 üldreegliks 2 aastat, kuid seaduses võib ette näha*

[1] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/aece8f34-146c-41f6-b3fd-90402dfdd470/audiitortegevuse-seaduse-finantskriisi-ennetamise-ja-lahendamise-seaduse-ning-teiste-seaduste-muutmise-seadus-finantsvaldkonna-vaarteokaristuste-reform-eli-oigusest-tulenevad-karistused

[2] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1bfa1944-2de6-449d-a788-887bc84cfd0f/karistusseadustiku-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus-euroopa-liidu-oigusest-tulenevad-rahatrahvid

			ka kuni 5-aastase aegumistähtaja (so kolme-, nelja- või viieaastase aegumistähtaja). Arvestades siiski, et 5-aastane aegumistähtaeg on ka teise astme kuriteo aegumistähtajaks, peaks nii pikk aegumistähtaeg väärtegude korral olema siiski erandlik.“. Viidatud reformi raames otsustati mitte rakendada maksimaalset (viieaastast) tähtaega, kuid tuginedes JuM selgitustele, oli põhjendatud näha ette kolmeaastane tähtaeg.
2. JuM	2. Eelnõu seletuskirjas (lk 26) kindlustustegevuse seaduse § 138 muutmise selgituse juures on asjakohane viide Euroopa Parlamendi ja nõukogu direktiivile (EL) 2019/2121, millega muudetakse direktiivi (EL) 2017/1132 seoses äriühingute piiriülese ümberkujundamise, ühinemise ja jagunemisega. Nimetatud direktiivi põhjenduspunkt 57 võimaldab finantssektori puhul direktiivist erandeid teha, samas tuleb tähele panna, et siseriiklikult kehtestatud erandid peavad olema siiski seotud krediidivahendusettevõtjate ja teiste finantsettevõtjate tegevust reguleerivate Euroopa Liidu (EL) reeglite ja normidega. Seetõttu palume eelnõu seletuskirjas täpsemalt välja tuua, millise EL-i regulatsiooni alusel erandid kehtestatakse. Palume lisada vastavad selgitused ka väärtpaberituru seaduse ning makseasutuste ja e-raha seaduse vastavate muudatuste juurde.	Arvestatud	Seletuskirja on täiendatud.
3. JuM	3. Palume lisaks arvestada käesoleva kirja lisades esitatud eelnõu ja seletuskirja failis jäljega tehtud normitehniliste ja keelemärkustega ning märkustega eelnõu mõju kohta.	Arvestatud	
MAJANDUS- JA KOMMUNIKATSIOONIMINISTEERIUM			
4.	**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 IKTriski 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	Mitte arvestatud	DORA määruse artikkel 46 annab selge normi, et DORA määruse kohane pädev asutus **on sama asutus**, kes on määratud riigis finantsasutuse üle **finantsjärelevalvet teostama**. Eestis on riiklikuks finantsjärelevalve asutuseks Finantsinspektsioon ja oluliste krediidiasutuste korral Euroopa Keskpank. Seega ei ole tegemist DORA määrusest tuleneva liikmesriigi valikukohaga, keda määrata DORA pädevaks asutuseks, vaid otsekohalduvast määrusest tuleneva asjaoluga, et pädev asutus on sama asutus, kes on finantsjärelevalveasutus. Seega tähendaks finantssektoris muu pädeva asutuse määramine finantsjärelevalve ümberkorraldamist Eestist. Vaata täiendavaid selgitusi seletuskirja punkti 2.3.2 alampunktis E. Nõustume, et RIA-s on parim küberturbe kompetents, kuid ka Finantsinspektsioon on aastaid teostanud finantssektoris järelevalvet selle üle, kuidas finantsasutused järgivad Finantsinspektsiooni kehtestatud nõudeid finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele, nõudeid finantsjärelevalve subjekti talitluspidevuse korraldusele, EBA suuniseid IKT- ja turvariskide

	75 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.		juhtimiseks ning EIOPA info- ja kommunikatsioonitehnoloogia turbe- ja juhtimissuuniseid ja pilveteenuse osutajatele tegevuse edasiandmise suunised. Rääkimata riskijuhtimise (operatsiooniriski) ja tegevuste edasiandmise järelevalvest üldisemalt. Finantssektor on terviklik, mida tuleb vaadelda kompaktselt, mis tähendab, et ka järelevalve on terviklik ja kompaktne. Esitame näite (seletuskirja kl 12 ja 13 on näiteid rohkem). Krediidiasutuste direktiivis on sätestatud „**Finantsinstitutsioonidel peab olema kindel äriühingu juhtimise korraldus, mis hõlmab** selget organisatsioonilist ülesehitust, mille puhul vastutusalad on selgesti määratletud, läbipaistvad ja järjepidevad, tõhusaid protseduure riskide või võimalike riskide kindlaksmääramiseks, juhtimiseks, jälgimiseks ja nendest teatamiseks, piisavat sisekontrollikorda, sealhulgas usaldusväärne juhtimis- ja raamatupidamiskord, **võrgu- ja infosüsteeme, mis on loodud ja mida hallatakse kooskõlas määrusega (EL) 2022/2554**, ning tasustamispoliitikat ja -tavasid, mis on kooskõlas usaldusväärse ja tõhusa riskijuhtimisega ja edendavad seda.“ Näite kohaselt ei oleks FI-l võimalik teostada krediidiasutuse juhtimise korralduse üle terviklikku järelevalvet, jättes järelevalvest välja võrgu- ja infosüsteemide järelevalve. Finantsinspektsioon on mh alustanud oma küberkompetentsi suurendamisega (täiendavate ekspertide kaasamine).

	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.		
5. MKM	**2. Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 ehk 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 Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ehk 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-l 13 olev tabel ja eelnõu § 3 sisu ning selgitus).	Selgitatud	Hoiu-laenuühistutele DORA nõudeid ei kohaldata, kuid kui hoiu-laenuühistute seaduseelnõu jõustumisel kohalduvad ühistupankadele mh krediidiasutuste seaduse sätted, siis see tähendab ühtlasi nende suhtes DORA nõuete kohaldamist ja Finantsinspektsiooni järelevalve alla kuulumist.
6. MKM	**3. NIS2 direktiivi järgimine** Seletuskirja lk-l 15 on tabel, mille üks tulp on ka NIS2 direktiivi kohta. Tolles tabelis on krediidiasutuste ja finantsturutaristute real märgitud NIS2 direktiivi artikli 4 lõigete 1 ja 2 sisu	Arvestatud	Seletuskirja on täiendatud. Samas juhime tähelepanu, et tegemist on suuresti riigi ja pädevate asutuste suhtes kohalduvate nõuetega ning vähesemal määral nõuetega, mida ettevõtjad peavad lisaks DORA-le järgima.

