Küberturvalisuse seaduse ja teiste
seaduste muutmise seaduse
eelnõu seletuskirja juurde

Lisa 1

MÄRKUSTE TABEL

	I Eesti Infoturbestandardiga seotud muudatused	
Jrk	**Märkuse või ettepaneku sisu**	**Majandus- ja Kommunikatsiooniministeeriumi seisukoht**
	1. Justiitsministeerium kooskõlastab eelnõu järgnevate märkustega.	
1.	Eelnõu seletuskirja 8. osas on märgitud „Uuendatud volitusnorm võimaldaks kehtestada ISKE asemel avalike ülesannete täitmiseks loodud äriprotsessidel (business process) põhineva turvameetmete süsteemi E-ITS. Vastava määruse eelnõu on koostamisel.“ Vabariigi Valitsuse algatatava seaduseelnõu seletuskirjale tuleb olenevalt volitusnormi sisust lisada Vabariigi Valitsuse või ministri määruse eelnõu kavand, mis sisaldab eelnõu esialgset sõnastust. Lisatav määruse eelnõu kavand tuleb ette valmistada sellise täpsusega, et oleks võimalik hinnata rakendusakti vajalikkust, volitusnormi ulatust, kohast tasandit ja muid asjaolusid, mis on vajalikud volitusnormi sõnastuse ja rakendusakti vastavuse hindamiseks (HÕNTE § 48 lg 2).	**Arvestatud**. Rakendusakti kavandid on eelnõule lisatud.
2.	Eelnõu seletuskirjas tuleb märkida, kui palju E-ITS ulatus laieneb võrreldes tänase andmekogude põhise lähenemisega. Uue infoturbe standardi kasutusele võtmine tähendab kõikide infosüsteemide turvameetmete ülevaatamist ja uute nõuete rakendamist. Eelnõu seletuskirjast peavad nähtuma selleks vajalike vahendite allikas, samuti ajaraam ning tagada tuleb ka koordineerimine.	**Arvestatud**. Seletuskirja on täiendatud.
3.	Kuna eelnõu seletuskirjas tuuakse oodatava mõjuna ära asjaolu, et edaspidi rakendaksid nii riigi kui omavalitsusasutused vajalikul tasemel infoturbemeetmeid, siis tuleks seletuskirja lisada hinnang, kas ja kuivõrd oleks sellest mõjutatud asutuste töökoormus ehk teisisõnu, kas uuenenud olukorras infoturbemeetmete rakendamine võiks osadel asutustel varasemaga võrreldes rohkem aega võtta või nõuaks neilt lisaressursse (viimasel juhul vt ka	**Arvestatud**. Seletuskirja on täiendatud.

	seletuskirja 7. osa) nt kasvõi koolitusvajaduse näol.	
4.	Palume täpsustada ettevõtjate ja kodanike halduskoormusele antud hinnangut, kuna praegu seisab seletuskirjas väide, et olulist mõju sellele ei ole. Hinnangu aluseks tuleb võtta aga asjaolu, kas halduskoormus nimetatud sihtrühmadele muudatuste järgselt võiks eelduslikult kasvada, kahaneda või jääb see üldjoontes samaks. Palume selle juurde lisada ka lühike selgitus.	**Arvestatud**. Seletuskirja on täiendatud.
5.	Juhime tähelepanu, et seletuskirja 7. osas peaks käsitlema ka rakendamisega seotud tulusid, kuid hetkel selline info seletuskirja sellest osast puudub. Viiteid muudatustest tulenevatele võimalikele tuludele leiab seletuskirjast punktist 6, kus on juttu võimalikust e-riigi lahenduste ekspordist. Palume tuludega seonduvat seletuskirja punktis 7 võimalusel vastavalt täiendada.	**Arvestatud**. Seletuskirja on muudetud.
6.	Kehtiv KüTS § 2 punkt 1 võimaldab defineerida infosüsteemi väga meelevaldselt. Infosüsteemiks võib lugeda näiteks ühte arvutit või kogu võrku koos kõigi oma komponentidega. Teeme ettepaneku analüüsida ja muuta KüTSi vastavalt. Selgus on oluline arusaamaks, kuidas edaspidiselt rakendada täna KüTS §-s 7 kajastatud riskianalüüsi läbiviimise nõuet, kui vastav kohustus jääb kehtima E-ITSi loomisel. Kui jääb, on see liigne halduskoormus, kuna uus E-ITS standardi või ISO rakendamine juba eeldab vastava standardipõhist riskide hindamist.	**Mittearvestatud**. Tegemist on Euroopa Parlamendi ja nõukogu direktiivi (EL) nr 2016/1148 (nn NIS 1 direktiiv) artikli 2 punktist 1 tuleneva mõiste siseriikliku defineerimisega. KüTS-s olev termin on sellega kooskõlas. Hetkel on käimas ka nimetatud direktiivi uuendamine ehk tulemas on NIS 2 direktiiv, mis tunnistab NIS 1 direktiivi kehtetuks. NIS 2 direktiivi sõnastuse esmane ettepanek avaldati detsembris 2020. a, kuid selle termini sõnastus on sarnane NIS 1 direktiivi terminile. KüTS §-s 7 oleva riskianalüüsi säte tunnistatakse kehtetuks.
7.	Eelnõu § 1 p 1 (KüTS § 9 lg 2) – palume kaaluda kompaktsemat ja vähem liiast süsteemi nimetust (praeguses on kaks korda info ja kaks korda süsteem): võrgu- ja infosüsteemide infoturbe haldussüsteemi asemel võrgu- ja infosüsteemide turbesüsteem. Seda asendust soovitame vaid juhul, kui lühemast nimetusest midagi olulist välja pole jäänud.	**Arvestatud.** KüTS § 9 tunnistatakse kehtetuks.
8.	Eelnõu § 2 p 3 muutmisvormel – *teist lauset* asemel peab olema *teine lause*.	**Arvestatud**. Eelnõud muudetud.
9.	Eelnõu § 2 p 3 (AvTS § 43^9 lg 1^1) – kui KüTS § 9 lõike 2 alusel kehtestatud määruse nõudeid tuleb täita, mistõttu on eelnõu § 2 punktis 5 ette nähtud ka RIA poolt tehtav haldus- ja riiklik	**Arvestatud osaliselt** Eelnõu sõnastust muudeti nii, et E-ITS-i nõuded ja selle järelevalve on sätestatud KüTS-s. Samuti

