Märkuste tabel

Nr	Märkus	Märkusega arvestamine
	1. Haridus- ja Teadusministeerium kooskõlastab märkusteta 10.02.2025 kiri nr 8-3/24/5450-2	
	2. Kaitseministeerium kooskõlastab märkustega 19.02.2025 kiri nr 5-7/24/173-4	
2.1	Planeeritava [KüTS] § 2 punkti 3^3 kohaselt on risk küberintsidendist tingitud kahju või häire võimekus, mida tuleb väljendada sellise kahju või katkestuse ulatust ja kõnealuse küberintsidendi esinemise võimalikkust arvesse võtva kombineeritud näitajana. Juhime tähelepanu, et kahju või häire ei saa olla võimekus. Palume asendada sõna „võimekus“ sõnaga „võimalus“. Lisaks on definitsioon sarnane NIS2 direktiivis tooduga, kuid osa sõnu on erinevad. Kuigi erinevad sõnad ei ole otseselt väärad, palume mitmetimõistetavuse vältimiseks kaaluda võimalikult suures osas direktiivi sõnastuse kasutamist.	Arvestatud
2.2	Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikkel 14 kohaselt luuakse koostöörühm, et toetada ja hõlbustada strateegilist	Võetud teadmiseks

	koostööd ja teabevahetust liikmesriikide vahel. Planeeritava [KüTS] § 5 lõike 2 kohaselt osalevad Justiits- ja Digiministeerium ning Riigi Infosüsteemi Amet koostöörühma tegevustes vastavalt koostöörühma ülesannetele. Koostöörühma ülesanne on tegeleda muuhulgas tarneahelakindluse, seonduvate õigusaktide, küberturvalisuse poliitikate, nõrkuste koordineeritud avaldamise ja teiste sarnaste tegevustega. Selleks, et omada loetletud ülesannete täitmisel terviklikku ohupilti, on Justiits- ja Digiministeeriumil ning Riigi Infosüsteemi Ametil vaja sisendit julgeolekuasutustelt. Vajadus julgeolekuasutuste kaasamise järele tuleneb ka „Küberturvalisuse strateegia 2024-2030“ rakenduskavast, kus muude tegevuste hulgas on välja toodud ootus, et elutähtsad taristu ja teenused on varustatud riikliku julgeoleku aspektist lähtuvate turvameetmetega, mis võimaldavad vastu seista nii praegustele kui ka tulevastele ohtudele. Palume luua koostöömehhanism, mille kaudu on julgeolekuasutustel võimalus anda vajadusel sisendit Justiits- ja Digiministeeriumile ning Riigi Infosüsteemi Ametile. Sellise koostöömehhanismi reguleerimine seaduse tasandil ei ole meie hinnangul vajalik.	
2.3	Planeeritava [KüTS] § 13^3 lõike 1 kohaselt võib Vabariigi Valitsus määrusega kohustada teenuse osutajat järgima käesoleva seaduse §-s 7 sätestatud nõuetele vastavuse tõenduseks teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside	Mittearvestatud ja selgitatud Eelnõust on vastav paragrahv välja jäetud, et võtta üle NIS2 direktiiv minimaalses mahus. Seetõttu vastavat volitusnormi ei ole võimalik kasutada, et kommentaaris olevat Vabariigi Valitsuse määrust kehtestada.

	kasutamist, mis on sertifitseeritud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel ning mis on: 1) töötatud välja teenuse osutaja poolt; või 2) hangitud kolmandalt isikult. Palume kaaluda võrgu- või infosüsteemi turvalisust tagavate IKT-toodete, IKT-teenuste ja IKT-protsesside puhul elutähtsa teenuse osutajatele kohustuse kehtestamist kasutada sertifitseeritud või turbehinnatud tooteid. Julgeoleku laiapindset käsitlust silmas pidades on ülimalt oluline, et elutähtsa teenuse osutajad lähtuvad oma võrgu- või infosüsteemide kaitsel sarnastest põhimõtetest nagu salastatud teabe töötlemiseks kasutatavate võrgu- ja infosüsteemide valdajad. Vähemalt need võrgu- või infosüsteemi komponendid, mille eesmärk on tagada teabe salajasus ja sidekanali turvalisus, peavad olema kaitstud toodetega, mis on saanud heakskiidu või mille turvalisust on hinnatud. Ettepanekut toetab ka Eesti võetud kohustus Põhja-Atlandi Lepingu Organisatsiooni (NATO) Washingtoni tippkohtumiselt, mille deklaratsioonis on öeldud järgmist: *"Lubame teha jätkuvaid jõupingutusi, et tugevdada riigi vastupanuvõimet, integreerides tsiviilplaneerimise riigi ja kollektiivkaitse planeerimisse rahu, kriisi ja konflikti ajal. Me jätkame oma vastupanuvõime suurendamist, suurendades alliansi kollektiivset*	