	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“ – leitav siit: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52023XC0918(01). 2.5. Eeltoodu tõttu **palume** seletuskirja täiendada eelmainitud sätetega.		
7. MKM	**4. Riigi Infosüsteemi Ameti 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 Riigi Infosüsteemi Ametit (edaspidi: RIA). 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, 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.	Teadmiseks võetud	
8. MKM	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 küberturvalisuse seadusele (edaspidi: KüTS). Seda ennekõike seetõttu, et NIS2 direktiiviga ei muutu „võrgu- ja infosüsteemi“ mõiste ning hetkel on selle mõiste sisu üle võetud KüTS § 2 punktis 1.	Arvestatud	FELS § 29 lõike 1 punktis 8 on DORA viide asendatud viitega KüTS § 2 punktile 1.
9. MKM	**6. Planeeritav finantsinspektsiooni seaduse (edaspidi: FIS) § 47[11]** FIS § 47[11] lg 1 punkti 2 kohaselt hõlmab Finantsinspektsiooni (edaspidi: FI) ja RIA vaheline koostöö muu hulgas RIA-lt tehnilise nõu ja abi küsimine ning FI-le selle andmine […].	Arvestatud	

	Me pole üldiselt vastu tolles 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.		
10. MKM	**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.	Selgitatud	Käesoleva eelnõu raames me ei näe vajadust FIS § 54 lõike 4 täiendamiseks.
11. MKM	**8. Ebatäpsused FIS §-ga 54^2** Juhime tähelepanu, et eelnõu § 2 punktiga 6 täiendatakse FIS § 54^2 lõikega 4, kuid seletuskirjas tolle lõike kohta ei ole selgitusi esitatud. Samuti on seletuskirjas (lk 20) toodud selgitus FIS § 54^4 täiendamise kohta lõikega 4^1, kuid eelnõus sellist lõiget pole.	Arvestatud	Seletuskirjas on asendatud lõige 4^1 lõikega 4.
12. MKM	**9. KüTS-i nõuete kohaldumine krediidiasutustele** Eelnõu § 7 punktiga 4 lisandub krediidiasutuste seadusesse (edaspidi: KAS) § 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 2. 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	Selgitatud	Meie hinnangul ei pruugi olla DORA määrusega kooskõlas lähenemine, et ettevõtjaid kohustatakse järgima konkreetseid standardeid. Näiteks DORA drafti kohaselt peaksid ettevõtjad võtma arvesse **juhtivaid tavasid ja vajaduse korral asjakohaseid rahvusvahelisi standardeid**, kui töötavad välja ja rakendavad järjepidevaid ja ajakohaseid IKT-turbepoliitikaid, mis toetavad DORA nõuetele vastavuse tagamist (ehk see on jäetud paindlikuks). DORA nõuetele vastavuse tõendamiseks **on soovitatud** finantsasutustel rakendada ISO/IEC 27001 standardit (RTS-ide väljatöötamisel on mh võetud arvesse viidatud standardit ja nagu eespool osutatud, on ka viidatud rahvusvahelistele standarditele). Juhime tähelepanu, et KüTS § 7 lõikes 5 sätestatud volitusnorm on kehtiva sõnastuse kohaselt ette nähtud samas paragrahvis ehk §-s 7 sätestatud kohustuste täitmise ja süsteemide küberturvalisuse tagamiseks. Kuna DORA kohaldamisalasse kuuluvatele finantsasutusele ei kohaldata §-i 7, siis ei kohaldu neile ka viidatud standardid. Ka võrgu- ja infosüsteemide küberturvalisuse nõuete määruse kohaselt ei ole teenuse osutaja kohustatud rakendama Eesti infoturbestandardit, kui tema turvameetmed vastavad rahvusvahelise standardiga ISO/IEC 27001 kehtestatud nõuetele ja tal on selleks sertifikaat. Seega meie arusaamise järgi ei ole ka kehtiva õiguse kohaselt nad kohustatud rakendama lisaks rahvusvahelise standardile Eesti spetsiifilisi nõudeid. Kui MKM hinnangul on asjakohane kohaldada finantsasutustele täiendavaid (mitte dubleerivaid), sh **Eesti spetsiifilisi** nõudeid, saame omapoolse

	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.		seisukoha kujundada pärast tutvumist vastavate muudatusettepanekutega.
13. MKM	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.	Selgitatud	Vastav täpsustus (viide peatükile 12) lisatakse punkti 11, mis loob eelduse, et ka sellele eelnevad paragrahvid on peatükis 12.
14. MKM	**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 4.	Selgitatud	Eelnõu puhul on otsustatud jääda DORA direktiivis kasutatava terminoloogia juurde. Näiteks asendatakse MERAS direktiivis termin „infosüsteem“ terminiga „info- ja kommunikatsioonitehnoloogia süsteem“. Sama on MiFID2 direktiivi terminoloogiaga.
15. MKM	**12. Eelnõu § 9 punktis 1 ehk väärtpaberite registri pidamise seaduse** (EVKS) § 7^1 lõike 5 esimese lause muudatuses on RIA nimetus nurksulgudes.	Arvestatud	Nurksulud on kustutatud.
16. MKM	**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	Selgitatud	Eelnõu on muudetud ja pensioniregistrile ei hakata kohaldama DORA määruse nõudeid ning neile jäävad kohalduma KüTS nõuded.

	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.		
17. MKM	**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 (edaspidi: VpTS) 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 8.	Arvestatud	Korraldaja puhul on eelnõusse lisatud täpsustus, et tema suhtes ei kohaldata KüTS 2. peatükis sätestatud küberturvalisuse nõudeid.
RIIGIKANTSELEI			
18. RK	**1.** Eelnõu seletuskirja lk-del 14-15 on esitatud eksitav CER direktiivi[1] tõlgendus. Seletuskirjas viidatakse CER direktiivi põhjenduspunktile nr 21 ning selgitatakse, et kuna finantssektori ettevõtjate toimepidevus on põhjalikult hõlmatud DORA regulatsiooniga[2], ei tuleks selliste ettevõtjate suhtes kohaldada CER direktiivi artiklit 11 ning III, IV ja VI peatükki, et vältida dubleerimist ja ebavajalikku halduskoormust. Vaatamata sellele peaksid liikmesriigid CER direktiiviga ette nähtud kriteeriumide põhjal ja selles sätestatud menetlust kohaldades identifitseerima sellised finantssektori ettevõtjad elutähtsa teenuse osutajana ning kohaldama nende suhtes CER direktiivi II peatükis sätestatud strateegiaid, liikmesriigi riskianalüüse ja toetusmeetmeid. **Seletuskirjas on jäetud täies ulatuses arvestamata direktiivi artiklites sätestatuga.** CER direktiivi artikli 3 kohaselt ei takista CER direktiiv liikmesriike elutähtsa teenuse osutajate	Arvestatud	Seletuskirja on lisatud täpsustus, et liikmesriigid võivad vastu võtta või säilitada liikmesriigi õigusnormid, millega saavutada kõnealuste elutähtsa teenuse osutajate toimepidevuse kõrgem tase, tingimusel et need õigusnormid on kooskõlas kohaldatavate liidu õigusenormidega.