	järelevalve, siis peab see ka normi sõnastusest nähtuma: (1^1) Andmekogude turvalisuse kindlustamisele kohaldatakse küberturvalisuse seaduse § 9 lõike 2 alusel kehtestatud nõudeid.	toodi KüTS-i teenuse osutajate hulka ka andmekogude vastutavad ja volitatud töötlejad.
10.	Tõstatame küsimuse, kas loodav standard on kooskõlas riigi teiste teenus- ja protsessipõhiste juhtimise suunitlustega nagu TKTA määrus, https://www.riigiteataja.ee/akt/131052017007 ja tegevuspõhine riigieelarve (TERE), https://www.rahandusministeerium.ee/et/riigieelarve-jamajandus/tegevuspohine-riigieelarve. Kasutatavad terminid peavad olema läbivalt samased selleks, et tagada asutustes ühtne määruste rakendamine ning selleks, et ära hoida korduvate tegevuste tegemine nt protsesside kaardistamine. Eeltoodust lähtuvalt ka küsimus, kas äriprotsessi termin on E-ITS-s, TERE-s ja TKTA määruses samasisulised. Palume seletuskirja täpsustada.	**Arvestatud**. Eelnõus ei kasutata äriprotsessi terminit.
11.	Seletuskirja alaosas 1.3. on märgitud, et „Eelnõu vajab seadusena Riigikogu vastuvõtmiseks koosseisu häälteenamust“. PS § 104 sätestab seadused, mida saab vastu võtta ja muuta ainult Riigikogu koosseisu häälteenamusega. Vastavalt HÕNTE § 41 lõike 4 punkti 5 kohaselt peab kvalifitseeritud häälteenamuse puhul olema lisatud ka selle põhjendus, seletuskirja tuleb kas parandada või esitada põhjendus kvalifitseeritud häälteenamuse kohaldamiseks.	**Arvestatud**. Seletuskirja on täiendatud.
12.	Seletuskirja 2. osa „Seaduse eesmärk“ peab sisaldama ka viidet HÕNTE-le (HÕNTE § 42 lg 2) tuues lühidalt välja väljatöötamiskavatsuse puudumise põhjuse ja selle aluseks oleva konkreetse erandi, milleks eelduslikult on HÕNTE § 1 lg 2 p 5.	**Arvestatud**. Seletuskirja on täiendatud.
13.	Eelnõu seletuskirja 5. osas on märgitud *„Võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge taseme tagamiseks kehtestatud Euroopa parlamendi ja nõukogu direktiiv 2016/1148 (NIS direktiiv) reguleerib üksnes ühiskondlikult oluliste teenuste operaatoreid, kuid mitte avalikku sektorit“ – kuivõrd kõnealuse direktiivi artikkel 4 punkt 4 sätestab „4) „oluliste teenuste operaator“– II lisas osutatud liiki avaliku või erasektori üksus, mis vastab artikli 5 lõikes 2 sätestatud kriteeriumidele;“*, siis tuleb seletuskirja	**Arvestatud**. Seletuskirja on muudetud.