	teadlikkust, valmisolekut ja suutlikkust kõigis ohtudes ja kõikides valdkondades, et tegeleda kasvavate strateegiliste ohtudega, sealhulgas meie demokraatlike süsteemide, kriitilise infrastruktuuri ja tarneahelate vastu. Kasutame kõiki võimalusi pahatahtlike tegevuste avastamiseks, nende eest kaitsmiseks ja neile reageerimiseks.“.	
	3. Kliimaministeerium 21.02.2025 e-kiri	
3.1	Lennundusvaldkonnas elutähtsa teenuse osutajatele laienevad KÜTS nõuded automaatselt, kuid **eelnõu § 1 punktiga 1 lisatakse mh KüTSi §-i lõige 1^2, mille punkt [19] ütleb**, et seadus kohaldatakse mh ka lennujaama haldajale lennundusseaduse tähenduses, Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ lennujaamatasude kohta (ELT L 70, 14.03.2009, lk 11–16) artikli 2 punktis 1 määratletud lennujaamale ning lennujaamas olevaid abirajatisi käitav üksusele, kui selliste ettevõtete/teenuseosutajatel on vähemalt 50 töötajat ja käive 10 mln eurot. Seletuskiri ei ava mida täpselt on mõeldud abirajatisi käitatavate üksustena (mis otstarve ja funktsionaalsus, kelle omand jne). Seega on põhjendatud täiendavalt selgitada, keda on mõeldud abirajatisi käitatava üksusena juhul kui ei ole mõeldud LennSi § 50^3 kohast lennujaama haldajat või tema volitatud isikut (maapealset teenindajat või omakäitlejat). Selgituseks lisan, et Tallinna lennujaamas olevate abirajatisi käitavate üksustena võib peale ASi Tallinna Lennujaam käsitleda ka tütarettevõtjaid (AS Tallinn Airport	Selgitatud Lennujaam on juba direktiivi 2009/12/EÜ järgi (art 2 p 1) defineeritud selliselt, et see hõlmab ka „lennuliikluse ja -teenuste nõuete täitmiseks vajalikud abirajatised, sealhulgas ärilendude teenindamiseks vajalikud rajatised“. NIS2 direktiivis on lähtutud sellest ja lennundusseaduses toodud definitsioonidest. Näiteks on selle seaduse § 50^3 lõikes 1 sätestatud, et lennujaama haldaja on lennujaama haldav isik, kelle ülesanne on õigusaktide ja lepingute alusel hallata ja juhtida lennujaama taristut ning koordineerida ja kontrollida lennujaamas tegutsevate käitajate tegevust. Sama paragrahvi lõige 2 sätestab, et kui lennujaama haldab mitu isikut, on lennujaama haldaja iga selline isik. Lennujaama abirajatise käitaja on NIS2 direktiivis (lisas I) kasutatud termin, mis võetakse eelnõuga üle. Lepingupartneritele, kes ise KüTS-i subjektiks ei kvalifitseeru, ei rakendu automaatselt ka KüTS-i nõuded. Samaväärsed nõuded tuleb soovi ja/või vajaduse korral näha ette lepinguliselt.

	GH ja AS Airport City) või muul juhul ka nende lepingulisi partnereid. Olgu lisatud, et lennujaama kui taristu vaatest tuleks piiritleda taristut, mis tervikuna teenindab õhusõidukeid ja on seotud selle protsessiga (nt konkreetsem viide tasudega seotud direktiivis art 2 lg 1 eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32009L0012). Samuti ei selgu, kas KÜTS nõudeid on võimalik laiendada automaatselt nt ka lepingupartneritele (nt lennundusjulgestusteenuse pakkujale) või tuleks see ette näha ise lepingutes?	
3.2	Merendusvaldkonnas elutähtsa teenuse osutajatele laienevad KÜTS nõuded automaatselt, kuid **eelnõu § 1 punktiga 1 lisatakse mh KüTSi §-i lõige 1², mille punkt 23** ütleb, et seadust kohaldatakse mh ka sadama pidajale või sellise sadamarajatise valdajale sadamaseaduse tähenduses, sealhulgas nende Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatised, ja sadamates tööde ning varustuse haldamisega tegelevale üksusele, kui selliste ettevõtete/teenuseosutajatel on vähemalt 50 töötajat ja käive 10 mln eurot. Seletuskiri ei ava, kas mõni sadama pidaja ilma sadamoperaatoriteta üldse kvalifitseeruks kohaldamisalasse. Lisatava lõike seletust võib lugeda, et esialgsel hinnangul on kommenteeritava punkti sõnastusele vastavaid üksusi 10 ja nendest 5 lähevad ka nn suuruse kriteeriumi alla. Täpset metoodikat ei ole avatud. Palume seletuskirja selles osas täpsustada.	Selgitatud Subjekt on määratletud vastavalt NIS2 direktiivi I lisas märgitud 2-c-teisele viitele ja Eesti seadusandjal ei ole võimalik seada loetelust välja jätta või muul viisil kohaldamisala kitsendada.