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ.
[2] Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (DORA määrus) ja -Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/25562, millega muudetakse direktiive 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, 2013/36/EL, 2014/59/EL, 2014/65/EL, (EL) 2015/2366 ja (EL) 2016/2341 seoses finantssektori digitaalse tegevuskerksusega (DORA direktiiv).

	suurema toimepidevuse saavutamiseks vastu võtmast või säilitamast oma õigusnorme, kui sellised õigusnormid on kooskõlas liikmesriikide liidu õiguses sätestatud kohustustega. Artiklis 8 on omakorda sätestatud, et liikmesriigid tagavad, et artiklit 11 ning III, IV ja VI peatükki ei kohaldata elutähtsa teenuse osutajate suhtes, kelle nad on identifitseerinud lisa tabeli punktides 3, 4 ja 8 esitatud sektorites. Sama artikli teine lause aga täpsustab, et l**iikmesriigid võivad vastu võtta või säilitada liikmesriigi õigusnormid, millega saavutada kõnealuste elutähtsa teenuse osutajate toimepidevuse kõrgem tase, tingimusel et need õigusnormid on kooskõlas kohaldatavate liidu õigusenormidega.** **Sellest tulenevalt ei ole CER direktiivi artikli 11 ning peatükkide III, IV ja VI välistamine DORA subjektide suhtes imperatiivne, vaid liikmesriigi enda valik**. Seletuskirjas on õigesti märgitud, et Riigikantselei on CER direktiivi ülevõtmiseks välja töötanud hädaolukorra seaduse ja teiste seaduste muutmise seaduse eelnõu[3] (*HOS CER eelnõu*). Nimetatud eelnõu väljatöötamisel on analüüsitud CER direktiivi ülevõtmise võimalused ning on jõutud järelduseni, et on mõistlik säilitada Eesti olemasolevat elutähtsate teenuste regulatsiooni ja integreerida CER direktiivist tulenvaid muudatusi olemasolevasse regulatsiooni. Seda siis ka elutähtsa teenuse osutajatest krediidiasutuste suhtes. Juhime ka tähelepanu sellele, et nii DORA regulatsioonid kui ka NIS2[4] direktiiv keskenduvad IKT riskidele ja küberturvalisusele. CER direktiiv on oluliselt laiem ning keskendub elutähtsate teenuste toimepidevusele tervikuna ning seega ei ole DORA ja NIS2 sellega samaväärsed. Oluline on panna tähele ka seda, et CER kohaselt on elutähtsa teenuse osutajate krediidiasutuste pädevaks asutusteks on lisaks Finantsinspektsioonile ja Euroopa Keskpangale ka Eesti Pank elutähtsa teenuse toimepidevust korraldava asutusena. Eelnevast tulenevalt palume asendada seletuskirjas toodud selgitusi, sh leheküljel 15 esitatud tabelis toodu CER direktiivi kohta eespool toodud selgitustega.		

[3] https://eelnoud.valitsus.ee/main/mount/docList/ad7af8cd-617c-45f3-b850-78ad002f6a3a.

[4] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148.

19. RK	Krediidiasutuste seadust täiendatakse §-ga 47^{11}, mis reguleerib koostööd küberturvalisuse valdkonnas. Paragrahvi 47^{11} lõike 1 punkti 3 kohaselt hõlmab koostöö Finantsinspektsiooni ja Riigi Infosüsteemi Amet teabe vahetamist asutuste vahel, sealhulgas küberintsidentide ja küberohtude kohta ning küsimustes, mis puudutavad **elutähtsaid** krediidiasutusi ja kauplemiskohti. Jääb ebaselgeks, mida mõeldakse elutähtsate krediidiasutuste all. NIS2 eristab elutähtsaid (lisa I) ja olulisi üksuseid (lisa II). Kas tegemist on elutähtsate üksustega NIS2 mõistes või soovitakse hoopis piirduda elutähtsa teenuse osutajatest krediidiasutustele? Elutähtsa teenuste osutajate ring on väga piiratud, elutähtsate üksuste ring NIS2 mõistes laiem. Palun täpsustada seda asjaolu ning vajadusel täiendada eelnõu ja seletuskiri.	Arvestatud	Märkuse puhul on ilmselt mõeldud Finantsinspektsiooni seaduse muutmist, mitte krediidiasutuste seaduse muutmist. Oleme eelnõus täpsustanud, et mõeldud on finantsjärelevalve subjekte, kes on elutähtsa teenuse osutajad.
FINANTSINSPEKTSIOON			