	täpsustada, et esitatud väide oleks direktiiviga kooskõlas. Juhime tähelepanu ka HOS 5. peatükile, mis sätestab elutähtsate teenuste toimepidevuse korralduse ning sätestab ülesanded ministeeriumidele. Palume eelnõu seletuskirja täpsustada.	
14.	Eelnõu seletuskirja 8. osa – eelnõu seletuskirja 4. osas on märgitud järgmist: „Senise „infosüsteemide turvameetmete süsteemi“ asemel kasutatakse uuendatud terminit „võrgu- ja infosüsteemide infoturbe haldussüsteem“.“, lisaks tunnistatakse eelnõu § 2 punktiga 1 kehtetuks AvTS § 43^9 lõike 1 punktiga 4 kehtestatud volitusnorm, mille alusel kehtestatud määruses kasutatakse ka „infosüsteemide turvameetmete süsteem“, millele viidatakse loetelus toodud määrustes. Sellest tulenevalt tuleb terminimuudatused ette näha ka järgmistes määrustes ning esitada teave nende muutmise kohta eelnõu seletuskirja 8. osas: - Majandus- ja taristuministri 12.03.2015. a määrus nr 21 „Nutika teenuste taristu arendamise toetamise tingimused ja investeeringute kava koostamise kord“; - Majandus- ja taristuministri 15.04.2015. a määrus nr 31 „Avalike teenuste pakkumise arendamiseks toetuse andmise tingimused ja kord“; - Vabariigi Valitsuse 31.07.2014. a määrus nr 121 „Struktuuritoetuste registri pidamise põhimäärus“; - Vabariigi Valitsuse 15.03.2012. a määrus nr 26 „Infoturbe juhtimise süsteem“; - Vabariigi Valitsuse 22.12.2011. a määrus nr 181 „Arhiivieeskiri“. Kuivõrd eelnõuga tunnistatakse kehtetuks AvTS § 43^9 lõike 1 punkt 4, mille alusel on kehtestatud Vabariigi Valitsuse 20.12.2007. a määrus nr 252 „Infosüsteemide turvameetmete süsteem“, tuleb seletuskirja 8. osas esitada kõnealuse määruse Riigi Teataja link (HÕNTE § 48 lg 3 p 3).	**Arvestatud**. Seletuskirja on täiendatud ning määruste kavandid on eelnõule lisatud.
15.	Eelnõu seletuskirja 9. osas tuleb põhjendada jõustumisaja, sh üldkorras jõustumise, valikut (HÕNTE § 49). Kuivõrd asendatakse aegunud kolmeastmeline etalonturbesüsteem (ISKE) turvameetmete süsteem uue infoturbestandardiga (E-ITS) ehk süsteem	**Arvestatud**. Seletuskirja on täiendatud.

	vahetub, rakendusakt peab jõustuma samaaegselt seadusemuudatusega, muudatuse adressaatidel peab olema piisav aeg muudatuste rakendamiseks, nendega tutvumiseks, mistõttu on uue süsteemi edukaks rakendamises vajalik vacatio legis, mida näeb ette ka HÕNTE § 14 (vt normitehnika käsiraamatu § 14 kommentaar 3), siis teeb Justiitsministeerium ettepaneku esitada eelnõus jõustumisaeg konkreetse kuupäevana, mis arvestab ka vacatio legis`t.	
	2. Kaitseministeerium kooskõlastab eelnõu järgnevate märkustega	
16.	Palume muuta KüTS § 9 lõiget 3 ja sõnastada järgmiselt: „(3) Rahvusvaheliseks sõjaliseks koostööks ning riigi sõjalise kaitse planeerimiseks vajalike süsteemide loetelu ja nende turvameetmete kirjelduse kehtestab valdkonna eest vastutav minister määrusega.“.	**Arvestatud osaliselt.** KüTS § 9 tunnistatakse kehtetuks, kuid KüTS-i luuakse eraldi volitusnorm (KüTS § 7 lg 5) Vabariigi Valitsusele süsteemidele kohalduvate nõuete kehtestamiseks. Vabariigi Valitsusele antakse KüTS-s ka volitus enda määrusega volitada valdkonna eest vastutavat ministrit kehtestama teatavaid nõudeid, mille hulgas on ka võimalus kaitseministril kehtestada Kaitseministeeriumi valitsemisala suhtes erinõudeid.
17.	Palume täiendada KüTS § 14 lõiget 3 pärast sõna „teevad“ sõnadega „riiklikku ja“	**Arvestatud osaliselt.** KüTS § 9 tunnistatakse kehtetuks, mõistõttu KüTS § 14 lg 3 sõnastus muudetakse vastavalt Kaitseministeeriumi välja pakutud sõnastusele.
	3. Siseministeerium kooskõlastab eelnõu	
18.	Siseministeerium kooskõlastab küberturvalisuse ja avaliku teabe seaduseseaduse muudatuse ning toetab uue standardi E-ITS volitusnormi liikumist küberturvalisuse seaduse alla.	**Teadmiseks võetud.**
	4. Välisministeerium kooskõlastab eelnõu vaikimisi	
	5. Eesti Linnade ja Valdade Liit kooskõlastab eelnõu järgnevate märkustega	
19.	Peame aga vajalikuks juhtida tähelepanu sellele, et seletuskirja punkt 7 (lk 6) kohaselt ei kaasne seaduse rakendamisega täiendavaid kulusid kohalikule omavalitsusele. Teisalt seletuskirja samal lehel (lk 6) tunnistatakse, et praktika on näidanud, et ilma kohustava normita ei rakenda asutused vajalikul tasemel infoturbemeetmeid. Samuti on väljendatud mõtet, et uus standard võib turgutada majandussektorit, mis aitab standardeid rakendada ja jälgida (nt tööriistade loomine, turunõudlus täiendavate audiitorite	**Arvestatud**. Seletuskirja on täiendatud.