3.3	Vee- ja kanalisatsioonivaldkonna elutähtsa teenuse osutajatele laienevad KÜTS nõuded automaatselt, kuid **eelnõu § 1 punktiga 1 lisatakse mh KüTSi §-i lõige 1^2, mille punkt 33** ütleb, et seadust kohaldatakse mh ka: 1) vee-ettevõtjatele, kelle põhitegevusalaks ongi reovee ärajuhtimine ja puhastamine, 2) ettevõtjatele, kes osutavad reovee ärajuhtimise ja puhastamise teenust ilma ametlikult vee-ettevõtjaks määramiseta, 3) kui ka nt tööstusettevõtjatele, kel on ühiskanalisatsioonist eraldiseisev reoveepuhasti, ent kelle põhitegevusalaks ei ole reovee ärajuhtimine ja puhastamine. Ja see hõlmab neid ettevõtteid/teenuseosutajaid, kellel on vähemalt 50 töötajat ja 10 mln eur käive. Seejuures on aga tehtud erand, et see ei kehti ettevõtjale, kelle puhul asulareovee, olmereovee või tööstusreovee kogumine, ärajuhtimine või puhastamine on väheoluline osa tema üldisest tegevusest. Teeme ettepaneku kaaluda „väheolulise osa“ sisustamisel näiteks neid tööstusettevõtjaid, kel on küll ühiskanalisatsioonist eraldiseisev reoveepuhasti, ent kelle põhitegevusalaks ei ole tegelikult reovee ärajuhtimine ja puhastamine. Soovitame selle ettepaneku sobivuse osas direktiivi eesmärgiga konsulteerida Euroopa Komisjoniga. Kuna joogivee puhul on oluline, et tarbijateni juhitaks/toimetataks alati kvaliteetne joogivesi, vältimaks terviseohtu, siis leiame, et joogivee osas ei ole võimalik määratleda selliselt „väheolulist osa“, mistõttu soovitame siinkohal „väheolulise	Selgitatud: Juhime tähelepanu, et kui kommentaaris mainitud ettevõtjad on hädaolukorra seaduse alusel elutähtsa teenuse osutajateks määratud, siis kohalduvad neile KüTSi nõuded hoolimata töötajate arvust ja käibe suurusest. NIS2 direktiiv ei anna selgust, mida tuleks silmas pidada „väheolulise osana“ tegevusest, mis paneb seda ülevõtvad liikmesriigid keerulisse olukorda - ühest küljest peab olema piisavalt selge, millised üksused kuuluvad direktiivis (ja seaduses) toodud määratluse ja seega kohaldamisala hulka, millised aga mitte. Teisest küljest oleks „väheolulise osa“ määratlemine näiteks kindla protsentväärtusena meelevaldne ja riskantne, kuna eksiks NIS2 direktiivi kandva põhimõtte vastu, milleks on siseturu üleselt küberturvalisuse alaste nõuete ühtlustamine. Kindlate lävendite seaduses sätestamine tooks aga (ning seda on juba ülevõtmispraktikate võrdluses kohati näha) kaasa vastupidise tulemuse ning praktiliselt kindlasti realiseeruva sisulise rikkumismenetluse ohu. Sellest tulenevalt on eelnõu autorid, arvestades mh mitme teise liikmesriigi valitud lähenemisega, otsustanud (i) esitada Euroopa Komisjonile päringu kõnealuses küsimuses liikmesriikidele selgete suuniste andmiseks; ja (ii) seni, vastavate suuniste puudumisel, võtta kõnealune kriteerium üle täpselt ja ühetaoliselt direktiivis toodud~~ga~~ kujul ning möönda, et vajadusel e vähetõenäolistes vaidlusalustes olukordades tuleb see sisustada praktikas ja juhtumipõhiselt, arvestades igakordselt asjaolude ja vaidlusaluse juhtumi objektiivsete tunnustega. Võrdluseks võib välja tuua, et sarnast lahendust on kasutatud ka teiste riikide direktiivi ülevõtmiseks koostatud eelnõudes. Näiteks on see selliselt kavandatud Eesti õiguskorra kujundamisel oluliseks eeskujuks olnud Saksa Liitvabariigi vastavas seaduseelnõus (kõnealuse eelnõu koostamise ajal ei ole Saksamaal veel eelnõu seadusena vastu võetud) ning Belgia kuningriigi vastavas seaduses Seletuskirja on vastavalt täiendatud.