	Eelnõu ettepanekud		
20. FI	1. Euroopa järelevalveasutused (ESA-d) on välja töötamas tehnilisi standardeid intsidentidest ja küberohtudest teavitamise kohta, mis esitatakse Euroopa Komisjonile hiljemalt 17.07.2024 (DORA määruse artikkel 20). Tehnilised standardid võivad kehtestada andmete esitamise formaadid, mida subjektid peavad kasutama FI-le andmeid edastades. FI hinnangul tuleb täiendada Eelnõu sätteid intsidentidest ja küberohtudest teavitamise puhul selliselt, et FI-l oleks vajadusel võimalik kehtestada andmete esitamiseks kindel formaat (sarnaselt näiteks MiCA tehniliste standartide eelnõu artiklile 41: „Issuers shall submit the information referred to in this Regulation in the data exchange formats and representations specified by the competent authorities and respecting the data point definition of the data point model and the validation formulae stated in Annex V and the following specifications…“). Sellest tulenevalt teeme järgmised ettepanekud:	Selgitatud	Vt kommentaari märkuse nr 20 juures.
21. FI	a) Täiendada Eelnõu § 4 punkti 7, millega täiendatakse investeerimisfondide seadust (edaspidi IFS) §- ga 345^1 , lisades IFS § 345^1 lõike 1 lõppu lause: „Finantsinspektsioon võib määrata tõsisest info- ja kommunikatsioonitehnoloogiaga seotud intsidendist teavitamise formaadi.“ Samasisulise muudatuse palume teha Eelnõu § 5 punktis 6 (kindlustustegevuse seaduse (edaspidi KindlTS) § 1051 lõige 1), § 7 punktis 5 (krediidiasutuse seaduse (edaspidi KAS) § 92^3 lõige 1), § 8 punktis 16 (makseasutuste ja e-raha asutuste seaduse (edaspidi MERAS) § 63^6 lõige 6), § 9 punkti 3 (väärtpaberite registri pidamise	Selgitatud	Märkuses on ettepanek, et Finantsinspektsioon võib määrata tõsisest IKT-ga seotud intsidendist teavitamise formaadi. Juhime tähelepanu DORA määruse ITS draftile, mille kohaselt teave esitatakse DORA vorme kasutades ning pädev asutus määrab andmevahetusvormingu ja esitusviisi[3]. Meie hinnangul ei ole valikuline formaadi määramine kooskõlas DORA regulatsiooniga. Art 8 – 1. *Financial entities shall submit the information referred to in this Regulation in the data exchange formats and representations specified by competent*

[3] https://www.eiopa.europa.eu/system/files/2023-12/JC%202023%2070%20-%20%20CP%20on%20draft%20RTS%20and%20ITS%20on%20major%20incident%20reporting%20under%20DORA.pdf

	seaduse (edaspidi EVKS) § 30^2 lõige 3), § 10 punktis 11 (väärtpaberituru seaduse (edaspidi VPTS) § 82^{18} lõige 1).		*authorities and respecting the data point definition of the data point model and the validation formulas specified in Annex V as well as the following specifications: ….* Samuti on artiklis 4 täpsustus, et *1. Financial entities shall use secure electronic channels to submitting intimal notification and intermediate and final reports as agreed with the competent authorities.*
22. FI	b) Täiendada Eelnõu § 4 punkti 7, lisades IFS § 345^1 lõike 3 lõppu lause: „Finantsinspektsioon võib määrata olulisest küberohust teavitamisel andmete esitamise formaadi.“ Samasisulise muudatuse palume teha Eelnõu § 5 punktis 6 (KindlTS § 1051 lõige 3), § 7 punktis 5 (KAS § 92^3 lõige 3), § 8 punktis 16 (MERAS § 63^6 lõige 8), EVKS § 30^2 lõige 5), § 10 punktis 11 (VPTS § 82^{18} lõige).	Selgitatud	Vt selgitust märkuse nr 21 juures.
23. FI	2. Riigisiseselt on tehtud valik mitte kohaldada DORA määrust hoiu-laenuühistule, sest õiguslikult ei ole hoiu-laenuühistud hetkel finantsjärelevalve subjektid. Käesoleva Eelnõuga samaaegselt on menetluses hoiu-laenuühistute seaduse ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu, mille lõplikust sisust sõltub, kuidas näha ette digitaalse tegevuskerksuse nõuete rakendamine ka hoiulaenuühistutele. Hetkel kehtiv KAS § 38 sätestab et ühistupankade tegutsemisel kohaldatakse hoiulaenuühistu kohta sätestatut, kui KAS-st ei tulene teisiti. Eelnõu §-iga 3 täiendatakse hoiu-laenuühistu seadust §-iga 2 1 , mille kohaselt hoiu-laenuühistule DORA määrust ei kohaldata, mistõttu on selle valguses võimalik ka tõlgendus, et DORA määruse nõuded ühistupankadele ei kohaldu. Selleks, et tagada õigusselgust, tuleb KAS-s selgelt sätestada, et DORA määrus kohaldub ka ühistupankadele. Kui hoiu-laenuühistud tulevad FI järelevalve alla ühistupankade vormis, siis pakutud täienduse alusel hakkab neile ka DORA määrus kohalduma.	Selgitatud	HLÜS eelnõus olev säte (KAS § 38 muutmine) „Ühistupanga asutamisel, tegutsemisel ja lõpetamisel kohaldatakse käesolevas seaduses (ehk KAS-is) sätestatut käesolevas peatükis toodud erisustega“ tagab, et ühistupanga tegutsemisele kohaldatakse mh DORA nõudeid, kuivõrd need on hõlmatud KAS uute §-dega 82^4 ja 92^3.
24. FI	3. Juhime tähelepanu, et Eelnõuga täiendatakse väärteokoosseise eriseadustes, kuid karistused on seal alternatiivsed – „karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas“ ja juriidilise isiku puhul „karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest“. Eelnõuga ei ole sätestatud juhiseid ega kriteeriume, mille alusel peab FI eeltoodud alternatiive kaaluma. Lisaks rõhutame uuesti, et väärteomenetlus pole tõhus menetlusvorm finantsõiguse rikkumiste menetlemiseks.	Selgitatud	Kuna DORA nõuded integreeritakse DORA direktiiviga finantssektori liidu õigusaktidesse, siis ka eriseadustes vastavate paragrahvide sõnastamisel on lähtutud asjaolust, et karistused peavad olema kooskõlas EL õigusega. Vt näiteid ka märkuse nr 36 juures.
	Täiendavad ettepanekud		
25. FI	4. Kuivõrd Eelnõuga muudetakse enamikke Finantsinspektsiooni seaduse § 2 lõikes 2 nimetatud eriseadusi, siis palume IFS-i, KindlTS-	Mitte arvestatud	Muudatusi analüüsitakse ja nähakse ette muu finantssektori eelnõuga.