	järele ja muu majandust elavdav). Sellest tulenevalt võib siiski ilmneda, et rahaliselt kaasneb täiendav kulu kohalikele omavalitusele. Arvestades ülaltoodut, palume täiendada seletuskirja punkti 7 seaduse rakendamisega seotud kohaliku omavalitsuse tegevuste detailsema kirjeldamisega ning eeldatavate kulude prognoosimisega koos kulutuste katteallika kavandamisega või põhjalikuma selgitusega kulude mittekaasnemise kohta.	
	6. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit esitas ettepanekud	
	Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) on eelnõud analüüsinud ja annab käesolevaga teada, et toetab eelnõuga tehtavat muudatust, millega kaasajastatakse ning viiakse infoturbe tagamine andmekogude põhiselt lähenemiselt üle võrgu- ja infosüsteemide põhisele lähenemisele. ITL toetab aegunud kolmeastmelise etalonturbesüsteemi (ISKE) turvameetmete süsteemi asendamist uue väljatöötamisel oleva Eesti infoturbestandardiga. Palume meid kaasata uue võrgu- ja infosüsteemide infoturbe haldussüsteemi määruse eelnõu menetlusse.	**Teadmiseks võetud.**
20	ITS Estonia ehk Eesti IKT Klastri poolt koordineeritava transpordi innovatsiooni koostöövõrgustiku esindajad juhtisid tähelepanu sellele, et ei ole kõige parem lahendus, kui Eesti infoturbestandardi lühendiks saab E-ITS. Nende hinnangul hakkab see tekitama segadust ja segiajamist ITS (ehk Intelligent Transport System) Estonia võrgustiku nimega. Seetõttu palume teil võimalusel leida uuele infoturbestandardile teine lühend. Kui midagi muud ei ole võimalik välja mõelda, siis abiks oleks ka see, kui lühend on EITS ehk ilma sidekriipsuta.	**Teadmiseks võetud ning selgitame**, et hetkel on planeeritud kasutada lühendit E-ITS.
	II Küberturvalisuse määrusega (EL määrus nr nr 2019/881) seotud muudatused	
	1. Justiitsministeerium kooskõlastab eelnõu järgmiste märkustega	
1	Eelnõu p 5 (uuendatud eelnõu § 1 punkt 15) - seletuskirja kohaselt arvestati sunniraha suuruse ülemmäära (100 000 eurot) määratlemisel Tarbijakaitse ja Tehnilise Järelevalve Ameti (edaspidi *TTJA*) antud tagasiside, mille kohaselt oleks eelnevalt mainitud ülemmäär piisav, mis vajadusel	**Eelnõud ja seletuskirja on muudetud ning anname selgituse.** Algselt kavatseti eelnõug määratleda ainult TTJA-le kohalduv sunniraha ülemmäär KüTS-s ning teiste KüTS-i alusel järelevalvet teostajate (eelnõu järgselt RIA ning Kaitseministeerium) korral tuleneksid sunniraha ülemmäärad Vabariigi Valitsuse seadusest (sama