	osa“ tõlgendamisel samuti konsulteerida Euroopa Komisjoniga. Lisaks tuleks seletuskirjas "joogiveeseadus" asendada "veeseadusega". Samuti märgime infoks ära, et n-ö vana (01.01.2025 jõustus uus asulareovee puhastamise direktiiv 2024/3019) asulareovee puhastamise direktiiv 91/271/EMÜ on lisaks ühisveevärgi- ja kanalisatsiooniseadusele üle võetud ka veeseadusega.	
4. Kultuuriministeerium kooskõlastab märkusteta 31.01.2025 märge eelnõude infosüsteemis		
5. Majandus- ja Kommunikatsiooniministeerium kooskõlastab märkustega 18.02.2025 e-kiri		
5.1	Kohaldamisala osas paremat selguse loomiseks palume täiendada seletuskirja näidetega, millistele ettevõtjatele uued nõuded kohalduvad.	Selgitatud Võimaluse korral on seletuskirja lisatud subjektide sõnastuste juurde ka näide, kuid kuna KüTSi üksuste nimekirja ei avalikustata (vt ka eelnõu KüTS § 3^1), siis ei ole ka võimalik kõikide üksuste juurde lisada ettevõtjate nimesid.
5.2	Eelnõu § 1 punktiga 1 lisatava KüTS § 1 lõikega 1^6 antakse Vabariigi Valitsusele õigus määrusega lisada uusi sektoreid või valdkondi, kellele hakkaksid KüTS-i nõuded kohalduma. Leiame, et antud volitus on ebaproportsionaalne. Juhul, kui peaks tekkima tulevikus vajadus laiendada KüTSi uutele sektoritele või valdkondadele, siis tuleks kohaldamisala laiendus sätestada seaduse tasandil.	Arvestatud - vastava määruse volitusnorm on eemaldatud eelnõust.
5.3	Eelnõu § 1 punktis 1 nähakse ette KüTS-i § 1 lõikes 1^1 kohaldamisalasse sattumisest teatud välistavad tingimused. KüTS ei kohaldu eelnõus loetletud tegevusaladel tegutsevale ettevõttele, kui ettevõttel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aasta bilansimaht või aastakäive jääb alla 10 miljonit euro. Samas võivad olla KüTSi	Selgitatud NIS2 direktiiv ei näe paraku ette taolise täpsustuse tegemise võimalust. Taoline erisus (tegemist on KüTSi teenuseosutajaga siis, kui mingi valdkonnaga seotud tegevusala on väheoluline osa tema kõikidest tegevustest) on NIS2 direktiivis ette nähtud ainult üksikute valdkondade puhul (nt reovee valdkonnas). Kui taolist põhimõtet rakendada ka muude valdkondade puhul, kus NIS2 direktiiv ise ei näe ette kitsendust, siis selline tegevus ei ole NIS2 direktiiviga kooskõlas.

	subjektis mitmed ettevõtted, kellele kohalduvad nõuded ka siis, kui ettevõte tegutseb subjektiks olevas sektoris vähetähtsal määral. Mistõttu palume tungivalt kaaluda võimalust siduda KüTSi subjektis oleva tegevuse osakaalu sidumist mõõdetava näitajaga (nt aastakäibega), et oleks võimalik välistada kohaldamisalast vähetähtsal määral KüTSi kohaldamisalas tegutsevad ettevõtjad. Eriti oluline on eelnimetatu erisuse loomine toidukäitlemise sektoris.	Kui tuua siia paralleel turvameetmete (NIS2 direktiivis riskijuhtimismeetmete) vaatenurgast, siis juhime tähelepanu Euroopa Komisjoni suunistele NIS2 artikli 4 lõigete 1 ja 2 kohaldamise kohta. Suuniste punkti 7 viimase lauses on selgitatud: *„Direktiivi (EL) 2022/2555 artikli 21 lõikes 1 sätestatud kohustus, mille kohaselt peavad [üliolulised] ja olulised üksused võtma asjakohaseid ja proportsionaalseid küberturvalisuse riskijuhtimismeetmeid, kehtib kõigi asjaomase üksuse tegevuste ja teenuste suhtes ega puuduta üksnes konkreetseid infotehnoloogia („IT“) varasid või [üliolulisi] teenuseid, mida üksus osutab.“*. Seega ei oleks ka kommentaaris pakutud „vähetähtsa määra“ variant ka kasutatav, kui Komisjoni enda suuniste kohaselt tuleb näiteks turvameetmete nõudeid kohaldada konkreetse üksuse kõikide tegevuste ja teenuste suhtes. Taustainfoks tasub teada, et sama küsimust on põhjalikult vaaginud ka teised liikmesriigid, kes on juba NIS2 direktiivi üle võtnud ning on andnud selle kohta välja ka selgitavaid materjale. Näiteks on soovi korral võimalik tutvuda ka Belgia kuningriigi pädeva asutuse vastavate selgitustega siin (lk 8 alajaotis B) ja siin (nt lk 8, lk 11, lk 12).
5.4	Eelnõu seletuskirjas on hinnatud mõju majandusele, sh on välja toodud, et ettevõtjate halduskoormus suureneb nt riskijuhtimismeetmete rakendamisel ja küberintsidentidest teavitamisel. Palume siiski mõjuanalüüsi täiendada ettevõtjatele lisanduvate kulude osas, vähemalt erinevate näidete baasil. Saame aru, et kulud erinevad sõltuvalt ettevõtete suurusest ja nende tegevuste hulgast, kuid on oluline ettevõtjatele vähemalt näidete baasil anda hinnangulised kulud.	Selgitatud Kuna nii KüTSi subjektide enda vajadused kui ka võrgu- ja infosüsteemid on erinevad, siis ei pruugi seletuskirjas toodud näited tuua võrreldavust teiste ettevõtjatega, kellel sarnaseid vajadusi ega võrgu- ja infosüsteeme pole.
5.5	Palume eelnõus arvestada, et on oluline tagada ettevõtjatele selgus, millised on NIS2 direktiivist tulenevad nõuded ning millised on siseriiklikult juurde lisatud. Olukorras, kus selle peab tuvastama	Arvestatud ja selgitatud Märgime, et NIS2 direktiivi ülevõtmisega saavad kõik sellest tulenevad nõuded siseriikliku õiguse osaks, seaduses sisalduvateks nõueteks. Direktiiv võetakse üle