	i, KAVS-i, KAS-i, MERAS-esse ja VPTS-i sisse viia muudatused kohapealse kontrolli sätetes, mille kohta oleme ettepanekud edastanud Rahandusministeeriumile 08.05.2023 kirjaga nr 5-1/2654. Täpsemad põhjendused leiab samuti nimetatud kirjast.		
26. FI	5. Teeme ettepaneku muuta MERAS-e järgmisi sätteid: a) MERAS § 17 lõige 5 sätestab, et FI võib jätta tegevusloa taotluse läbi vaatamata, kui taotleja ei ole kõrvaldanud puudusi ettenähtud tähtaja jooksul või ei ole esitanud tähtpäevaks nõutud andmeid ja dokumente. Soovime laiendada läbi vaatamata jätmise võimalust ka olukorrale, kus taotlus on esitatud oluliste puudustega. Meie ettepanek on muuta MERAS § 17 lõiget 5 järgmiselt: *„(5) Kui taotleja ei ole kõrvaldanud käesoleva paragrahvi lõikes 1 nimetatud puudusi ettenähtud tähtaja jooksul või ei ole tähtpäevaks esitanud Finantsinspektsiooni nõutud andmeid või dokumente või taotlus on esitatud oluliste puudustega, võib Finantsinspektsioon jätta tegevusloa taotluse läbi vaatamata*.“.	Arvestatud	
27. FI	b) MERAS § 24 lõige 3. FI hinnangul on MERAS-e sätted, mis puudutavad piiriüleselt makseteenuse osutamist kolmandas riigis, ebaselged ja puudulikud, mistõttu on Finantsinspektsioonil takistatud nende taotluste menetlemine, kus taotleja soovib piiriüleseid makseteenuseid osutada kolmandas riigis (näiteks Suurbritannia ja Põhja-Iirimaa Ühendkuningriigis). MERAS § 24 lõike 3 kohaselt kohaldatakse Eesti makseasutuse ja e-raha asutuse poolt kolmandas riigis teenuste osutamisele MERAS §-des 25-28, § 29 lõigetes 1, 2, 8 ja 10 ning § 92 lõigetes 11 ja 12 sätestatut. Käesoleval juhul on asjakohane üksnes § 29 lõiked 1, 2, 8 ja 10. Nimetatud sätetest ükski ei viita sellele, mida FI talle esitatud teabega tegema peab. MERAS § 29 lõike 8 teine lause viitab läbi lõike 6 punkti 1 justkui, et FI peab heakskiidu andma, aga samas nimetatud heakskiidu aluseks on MERAS § 29 lõike 6 kohaselt „sihtriigi finantsjärelevalve asutuse hinnang“. Nimetatud sihtriigi finantsjärelevalve asutuse hinnangu saamine eeldab siiski MERAS § 29 lõikes 3 nimetatud tegevusi. Sellisel juhul oleks vajalik MERAS § 24 lõike 3 viidete täiendamine. Vastav täiendus kõrvaldaks ka puuduse menetlustähtaja osas, mida käesoleval juhul sätestatud ei ole. Probleemseks peame ka seda, et kolmandas riigis piiriüleselt teenuste osutamise avalduse osas ei ole FI-le jäetud MERAS § 29 lõike 5 kohast dokumentide edastamise keeldumisõigust. Kokkuvõtvalt soovime piiriüleste makseteenuste osutamise avalduste osas kolmandas riigis selgemat reeglistikku, mis ei pea olema üks-ühele lepinguriigi sätetega, aga võiks sisaldada olulisemat, st FI ülesanne, menetlustähtaeg,	Arvestatud	MERAS § 24 lõiget 3 on muudetud ja sama paragrahvi on täiendatud uue lõikega 4^1.

	keeldumisalused jms. Seejuures ei peaks eeltoodud olukorras menetlus olema n-ö kahe-etapiline (lepinguriigi osas teeb FI sisuliselt kaks otsust MERAS § 29 lõiked 3 ja 6), vaid FI teeb samaaegselt otsuse andmete ja dokumentide edastamise ning nimekirja kandmise kohta.		
28. FI	c) MERAS § 44 lõike 1 punktis 3 on viide paragrahvile 54, kuid õige oleks viide §-le 39. Palume nimetatud viide parandada.	Arvestatud	
PANGALIIT			
29. EPL	**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.	Selgitatud	Märkus on seotud CER direktiivi ülevõtmise menetlusega, mille vastutavaks asutuseks on Riigikantselei.
30. EPL	**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.	Selgitatud	Märgime, et ettepanek kuulub HOS eelnõu skoopi, mis reguleerib elutähtsate teenuste toimivust ja koostööd vastavate asutuste vahel. HOS eelnõu vastutavaks asutuseks on Riigikantselei. Juhime tähelepanu, et FIS-is on juba olemas Finantsinspektsiooni ja Eesti Panga koostöö kokkulepet reguleeriv säte. § 50 kohaselt võib Inspektsioon sõlmida kahe- või mitmepoolse kokkuleppe koostöö korraldamiseks Eesti Panga, Rahandusministeeriumi või muu riigiasutusega, kui selline koostöö on vajalik, et aidata kaasa finantsjärelevalve eesmärgi saavutamisele. Inspektsioon, Rahandusministeerium ja Eesti Pank teevad kirjaliku kokkuleppe alusel koostööd aruannete kogumisel ja analüüsimisel, õigusaktide eelnõude väljatöötamisel ning kriisilahendusmeetmete või -õiguste kavandamisel ja rakendamisel ning teabe vahetamisel finantssektori olukorda oluliselt mõjutavate sündmuste korral.
31. EPL	**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. 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	Selgitatud	CER direktiivi rakendamine on Riigikantselei vastutusalas. Riigikantselei on osutanud, et CER direktiivi artikli 8 lõike 1 teine lause ütleb, et liikmesriigid võivad vastu võtta või säilitada liikmesriigi õigusnormid, millega saavutada kõnealuste elutähtsa teenuse osutajate toimepidevuse kõrgem tase.

	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.		
32. EPL	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.	Selgitatud	Kuna eelnõu kohaselt ei kohaldata krediidiasutustele küberturvalisuse seaduse 2. peatükis sätestatud küberturvalisuse tagamise nõudeid, tähendab see ühtlasi, et krediidiasutustele ei kohaldata seaduse §-i 7, mille lõikes 5 on volitusnorm viidatud määrusele. Volitusnorm on ette nähtud §-s 7 sätestatud kohustuste täitmise ja süsteemide küberturvalisuse tagamiseks. Seega, kuna krediidiasutustele ei kohaldata §-i 7, ei ole asjakohane ka määruse kohaldamine. Lisaks on eelnõusse lisatud õigusselguse tagamiseks muudatus, millega välistatakse ka hädaolukorra seaduse § 41 lõike 1 kohaldamine, milles on viited küberturvalisuse seaduse § 7 ja 8 kohaldamisele.