	motiveeriks vastavushindamisasutust, Euroopa küberturvalisuse sertifikaadi omanikku ja ELi vastavusdeklaratsiooni väljaandjat lähtuma küberturvalisuse määruse ja tulevikus konkreetse valdkonna osas vastu võetava Euroopa küberturvalisuse sertifitseerimise kava nõuete kohaselt. Sunniraha ülemmäär võimaldab TTJA-l efektiivselt sekkuda küberturvalisuse sertifitseerimisega seotud nõuete rikkumisel. Näiteks, kui eesmärk on ettekirjutusega nõuda küberturvalisuse määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist ning selle nõude täitmise tagamiseks tehakse samas ettekirjutuses ka sunniraha määramise hoiatus – kui ettekirjutust kohaselt ei täideta, siis kohaldatakse sunniraha. Kehtiva KüTS § 14 lõike 1 kohaselt teostab KüTS-is ja selle alusel kehtestatud õigusaktides sätestatud nõuete täitmise üle riiklikku ja haldusjärelevalvet Riigi Infosüsteemi Amet, lõike 3 kohaselt KüTS § 9 lõike 3 alusel kehtestatud määruses sätestatud süsteemide nõuete täitmise üle Kaitseministeerium ja Kaitsevägi. Palume seletuskirjas selgitada, kas Riigi Infosüsteemide Amet, Kaitseministeerium ning Kaitsevägi ei koosta KüTS-i nõuete täitmise tagamiseks ettekirjutusi ning ei rakenda sunniraha? Kas praktikast ei tulene vajadust ka neile anda võimalus sunniraha kohaldamiseks.	seaduse § 75^1 lõike 4 tingimuste täitmise korral) ning korrakaitseseadusest (sama seaduse § 23 lõike 3 ja/või § 28 tingimuste täitmise korral). Tagasiside tulemusena on kõigi nimetatud asutuste määratavate sunniraha ülemmäär sama.
2	Eelnõu p 6 (uuendatud eelnõu § 1 punkt 16) − Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 53 lõikes 2 on sätestatud, et IKT-toodete, -teenuste või -protsesside tootja või pakkuja võib anda välja ELi vastavusdeklaratsiooni, milles kinnitatakse, et kavas esitatud nõuded on täidetud. ELi vastavusdeklaratsiooni väljaandmisega võtab IKT-toodete, -teenuste või -protsesside tootja või pakkuja vastutuse IKT-toote, -teenuse või -protsessi vastavuse eest kõnealuses kavas sätestatud nõuetele. Palume seletuskirjas selgitada, milliste kava nõuetega on tegemist, sh tuua näiteid. Kuigi norm näeb ette vastutuse tingimustele mittevastava vastavusdeklaratsiooni väljaandmise eest, siis määruse artikli 53 lõikes 2 ei ole neid tingimusi esitatud.	**Seletuskirja on täiendatud.**

	Räägitakse üksnes kinnitusest, et kavas esitatud nõuded on täidetud. Palume täpsustada, kus need konkreetsed nõuded sätestatud on, mille järgimata jätmise eest saab vastutusele võtta.	
3	Kehtivad vastutussätted − kehtivas seaduses ei ole juriidilisele isikule haldusmenetluses kohaldatava sunniraha ülemmäära kehtestatud, kehtiva KüTS § 18 kohaselt aga on võimalik juriidilist isikut väärteo eest karistada kuni 20 000 euro suuruse rahatrahviga. Kui nüüd soovitakse eelnõuga ette näha järelevalve raames rakendatava sunniraha ülemmäärana 100 000 eurot, siis ei ole kuidagi õigustatud, et väärteo puhul jääb maksimaalseks karistuseks juriidilisele isikule kuni 20 000 eurot. Karistused peavad oma proportsioonilt ja mõjususelt olema karmimad kui haldusmenetluse raames kohaldatav sunnimeede. Seega eelnõuga lisanduvas §-s 18[1] kavandatavat, samuti kehtiva seaduse §-s 18 olevat juriidilise isiku karistusmäära kuni 20 000 eurot tuleb Justiitsministeeriumi arvates muuta, kui sunniraha suurusena kavandatakse sätestada 100 000 eurot. Juhime siinkohal tähelepanu sellele, et füüsilise isiku karistusmäär on KüTS-is kehtestatud kuni 200 trahviühikut, mis on maksimaalselt lubatud karistusmäärast (kuni 300 trahviühikut) vaid 100 trahviühikut madalam. Seda lähenemist ei ole aga järgitud juriidilise isiku osas. Kui füüsilise isiku keelatud tegevus on võimaliku rahatrahvimäära järgi võrdlemisi tõsiselt karistatav, siis juriidilise isiku karistus jääb sellest väga kaugele. Seletuskirjas tuuakse välja, et liikmesriigile on küberturvalisuse määruse 3. jaotises (küberturvalisuse sertifitseerimise raamistik) antud kohustus kehtestada küberturvalisuse sertifitseerimise raamistiku ja Euroopa küberturvalisuse sertifitseerimise kavade rikkumise korral kohaldatavad karistusnormid ning võtta kõik vajalikud meetmed nende rakendamise tagamiseks. *Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad.* Samas märgitakse ka seda, et tulevikus on võimalik hinnata, kas KüTS §-s 18 ning	**Anname selgituse.** Eelnõuga lisanduva KüTS §-i 18[1] sisustamisel võeti eeskuju KüTS §-st 18 ning esialgu on soov määratleda kavandatavate süüteokoosseisude rikkumistega seotud rahatrahvide suurused võrreldavaks hetkel KüTS-s olevate rahatrahvidega. Kuna eelnõu sisaldab lisaks küberturvalisuse määruse siseriikliku rakendamisega ka muid muudatusi, mis tehakse KüTS-s, siis eelnõu käesolevas staadiumis ei ole võimalik täiendavalt analüüsida KüTS-i olemasolevate ja lisanduvate süüteokoosseisude suuruste sobivust Eesti karistusõiguse süsteemi. Seda on võimalik teostada KüTS-i revisjoni (alustatakse 2021. a II poolaastal) käigus. Lisaks sellele tuleb siin ka arvestada, et NIS 2 direktiivi ettepanekus on rahatrahvide suurused märgatavalt tõusnud – direktiivi ettepaneku kohaselt tuleb teatud isikutele määrata NIS 2 direktiivi nõuete rikkumise korral määrata haldustrahv, mille maksimummäär on „vähemalt 10 000 000 eurot või kuni 2 % (olenevalt sellest, kumb summa on suurem) selle ettevõtja ülemaailmsest aastasest kogukäibest, kellele oluline üksus eelneval majandusaastal kuulub” (vt ettepaneku[1] artikkel 31 lõiget 4). Seetõttu on sobilikum teostada KüTS-s olevate süüteokoosseisude eest ette nähtavate väärteokaristuste määrade üle vaatamine, kas KüTS-i revisjoni või NIS 2 direktiivi üle võtmise käigus. Nimetatud muudatuste tegemine oleks ka seotud Eesti õigusesse haldustrahvi instituudi loomisega.