	ettevõtja ise, tekitab see ettevõtjale täiendavat halduskoormust.	minimaalsel võimalikul määral, arvestades siseriiklike eripäradega. Seetõttu eelnõus endas ei ole muid uusi nõudeid, mis tekitaksid teenuseosutajatele uusi kohustusi.
5.6	Juba KüTSi kohaldamisalas olevatele ettevõtjatele (subjektidele) tuleks võimaldada uute nõuete osas asjakohast üleminekuaega kuni 3 aastat, nagu uutele subjektidele.	Arvestatud – vt eelnõu KüTS § 28^1. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
6. Rahandusministeerium kooskõlastab märkustega 17.02.2025 kiri nr 1.1-11/5510-4		
6.1	Eelnõu § 1 punktiga 24 täiendatakse küberturvalisuse seadust (edaspidi *KüTS*) §-ga 6^1, mille lõigetega 2 ja 3 võetakse üle NIS2 direktiivi artikli 20 lõige 2, mis on seotud NIS2 direktiivi põhjenduspunktiga 137, mille kohaselt peaksid elutähtsate ja oluliste üksuste juhtorganid kiitma küberturvalisuse riskijuhtimismeetmed heaks ja jälgima nende rakendamist. Seletuskirja kohaselt võiks teenuse osutaja juhtorgani liikmete erikoolituste sisu ehk õpiväljundid olla järgmised: küberturvalisusega seotud riskid, ohud, levinumad rünnakutüübid kui ka riskide haldamine. Samuti ootab eelnõu koostaja tagasisidet, kas taoline välp tuleks reguleerida ning kui jah, siis mis võiks olla sobiv välba pikkus. Teeme ettepaneku, et välba pikkus võiks olla kaks aastat. Palume eelnõus selgelt sätestada ja seletuskirjas selgitada, mida peetakse silmas erikoolituse all (miks mitte lihtsalt koolitus), millistele nõuetele peavad vastama erikoolituse läbiviimiseks pädevad koolitusasutused ja mis on koolituse läbimist tõendavaks dokumendiks. Ühtlasi palume normitehniliselt täpsustada uue § 6^1 asukohta, sest oma olemuselt kuulub uus § 6^1 1.	Selgitatud Eelnõu tekstis on sõna „erikoolitus“ asendatud sõnaga „koolitus“. NIS2 direktiiv ei määratle koolituste läbimise välpa ega spetsiifilisi õpiväljundeid. Samas on eesmärk üle võtta minimaalsete võimalike kohustustega. Sellest tulenevalt ei ole põhjendatud koolituse sisu/kvaliteedi/muude kriteeriumite põhjalikum reguleerimine. Seetõttu ei sätestata eelnõuga seaduse ega ka selle alusel antava määruse tasandil selle välba pikkust (vt määruste kavandeid). Selle määratleb konkreetne üksus ise (nt ideaalselt üks kord aastas, et juhatuse liige saaks tuletada meelde seletuskirjas kirjeldatud õpiväljundite teemasid). See, kas üksuse koolitusplaan ja selle nõude täitmine on olnud piisav, saab hinnata järelevalve käigus. Alates sellest, et kas juhtkond mõõdab koolitustulemusi, teeb sellest mingeid järeldusi, korrektuure, kas juhtkond oskab selgitada oma vastutusalasse kuuluvaid asju, nõuda infoturbega tegelevatelt töötajatelt selgitusi, aruandeid, langetada selle põhjal argumenteeritud otsuseid jne. Eelnõu ei määratle nõudeid koolitaja pädevusele ning mis on koolituse läbimise tõendavaks dokumendiks. Samuti ei määratleta eelnõus, kes võib seda koolitust juhatuse liikmele teha – nt kas selle võib teha ka sama üksuse infoturbejuht. Euroopa Komisjoni suunistes direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta 2023/C 328/02, on suuniste punkti 37 teise tekstilõikes märgitud, et NIS2 direktiivi artiklitest 20 ja 21 tulenevad kohustused on omavahel seotud. Seetõttu on eelnõu KüTS § 6^1 asukoht õige, st tegemist on nõudega, mis on seotud ennekõike KüTS §-ga 7, mistõttu on selle asukoht sobivaim KüTSi 2. peatükis. Eelnõu seletuskirja asjaomase sätte juures täiendatud.