	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 auditit el; 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.		
FINANCE_ESTONIA			

33. FE	Ebaselgus seoses halduskaristuste laienemisega DORA määruse[4] artikli 19 lg-s 2 toodud vabatahtliku raporteerimiskohustuse täitmatajätmisele. DORA määruse artikkel 19 näeb tõsistest IKT intsidentidest teavitamise kohustuse kõrval ette ka finantssektori ettevõtjate poolt vabatahtlikult olulistest küberohtudest teavitamise võimaluse. Seejuures viitab määruse artikli 19 pealkiri, selle lg 2, samuti määruse asjaomased põhjenduspunktid (24) ja üldsätted (sh artikli 1 lg 1 punkt a alapunkt ii), ning ka eelnõu enese seletuskiri läbivalt sellele, et küberohtudest teavitamine finantssektori ettevõtjate poolt toimub vabatahtlikkuse alusel. Kuigi eelnõu kohaselt ei plaanita asjaomase teavitamisvõimaluse kajastamisel eri finantssektori ettevõtjate tegevust reguleerivates eriseadustes (nt nagu krediidiasustuste seadus, investeerimisfondide seadus, kindlustustegevuse seadus jne) viidata selgelt vabatahtlikkusele, vaid teavitamise vabatahtlikkusele viidatakse mõnevõrra kaudsema sõnastusega („*kui [asjaomane finantssektori ettevõtja] otsustab Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554 artikli 19 lõike 2 kohaselt teavitada /---/*“), on määruse mõte ja seega peaks olema ka eelnõu mõte sätestada olulistest küberohtudest teavitamine just võimaluse ja mitte kohustusena. Sellest hoolimata on erinevate finantssektori ettevõtjate tegevust reguleerivate õigusaktide vastutust reguleerivate sätete muudatused eelnõu kohaselt kavandatud selliselt, et halduskaristusi digitaalse tegevuskerksuse nõuete rikkumise eest on võimalik kohaldada ka DORA määruse artikli 19 lg-s 2 toodud vabatahtlikkuse alusel täidetava raporteerimiskohustuse mittetäitmise korral, täpsemalt hõlmavad vastavad vastutuse sätted muu hulgas DORA määruse artikli 19 lg-d 1-5 s.t ka lg-s 2 sätestatud vabatahtliku teavitamisvõimaluse. On arusaadav, et DORA määruse mõttega on enim kooskõlas ning selle eesmärke aitab parimal võimalikul määral saavutada olukord, kus määruse nõuetega hõlmatud finantssektori ettevõtjad teavitavad pädevat asutust ka DORA määruse artikli 19 lg-s 2 nimetatud olulistest küberohtudest. Teisalt näeb DORA määrus vastava teavitamise (erinevalt olulistest IKT intsidentidest	Arvestatud	Nõustume, et karistuste ulatusse ei peaks jääma vabatahtlik teavitamiskohustus. Eelnõu on vastavalt korrigeeritud.

[4] Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011

	teavitamisele) selgelt ette vabatahtlikuna, mistõttu ei ole võrdväärsete halduskaristuste kohaldamise võimaluse ettenägemine kõnealuse vabatahtliku teavitamisvõimaluse mittekasutamise puhul ebaloogiline ning ka ebaproportsionaalne. Võimalik, et eelnõu ettevalmistajate eesmärgiks on olnud võimaliku sanktsioneeritava kohustusena määruse artikli 19 lg 2 kontekstis hõlmata vaid see, kui asjaomane finantssektori ettevõtja teavitab vabatahtlikult oluliselt küberohust Finantsinspektsiooni, kuid jätab seejuures täitmata kohustuse edastada teavitus ka Riigi Infosüsteemide Ametile, siis kõnealusel juhul see plaanitavate sätete sõnastusest ega ka seaduse seletuskirjast meie hinnangul piisavalt selgelt välja ei tule. Seetõttu soovitame kaaluda määruse artikli 19 lg-s 2 viidatud kohustuse välja jätmist asjaomastest vastutuse sätetest või kajastada vähemalt seaduse seletuskirjas selgelt, et vastavate sätete eesmärgiks ei ole sanktsioneerida vastava vabatahtliku raporteerimisvõimaluse kasutamatajätmist. Vastasel korral ei ole antud raporteerimisvõimalus sanktsiooni kohaldamise võimaluse läbi vabatahtlik, vaid kohustuslik.		
EESTI KINDLUSTUSSELTSIDE LIIT			
34. EKsL	**1) KindlTS § 138. Kindlustusandja ümberkujundamine** Paragrahvile soovitakse lisada uus lõige, mille kohaselt ei ole kindlustusandjate piiriülene ümberkujundamine lubatud. Piiriülene ümberkujundamine tähendab, et Eesti äriühingu saab ümber kujundada lepinguriigi äriühinguks. Arvestades, et finantssektoris teenuse osutamiseks peab isikul olema tegevusluba, mille ta saab asukoha finantsjärelevalve asutuselt, ei ole tarbijakaitse seisukohast asjakohane olukord, kus kindlustusandja viib tegevuse ja kindlustusportfelli üle teise lepinguriiki, kus tal puudub vastava lepinguriigi finantsjärelevalve asutuse luba selles riigis kindlustusteenuse osutamiseks. Samas ei ole tal võimalik tegevusluba taotleda, kui ta on alles Eesti registrisse kuuluv äriühing. Seega kindlustusvõtjate ja kindlustatute kaitse seisukohast ei ole võimalik tagada, et piiriülese ümberkujundamise korral oleks viidatud isikute huvid piisavalt kaitstud. Alternatiiv on asutada lepinguriigis uus kindlustusandja, kellega Eesti kindlustusandja ühineb või kellele Eesti kindlustusandja annab kindlustusportfelli üle. Sellisteks olukordadeks näeb KindlTS ette ka vastava regulatsiooni klientide kaitseks. Euroopa Parlamendi ja Nõukogu Direktiiv (EL) 2019/2121, millega muudetakse direktiivi (EL) 2017/1132 seoses äriühingute piiriülese ümberkujundamise, ühinemise ja jagunemisega põhjenduspunkti 57 kohaselt ei tohiks viidatud direktiiv mõjutada liidu õiguse kohaldamist, mis reguleerib krediidivahendusettevõtjaid ja teisi	Selgitatud	Eelnõusse on lisatud täpsustus, et keeldu ei kohaldata Euroopa Äriühingust kindlustusandjate ümberkujundamisele. Nagu ka seletuskirjas on osutatud, ei ole meie hinnangul Euroopa Liidu õigusega kooskõlas lähenemine, mille kohaselt liigutakse kindlustustegevusega teise lepinguriiki, omamata seal tegevusluba. Kindlustusandjal ei ole võimalik omada kahes riigis samaaegselt tegevusluba. Teise riiki liikumisel tuleks Eesti tegevusluba kehtetuks tunnistada, aga mis saab sellisel juhul kindlustuslepingutest ja lepingutest tulenevate kohustuste täitmisest? Tegevusluba ei liigu koos äriühinguga automaatselt teise liikmesriiki.