[1] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020PC0823.

	eelnõuga lisanduva § 18[1] väärteokoosseisude rahatrahvide suurusi tuleks suurendada. Seda on võimalik teha uue küberturvalisuse direktiivi üle võtmise käigus (nn NIS 2 direktiiv; hetkel ettepaneku staatuses). Kui küberturvalisuse määrus tegelikult nõuab, et karistused oleksid tõhusad, proportsionaalsed ja hoiatavad, siis oleme arvamusel, et reguleeritavas valdkonnas kavandatav juriidilise isiku karistusmäär kuni 20 000 eurot ei ole tõhus ja proportsionaalne. Eriti arvestades asjaolu, et sunniraha soovitakse suuruses kuni 100 000 eurot. Selle määra puhul on eesmärgiks, et ülemmäär vajadusel motiveeriks vastavushindamisasutust, Euroopa küberturvalisuse sertifikaadi omanikku ja ELi vastavusdeklaratsiooni väljaandjat lähtuma küberturvalisuse määruse ja tulevikus konkreetse valdkonna osas vastu võetava Euroopa küberturvalisuse sertifitseerimise kava nõuete kohaselt. Kuna tõenäoliselt kooskõlastamiseks esitatud eelnõu menetlemine saab toimuma Riigikogus alles alates septembrist, siis oleme arvamusel, et vahepealne aeg on piisav, analüüsimaks veelkord, kas juriidilise isiku karistusmäär kuni 20 000 eurot vastab liikmesriikidele esitatud nõuetele. Väga positiivne ja tervitatav on see, et seletuskiri sisaldab näiteid ka teistest riikide karistusmääradest (Poola: 230 000 eurot; Slovakkia 300 000 eurot). Siit on näha, et mujal suhtutakse karistusmäära märksa tõsisemalt kui hetkel Eestis kavandatakse.	
4	Eelnõu p 4 (uuendatud eelnõu § 1 punkt 14) – kui kehtiva seaduse § 16 lõiked 2 ja 3 kehtivad ka TTJA poolt määruses sätestatud meetmete kohta – st nendest peab teavitama esimesel võimalusel ja need peab protokollima, siis on parem koht kavandatavaks uueks sätteks lõike 2[1] asemel lõige 1[1]. Palume arvestada ka kooskõlastava kirja lisas esitatud eelnõu ja seletuskirja kohta tehtud normitehniliste ja keelemärkustega ning märkustega eelnõu mõjude kohta.	**Arvestatud.** Eelnõu § 1 punkti 14 (KüTS § 16 täiendamine lõikega 1[1]) sõnastust on vastavalt muudetud. Samuti arvestatakse eelnõu ja seletuskirja kohta tehtud märkustega.
	2. Rahandusministeerium kooskõlastab eelnõu järgmiste märkustega	
5	Seletuskirjast ei selgu üheselt, kas ja kui palju lisapersonali RIA muudatuse elluviimiseks vajab ja kas võimalikud tekkivad lisakulud (sh	**Arvestatud**. Seletuskirja on täiendatud.