	peatükki alla, kuna ei peaks kohalduma nendele finantssektori ettevõtjatele, kellele KüTS 2. peatükk ei kohaldu (krediidiasutustele krediidiasutuste seaduse § 82^4 lõige 3, registripidajatele väärtpaberite keskregistri seaduse § 30^2 lõige 2 ja reguleeritud turu korraldajale § 124^6 lõike 3 kohaselt).	DORA määruse subjektide osas vt Finantsinspektsiooni kommentaari 15.2 vastust.
6.2	Eelnõu § 1 punktiga muudetakse KüTS § 1 lõiget 4. Teeme ettepaneku seletuskirjas välja tuua, et näiteks on see säte asjakohane seoses määruse (EL) 2022/2554 (DORA) nõuete kohaldamisega finantssektoris. DORA määruse põhjenduspunktis nr 16 on selgitatud, et DORA määrus on NIS2 suhtes *lex specialis*. NIS2 direktiivi põhjenduspunkt 28 selgitab lisaks, et NIS2 direktiivi sätete asemel tuleks kohaldada DORA määruse sätteid, mis käsitlevad IKT riskijuhtimist, IKT intsidentide haldamist ja eelkõige tõsistest IKT intsidentidest teavitamist, samuti digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevat IKT-riski. Seetõttu ei tohiks liikmesriigid NIS2 direktiivi sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist, DORA määruse kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada. Palume selgitada, kas/kuidas tuleks kohaldada KüTS § 17^5 nii KüTS kui ka DORA kohaldamisalasse jäävatele finantssektori ettevõtjatele. Eelosutatud NIS2 põhjenduspunkti	Arvestatud ja selgitatud: KüTS § 1 lg 4 muutmise osas on seletuskirja täiendatud. KüTS § 17^5 on võimalus, mitte kohustus teavet vahetada, sh see on mõeldud nii KüTSi kohaldamisalas olevatele isikutele kui ka muudele osapooltele, kes vastavas teabevahetuse kokkuleppes soovivad osaleda. Seega võivad ka DORA määruse kohaldamisalas olevad isikuid lähtuda KüTS §-ist 17^5. Lisaks juhime tähelepanu Komisjoni teatisele Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta 2023/C 328/02, milles ei ole välistatud võimalus, et DORA määruse subjektile kohaldub ka NIS2 direktiivi artikkel 29.

	28 kohaselt tuleks NIS2 direktiivi sätete asemel kohaldada DORA määruse sätteid, mis käsitlevad mh teabevahetuse kokkuleppeid. NIS2 artikli 4 lõike 1 sõnastus on kitsam, viidates ainult küberturvalisuse riskijuhtimismeetmete võtmisele või olulistest intsidentidest teatamisele (nagu on ka KüTS § 1 lg 4). DORA määruses on teabevahetus reguleeritud artiklis 45, kuid hõlmab ainult finantssektori ettevõtjate omavahelist teabevahetamist ja kokkuleppeid. Kui näiteks kaks finantssektori ettevõtjat (nt kaks ETO panka) soovivad omavahel vahetada teavet, siis kas teabevahetusele kohalduvad topelt normid?	
6.3	Eelnõu § 1 punktiga 26 kohustatakse teenuse osutajat turvameetmete rakendamisel koostama ja kehtestama varade halduse põhimõtted ja seotud protseduurijuhendid (p 12). Kuigi ilmselt on enamus teenuse osutajatel kehtestatud vara halduse põhimõtted ja protseduurijuhised mistahes vara puhuks, ei ole küberturvalisuse vaatenurgast selline ulatuslik nõue KüTSis siiski asjakohane. Palume sättes varad piiritleda KÜTS § 1 lõikest 1 lähtuvalt.	Selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Kuna NIS2 direktiiv tekitab vajaduse laiendada KüTSi nõuded kogu teenuseosutaja tegevusele, siis ei ole ka võimalik piirata kommentaaris mainitud varade halduse teemat ainult KüTS § 1 lõikega 1. Vt ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.
6.4	Seletuskirja punktis 6.2.3 on hinnatud eelnõu mõju majandusele. Üldistatult saab kokku võtta, et olemasolevaid subjekte on 3537 ning uusi subjekte on ligikaudu 2000 ehk kokku on ligikaudu 5500 subjekti, kellele KüTSi nõuded hakkavad kohalduma. Üks osa Eesti infoturbestandardi rakendamisest on ka Eesti infoturbestandardi vastavusauditi tegemine iga kolme aasta järel, mis on eelduslikult ühe suurema kulu allikas uutele KüTSi	Arvestatud Eelnõu seletuskirjas on auditi maksumuse andmeid täiendatud Riigi Infosüsteemi Ameti sisendi põhjal. Võimaluse korral on ka seletuskirjas täiendatud mõjude osa seoses turvameetmete rakendamisega. Siin vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.