	finantsettevõtjaid, ega vastavalt kõnealusele liidu õigusele kehtestatud liikmesriigi õigusnormide kohaldamist. Kindlustustegevust reguleeriva Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EÜ peaeesmärk on kindlustusvõtjate ja soodustatud isikute asjakohane kaitse (põhjenduspunkt 14). Seega on kindlustusandjate piiriülese ümberkujundamise piirang kooskõlas eelnimetatud direktiivi põhimõttega, et tagada tuleb kindlustusvõtjate ja soodustatud isikute kaitse. EKsL-i hinnangul ei ole lisatava kitsenduse põhjus selge ja lisaks ei ole selge selle kitsenduse kooskõla EU määruse nr 2157 /2001 ja Euroopa Liidu Nõukogu määruse (EÜ) nr 2157/2001 «Euroopa äriühingu (SE) põhikirja kohta» rakendamise seaduse nõuetega. Kindlustusandja tegevuse üleviimisel teise lepinguriiki on eelduslikult kaasatud mõlema lepinguriigi järelevalveasutused, kes võivad portfelli üleviimisele seada lisatingimusi/kõrvaltingimusi, tagamaks kindlustusvõtjate kaitse uues tegevuskohas vähemalt samaväärses ulatuses kui seda oli endises ettevõtte asukohas. Võttes arvesse eeltoodut jääb ebaselgeks lisatava kitsenduse vajalikkus.		
35.	**2) KindlTS § 257[1].** Digitaalse tegevuskerksuse nõuete rikkumine Seadust soovitakse täiendada uue karistusnormiga, mida Finantsinspektsioon saab kohaldada DORA määruses sätestatud nõuete rikkumise korral. Nimelt on DORA määruse artikli 50 lõikes 3 sätestatud, et liikmesriigid kehtestavad õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise. Sama artikli lõikes 4 punktis c on sätestatud, et liikmesriigid annavad pädevatele asutustele õiguse võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist. Eelnõuga nähakse ette, et füüsilise isiku korral on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas ning juriidilise isiku korral karistatakse rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest. Uue planeeritava paragrahvi lõike 1 sõnastuses on viidatud järgmistele DORA määruse nõuete rikkumistele:	Selgitatud	Karistusmäärade kehtestamisel on lähtutud finantssektorile kohalduvatest kehtivatest karistusmääradest ja karistuse määramise alustest, mis nähti ette finantsvaldkonna väärteokaristuse reformiga. Siiski oli eelnõus ekslikult füüsilise isiku karistusmääraks 5 000 000 eurot, kuid see peaks olema 700 000 eurot, et karistus oleks samaväärne §-s 257 sätestatud juhtimissüsteemi nõuete rikkumise määradega ja selle määramise alustega. Finantsvaldkonna väärteokaristuse reformi selgitused on Riigikogu lehelt leitava eelnõu SE111 juures[5]. Näiteks analüüsiti viidatud eelnõu koostamisel, kas kõrgema ülemmääraga rahatrahvide kohaldamine oleks põhjendatud ka KindlTS-s sätestatud kohustuse rikkumise eest, mis otseselt EL õigusaktiga ette ei nähta. Siinkohal kaaluti süüteo tagajärgede tõsidust, mille järgi asuti seisukohale, et teatud juhtudel on klientide huvide kaitse vajadus oluliselt suurem, kui olemasolevast sanktsioonist eeldada võib. Sealjuures võeti arvesse, et karistus oleks võrreldav samaväärse rikkumise eest ette nähtud karistusmääraga teistes finantsvaldkonna õigusaktides. Suur osa EL õigusaktidest näevad ette finantsjärelevalve subjektide tegevusnõete rikkumise eest kuni 5 miljoni euro suuruse rahatrahvi. Seetõttu nähti ka kindlustusandjate suhtes ette kohaldatav rahatrahv samas suurusjärgus.

[5] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/aece8f34-146c-41f6-b3fd-90402dfdd470/audiitortegevuse-seaduse-finantskriisi-ennetamise-ja-lahendamise-seaduse-ning-teiste-seaduste-muutmise-seadus-finantsvaldkonna-vaarteokaristuste-reform-eli-oigusest-tulenevad-karistused