	teenistujate kompetentsi tõstmise kulud) suudetakse katta olemasolevate vahendite arvelt. Kuivõrd seletuskirjas on märgitud, et võimalikud kulud tulenevad otseselt küberturvalisuse määrusest, siis eeldatavalt on need siiski teada.	
6	Seletuskirja punktis 2 on märgitud, et EL küberturvalisuse sertifitseerimise raamistiku üheks eesmärgiks on aidata vältida üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifitseerimise kavade paljusust. Seeläbi peaks vähendatama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid. Seletuskirja mõjude osas ei ole seda osa siiski kajastatud. Oleks asjakohane tuua mõjudes lisaks näiteid, milliseid teenuseid see eelkõige puudutama hakkab või mis kulusid see kokku hoida aitab.	**Arvestatud**. Seletuskirja on täiendatud.
	3. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit esitas	
7	Oleme seisukohal, et eelnõu ja seletuskiri peaksid käsitlema üksnes Euroopa Parlamendi ja nõukogu määruse (EL) nr 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 tuleneva kohustusliku osa rakendamist ehk siis riikliku küberturvalisuse sertifitseerimise asutuse ja vastavate karistusnormide määramisega. Teatud ajaperioodi möödudes, kui Eestis on välja kujunenud sertifikaati vajavate toodete (IKT lahenduste) turg, saab kaaluda edasisi samme sertifitseerimise mudeli edasi arendamiseks.	**Võtame teadmiseks**
8	Toetame ettepanekut määrata riiklikuks infopunktiks ehk Euroopa Parlamendi ja nõukogu määruse (EL) nr 2019/881 mõistes riiklikuks sertifitseerimise asutuseks Tarbijakaitse ja Tehnilise Järelevalve Amet. Sellega oleks täidetud määrusest tuleneva kohustuse täitmine. Samuti on ettevõtjatel vajadus asutuse järgi, kes aitaks neid nõustada olukorras, kui sertifikaati on vaja (nt teise riigi riigihankes osalemiseks).	**Võtame teadmiseks**
9	Soovitame teha teiste liikmesriikidega rohkem koostööd. Vastavushindamine on väga kallis protseduur ning arusaadavatel põhjustel ei jaksa väikeriigid seda ise teha. Seetõttu on ettevõtjatel ootus, et riik töötaks välja	**Võtame teadmiseks.** Kuigi eelnõu ja seletuskirja koostamise käigus ei uuritud teistelt riikidelt nende valmisolekut ja võimekust vastavushindamise läbi viimiseks, siis