	subjektidele. Auditi maksumus jääb seletuskirja kohaselt 4500–20 000 euro vahemikku. Eelnõu koostajad märgivad, et nimetatud summa on kajastatud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (426 SE) seletuskirjas ning antud eelnõu koostamise hetke seisuga ei olnud võimalik kontrollida, kas mainitud maksumuste suurusjärk on jätkuvalt sama või on siin mingeid muudatusi toimunud. Juhime tähelepanu, et hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (426 SE) eelnõu saadeti ministeeriumidele EIS-i kaudu esimesele kooskõlastusringile septembris 2023. a. Seega on auditi maksumuse andmed ilmselgelt vananenud. Palume seletuskirjas olevad auditeerimise hinnad korrigeerida. Värskemaid andmeid on võimalik saada riigihangete registrist või tehes päringuid audiitorfirmadele (Audiitorkogule). Lisaks palume seletuskirjas realistlikult hinnata subjektidele kaasnevat mõju (nii halduskoormusele kui ka kuludele) seoses Eesti infoturbestandardi rakendama hakkamisega.	
6.5	Seletuskirjas on puudu andmed, kui paljud audiitorfirmad (audiitorid) IT-auditeerimise teenust pakuvad. Arvestades seda, et Eesti infoturbestandardi auditeerimisjuhendi kohaselt koosneb E-ITS audit minimaalselt põhiauditist ja vaheauditist (viiakse läbi hiljemalt üks aasta pärast põhiauditit või eelmist vaheauditit), on eeldatavasti juba praegu olemasolevad IT-auditeerimise teenuse	Arvestatud ja selgitatud Seletuskirja on täiendatud. Vastavate audiitorite andmed on leitavad siit: https://eisay.ee/e-its-ja-iso-27001-alaste-teenustega-tegelevate-ettevotete-loetelu. Eelnõu koostajate teadmiste kohaselt ei ole audiitoritel pikki järjekordi, kuid ajapikku võib turutõrge tekkida olukorras, kui enamus teenuseosutajaid hakkavad ühel ajahetkel tellima endale välist auditit. Kui siin peakski tekkima turutõrge (tekib audiitorite vähesuse olukord), siis saab tol hetkel analüüsida, kas ja mil moel on võimalik turutõrke olemasolu tõendada järelevalveasutusele (nt kas piisab sellest, et teenuseosutaja on

	pakkujad väga hõivatud. Seega võivad lisanduvad 2000 subjekti nõuetekohaste auditite läbiviimise muuta võimatuks ja/või tõsta auditeerimise teenuse hinna kõrgeks. Seega palume seletuskirja täiendada IT-auditeerimise teenust pakkuvate audiitorite andmetega, kaaluda auditeerimistsükli pikendamist või esitada seletuskirjas muud olukorra leevendamise meetmed. Väheste audiitorite ja kulu suurendamise olukorras pannakse kohustatud isikutele üle jõu käivad kohustused.	mitmelt audiitorilt küsinud pakkumisi ja nad kõik on keeldunud vms), sh mil määral järelevalveasutus sellega arvestab enda toimingute tegemisel. Eesti infoturbestandardi auditeerimistsükkel lähtub samaväärse rahvusvahelise standardi ISO/IEC eeskujul 3 aastasest tsüklist ning kui Eesti infoturbestandardi puhul seda muuta, siis tegemist ei ole samaväärsete nõuete kogumiga. Täiendavalt märgime, et ettevalmistamisel on ka koolitused, mis on seotud infoturbe audiitorite järelkasvu küsimusega. Siin vt ka Siseministeeriumi kommentaari 8.3 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust.
6.6	Eelnõu § 1 punktis 1 (lisatav KüTS § 1 lg 1^6), § 1 punktis 5 (KüTS § 1 lg 4^1) ja § 1 punktis 49 (KüTS § 13^3 lg 1) ei ole normi sõnastusest võimalik aru saada, kas mõeldud on pädevusnormi või määruse andmise volitusnormi, seega palume sõnastuste vastavust HÕNTE-le kontrollida.	Selgitatud Viidatud sätete puhul oli soov tekitada volitusnorm konkreetse määruse andmiseks. Eelnõud üle vaadates otsustati vastavad volitusnormid välja võtta.
6.7	Eelnõu § 1 punktiga 58 täiendatakse KüTS vastutuse osa, lisades seaduse nõuete rikkumise eest karistused ka füüsilisest isikust üksustele. Palume seletuskirjas tuua näiteid Eestis olevatest füüsilistest isikust elutähtsast, olulisest ja komisjoni delegeeritud määruse EL 2024/1366 nimetatud üksustest.	Selgitatud Vajadust lisada karistused ka füüsilisest isikust üksustele on ammendavalt selgitatud eelnõu seletuskirjas KüTS § 18^2 jj selgitustes. Eelnõu autoritel ei ole võimalik täna ega tuleviku vaates välistada olukordi, mille kohaselt üksuseks ehk eelnõu subjektiks võib kvalifitseeruda füüsiline isik - näiteks füüsilisest isikust ettevõtja. Näidete toomise kommentaari osas vt Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.1 vastust.
6.8	Eelnõus pannakse kohustatud isikutele mitmeid teavituskohustusi, mida ja millal ja kuidas peab kohustatud subjekt Riigi Infosüsteemi Ametit teavitama. Samas pole täpsustatud, kas ja kuidas peaks Riigi Infosüsteemi Amet nendele teavitustele vastama.	Selgitatud KüTSi kohaldamisalas olev isik teavitab enda andmetest (vt uuendatud eelnõu KüTS § 3^1 lõiget 1 ja § 4 lõiget 1), kuid tol teemal ei ole NIS2 direktiivis ette nähtud, et pädev asutus peaks neile vastama. Sel põhjusel ei ole vajalik ega otstarbekas ka siseriiklikult pädevale asutusele mingil kindlal kujul vastamiskohustust ette näha. Kui subjekt on teavituskohustuse täitnud, on tema vastav KüTS-st tulenev kohustus sellega täidetud.