	- art 5–14: IKT- riski juhtimine; -art 16–18, art 19 lõiked 1–5: IKT intsidentide haldamine ja liigitamine ning nendest teavitamine; - art 24, 25, art 27 lõiked 1–8: digitaalse tegevuskerksuse testimine; - art 28 lõiked 1–8, art 29, art 30 lõiked 1–4: kolmandast isikust tuleneva IKT-riski juhtimine; - art 42 lg 3: kolmanda isikuga seotud riskide arvesse võtmine EKsL soovib teada, et miks just selliseid trahvimäärasid peetakse tulemuslikeks, proportsionaalseks ja hoiatavateks? Kuidas suhestuvad antud karistusmäärad Euroopa Liidu teiste liikmesriikide (sh Eesti lähiriikide) poolt rakendatavatesse karistusmääradesse samalaadsete tegude eest ja kuidas on hinnatud vastavate karistusmäärade proportsionaalsust Eesti kindlustusturu mahu suhtes?		Arvestades, et kindlustusandjad töötlevad mh kliendi terviseandmeid, on äärmisel oluline, et nii klientide teabevara kui ka finantsvara on kaitstud ja kindlustusandja järgib selle tagamiseks nõuetekohaselt digitaalse tegevuskerksuse nõudeid. Lisame siia võrdluseks, et isikuandmete kaitse seaduse § 65 kohaselt on isikuandmete töötlemise nõuete rikkumise eest rahatrahv 20 000 000 eurot. Kuna DORA nõuded integreeritakse kehtivatesse liidu õigusaktidesse, võib eeldada, et ka teistes liikmesriikides ette nähtud karistusmäärad on samaväärsed juba kehtivate määradega, mis on ette nähtud juhtimissüsteemi nõuete rikkumise puhul.
EESTI KAUBANDUS-TÖÖSTUSKODA			
36.	Eelnõu § 4 p 10, § 5 p 14, § 7 p 10, § 8 p 19, § 9 p 8, § 10 p 24 kohaselt võib haldustrahv olla summas kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas või kuni kümme protsenti juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest. Füüsilise isiku puhul on võimalik karistada rahatrahviga kuni 5 000 000 eurot või kuni kahekordse väärteo tulemusel teenitud kasule või ära hoitud kahjule vastavas summas. Seega eelnõu koostajad on ette näinud mitmeid alternatiivseid karistusi. Eelnõu ja seletuskirjaga tutvudes ei hakanud silma juhiseid ega kriteeriume, mille alusel järelevalveasutus otsustab, millist karistust määrata. Näiteks jääb ebaselgeks, millal määratakse rahatrahv 5 miljonit eurot ja millal lähtutakse põhimõttest, et haldustrahv võib olla kuni 10 % juriidilise isiku või tema konsolideerimisgrupi konsolideeritud käibest. Leiame, et seletuskirja või eelnõu sätteid tuleks selles osas täiendada, et oleks nii järelevalveasutusele kui ka finantsasutusele selgem, mille alusel otsustab järelevalveasutus, millist trahvi määramise skeemi kasutada. Samuti tekkis meil küsimus, kuidas eeltoodud karistusmäärad suhestuvad Euroopa Liidu teiste liikmesriikidega. Palume seletuskirja selles osas täiendada ja täpsustada, et tekiks võrdlus Eesti ja teiste liikmesriikide karistusmäärade osas.	Selgitatud	Selgitame, et karistusnormide sätestamisel on lähtutud kehtivatest finantssektori karistusmääradest ja karistuste määramise alustest. Finantssektori karistusnormid on suures osas reguleeritud liidu õiguses, kus on ette nähtud analoogsed meetmed (alternatiivid) karistuse rakendamiseks. Eelnõu eesmärk on näha ette ühetaoline lähenemine, sh trahvimäärade osas. Kuna DORA nõuded integreeritakse DORA direktiiviga vastavatesse finantssektori õigusaktidesse, on ka eelnõu puhul tagatud, et DORA nõuete rikkumise eest ette nähtud karistused oleksid kooskõlas vastavates liidu õigusaktides ette nähtud karistussätetega. Näiteks VpTS uue paragrahvi puhul on võetud aluseks direktiivi 2014/65/EL artikli 70 lõike 3 punkti a alapunktid iv, v, xxvii ja xxviii ning lõike 6 punktid f–g. DORA direktiivi kohaselt muudetakse 2014/65/EL direktiivi artikleid 16 ja 17 ning 47 ja 48 nii, et sinna lisatakse viited DORA nõuete rakendamisele. Kuna direktiivi 2014/65/EL artikli 70 lõike 3 punkti a alapunktid viitavad nende artiklite rikkumistele, hõlmab see ühtlasi DORA nõuete rikkumist. KAS uue paragrahvi puhul on võetud aluseks 2013/36/EL direktiivi artikli 67 lõike 1 punkt d ja lõike 2 punktid e–g. DORA direktiivi kohaselt muudetakse 2013/36/EL direktiivi artiklit 74 nii, et sinna lisatakse viide DORA nõuete rakendamisele. Kuna 2013/36/EL direktiivi artikli 66 lõike 1 punkt d viitab artikli 74 rikkumisele, hõlmab see ühtlasi DORA nõuete rikkumist. IFS uue paragrahvi puhul on võetud aluseks 2009/65/EÜ direktiivi artikli 99 lõike 6 punktid e–g ja artikli 99a punkt j. DORA direktiivi kohaselt muudetakse 2009/65/EÜ direktiivi artiklit 12 nii, et sinna lisatakse viide DORA nõuete rakendamisele. Kuna 2009/65/EÜ direktiivi artikli 99a punkt j viitab artikli 12 rikkumisele, hõlmab see ühtlasi DORA nõuete rikkumist.

			Seega on nö alternatiivsed karistused ette nähtud ka EL õiguses. Näiteks võib fikseeritud rahatrahvimäär osutuda vajalikuks olukorras, kus käibepõhiselt arvutatav rahatrahv ei oleks rikkumise iseloomu ja ulatust arvestades proportsionaalne, seda eelkõige juhul, kui subjekt on tegutsenud alla aasta. Kehtiv FIS § 5 sätestab Finantsinspektsiooni tegevuse põhimõtted. Selle lõige 2 näeb ette, et inspektsiooni järelevalvetoimingute sagedus ja rakendatavad meetodid arvestavad finantsjärelevalve subjekti suurust, tegevuse mõju finantssüsteemile ning tegevuse laadi, ulatust ja keerukust, lähtudes proportsionaalsuse põhimõttest. Inspektsioon arvestab karistuse kohaldamisel riskide ja võimaliku rikkumise iseloomu, kestust ja korduvust, järelevalvesubjekti majanduslikku võimekust, tekkinud või tekkida võinud kahjude suurust ning võimalikku mõju finantssüsteemi stabiilsusele. Sisuliselt sätestab antud säte proportsionaalsuse printsiibi, mis on finantsjärelevalves üks peamistest põhimõtetest. Märkuses on esitatud ka küsimus, kuidas karistusmäärad suhestuvad Euroopa Liidu teiste liikmesriikidega. Nagu eespool osutatud, on karistusmäärade aluseks EL õigus, mistõttu võiks eeldada, et trahvimäärad ja nende määramise alused on kooskõlas teiste liikmesriikide karistustega.
37.	Eelnõu § 4 p 7, § 5 p 6, § 7 p 5, § 8 p 16, § 9 p 3, § 10 p 11 ja p 19 tuleneb finantsasutustele kohustus teavitada ühekordse edastamisviisiga nii Finantsinspektsiooni kui ka Riigi Infosüsteemi Ametit (RIA) tõsistest info- ja kommunikatsioonitehnoloogiaga seotud intsidentidest ning soovi korral olulistest küberohtudest kasutades selleks sama teavitusvormi. Eelnõu § 4 p 10, § 5 p 14, § 7 p 10, § 8 p 19, § 9 p 8 ning § 10 p 24 näevad ette, et kui finantsasutus rikub eelnevalt nimetatud kohustust, siis on järelevalveasutusel õigus kohaldada rahatrahvi. Mõistame, et eelnõu ei näe ette finantsasutuste karistamist olukorras, kus finantsasutus ei teavita soovi korral olulistest küberohtudest. Samas seletuskirjas ei ole seda selgelt välja toodud. Seega Kaubanduskoda palub eelnõu koostajatel seletuskirja täiendada selliselt, et finantsasutust ei karistata, kui ta ei täida eelnõu sätestatud võimalust teavitada olulisest küberohust.	Arvestatud	Kinnitame, et eelnõu eesmärk ei ole ette näha karistust olulisest küberohust teavitamise nõuete rikkumise korral, kuivõrd tegemist on ettevõtja valikuvabadusega otsustada, kas ta edastab vastava teavituse FI-le ja RIA-le või mitte. Selguse huvides on eelnõus vastutuse sätteid korrigeeritud ja koosseisudest välja jäetud viide artikli 19 lõikele 2.