	koostöömudeli, kuidas ettevõtted saaksid teistes riikides vajaliku sertifitseerimist teha ja tekiks arusaam, mis vormis ja kuidas vastavushindamine päriselt tööle hakkab. Üheks võimaluseks on luua näiteks koos naaberriikidega ühine akrediteerimiskeskus.	tulevikus võib analüüsida, milliste riikidega sel teemal koostööd teha. Ennekõike siis, kui hakkab selguma, milliseid Euroopa Liidu üleseid sertifitseerimiskavu koostatakse ning vastu võetakse.
10	Me ei pea otstarbekaks lähtuda eelnõu seletuskirjas kirjeldatud mudelist mille kohaselt määrataks Eesti Standardimis-ja Akrediteerimiskeskus riiklikuks akrediteerimiskeskuseks, kuna neil puudub (täna ja ilmselt ka tulevikus) pädevus seda tööd sisuliselt teha. Selle pädevuse loomine oleks aga väga kallis ja põhjendamatu olukorras, kus me ei tea, kas Eestis oleks üldse piisavas mahus seda teenust vaja. Seega nad täidaksid sisuliselt vaid infopunkti rolli andes aga teistele riikidele ja ettevõtetele (nii Eestis kui välismaal) vale signaali nagu meil oleks olemas sisulist tööd tegev akrediteerimiskeskus. Pole tehtud uuringut, kui palju Eesti ettevõtjaid tahaksid saada erasektori vastavushindamise asutuseks ja kui palju on tooteid, mida oleks vaja sertifitseerida.	**Võtame teadmiseks.** Euroopa Parlamendi ja nõukogu määruse (EL) nr 2019/881 artikli 60 lõike 1 kohaselt akrediteerivad vastavushindamisasutusi määruse (EÜ) nr 765/2008 kohaselt nimetatud riiklikud akrediteerimisasutused. Määruse nr 2019/881 artikli 2 punkti 16 kohaselt on „riiklik akrediteerimisasutus“ määruse (EÜ) nr 765/2008 artikli 2 punktis 11 määratletud riiklik akrediteerimisasutus. Eestis on riiklik akrediteerimisasutuse ülesandeid täitev isik määratletud toote nõuetele vastavuse seaduse § 37 alusel. Seda ülesannet teostab Eesti Standardimis- ja Akrediteerimiskeskus, konkreetsemalt selle struktuuriüksus Eesti Akrediteerimiskeskus.
11	Me ei pea otstarbekaks lähtuda eelnõu seletuskirjas kirjeldatud mudelist mille kohaselt planeeritakse Riigi Infosüsteemi Ametile küberturvalisuse sertifitseerimise raames ülesannete (riiklik vastavushindamisasutus) panemist olukorras, kus nende ülesannete täpne sisu ei ole veel teada. Nende ülesannete panek oleks riigile vaid kulu, seda millist lisandväärtust see Eesti majandusele annaks, ei ole teada.	**Võtame teadmiseks.** Selgitame, et Riigi Infosüsteemi Amet saab riikliku vastavushindamisasutuse ülesanded siis, kui ta vastava akrediteeringu läbib – õigusaktis ei ole võimalik määratleda, et ta täidab neid ülesandeid. Samuti võidakse Euroopa küberturvalisuse sertifitseerimise kavades ette näha, et nimetatud kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avaliku sektori asutus (vt määruse nr 2019/881 artikli 56 lõiget 5) ning selleks saab olla kas riiklik küberturvalisuse sertifitseerimise asutus või vastavushindamisasutusena akrediteeritud avaliku sektori asutus. Kuna nende kahe asutuse tegevused peavad olema üksteisest sõltumatud ja lahus (vt määruse nr 2019/881 artikli 58 lõiget 3), siis eelnõu koostamisel jõuti järeldusele, et riikliku vastavushindamisasutuse ülesanded ei saa olla Tarbijakaitse ja Tehnilise Järelevalve Ametis.
	4. Eesti Standardimis- ja Akrediteerimiskeskus esitas ettepanekud	
12	**Ettepanek**: eelnõus tuleks selgelt väljendada, et akrediteerimisasutus saab olla kas toote	**Arvestatud**. Nimetatud muudatust eelnõusse ei lisatud, kuna sisuliselt sama nõue on

	nõuetele vastavuse seaduse 4. peatükis nimetatud riiklik akrediteerimisasutus (Eesti Standardimis- ja Akrediteerimiskeskus, konkreetsemalt selle struktuuriüksus Eesti Akrediteerimiskeskus ehk EAK) või mõni muu akrediteerimisasutus, kes vastab määruse (EÜ) nr 765/2008 II peatükis sätestatule (ehk mõne teise liikmesriigi riiklik akrediteerimisasutus). Praegusel sõnastuse kujul ei ole päris üheselt selge, et saab aktsepteerida ka mõne muu riigi akrediteerimisasutust. EAK-l puudub paraku igasugune kompetents ja võimekus küberturvalisuse valdkonnas vastavushindamisasutusi akrediteerida, mistõttu potentsiaalsetel akrediteerimisest huvitatutel peab olema võimalus pöörduda mõne muu riigi akrediteerimisasutuse poole, kes küberturvalisuse valdkonnas akrediteerimisteenust pakub. Riiklik akrediteerimisasutus otsustab ise, milliseid tehnilisi valdkondi ta akrediteerib ja milliseid mitte ning see sõltub erinevatest asjaoludest nagu seletuskirjas on välja toodud. Tänase EAK võimekuse juures me oma tegevust küberturvalisuse valdkonda laiendama ei ole võimelised.	küberturvalisuse määruses (vt määruse nr 2019/881 artikli 60 lõiget 1), mistõttu seda ei hakatud üle kordama. Lisasime EAK tagasiside seletuskirja, sh seletuskirja on lisatud ka selgitus, et EAK asemel võib vastavat ülesannet täita ka muu riigi riiklik akrediteerimisasutus, mis vastab määruse nr 765/2008 nõuetele.
13	Seletuskirjas märkasime akrediteerimise kohta mitmed faktivigu. Koheselt hakkas silma, et lk 7 on esitatud standardimisasutuse logo, kuid antud kontekstis peaks see olema ikkagi EAK logo. Edastasime kirjale EAK logo. Lk 8 esimeses lõigus on info EAK ja EVS ühinemise kohta ebatäpne - korrektne oleks "SA Eesti Akrediteerimiskeskus andis oma tegevuse üle MTÜ-le Eesti Standardimiskeskus, mis vahetas 2020. aasta lõpus oma nime. Akrediteerimisteenust osutab selle MTÜ eraldi struktuuriüksus EAK.")	**Arvestatud**. Seletuskirja on parandatud.