		Kui kommentaari puhul ei mõeldud andmetest teavitamist, vaid küberintsidentidest teavitamise vaatenurgast, siis eelnõus on sel teemal tagasiside andmine reguleeritud eelnõus KüTS § 12 lõikega 3^1.
6.9	Palume lisada eelnõusse üleminekusätted, mille kohaselt antakse uutele kohustatud isikutele piisav üleminekuaeg Eesti infoturbestandardi ja sellest tulenevate turvameetmete rakendamiseks. Eesti infoturbestandardi rakendamisega seonduv tööhulk ja kulud (eelarvelised piirangud) võivad olla arvestatavad ja ei pruugi arvestades seaduse eelnõus sätestatud seaduse jõustumise aega olla tehtavad. Seejuures tuleks eelnevalt analüüsida, kas kõikidele kohustatud subjektidele ühetaolise Eesti infoturbestandardi või ISO27002 standardi rakendamise kohustuse panemisele on võimalik leida väiksemat halduskoormust (ja kulu) kaasa toov alternatiiv.	Arvestatud – vt eelnõu KüTS §-e 4^1 ja 28^1. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
6.10	Palume üle kontrollida eelnõuga kasutusele võetavate ja kehtivas seaduses kasutatavate terminite kasutus (et sama mõiste jaoks ei kasutataks erinevaid termineid). Näiteks kasutatakse eelnõus intsidentide avastamise ja halduse termineid läbisegi, samuti on eelnõu tekstis korduvalt kasutatud loetelusid stiilis „küberriskide-, -ohtude, -intsidentide…“, kus selline üldistamine ei loo selgust ning jätab liigselt tõlgendusruumi nii seaduse täitmiseks kui järelevalveks.	Arvestatud – sõnastused on üle vaadatud.
6.11	Eelnõus esineb palju keelevigu, seega palume eelnõu enne selle edasist menetlemist keeleliselt toimetada.	Arvestatud – sõnastused on üle vaadatud.
7. Regionaal- ja Põllumajandusministeerium kooskõlastab märkustega 06.02.2025 kiri nr 1.4- 2/5166-1		

7.1	Eelnõu seletuskirja kohaselt on eelnõu eesmärgiks võtta 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, üle kitsalt ehk minimaalsel vajalikul tasemel. Muus osas võetakse direktiiv eelnõus üle minimaalses osas, kuid mitte ettevõtja rakendatavate meetmete osas. Rõhutame, et Regionaal- ja Põllumajandusministeerium ei pea põhimõtteliselt õigeks, et kõnealuse direktiivi ülevõtmisel Eesti õigusesse rakendatakse kõigi valdkondade ettevõtjate suhtes ühetaoliselt üksnes suure halduskoormusega Eesti infoturbestandardit (edaspidi *E-ITS*) või lausa rahvusvahelist ISO27001 standardit. Leiame, et tasakaalu leidmiseks nimetatud direktiivis sätestatud eesmärkide saavutamise ja kõigile ettevõtjatele langeva halduskoormuse vahel tuleks esimese valikuna E-ITSi rakendamise asemel töötada välja ka teatud valdkonna ettevõtja jaoks väiksema halduskoormusega ning vaid direktiivis nõutud valdkondi reguleeriv raamistik. Näiteks toidukäitlemisettevõtjate, kohalike teede korrashoiuga tegelevate ettevõtjate jmt valdkondade ettevõtjate jaoks on isegi juhul, kui tegemist on elutähtsa teenuse osutajatega, E-ITSi rakendamine ebamõistlikult suure halduskoormusega.	Arvestatud – vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

7.2	Eelnõu § 1 punktiga 1 täiendatakse küberturvalisuse seaduse § 1 lõikega 1^1, mille kohaselt võetakse küberturvalisuse seaduses kasutusele termin „üksus“. Eelnõu § 1 punkti 7 ja seletuskirja punkti 4.1 kohaselt on üksuseks füüsiline isik või juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigisisese õiguse kohaselt, kes võib enda nimel omada õigusi ja kanda kohustusi. Uute terminite kasutuselevõtmise korral tuleb seletuskirja osas „Eelnõu terminoloogia” lisaks seaduseelnõu uute terminite, mida õigusaktides ei ole varem kasutatud, tutvustamisele ka põhjendada nende kasutamise vajalikkust. Kuna nii termini selgitusest seletuskirjas kui ka eelnõust nähtub, et üksuse puhul peetakse silmas isikut, siis jääb arusaamatuks, miks õigusaktides juba kasutatava ja selgelt määratletud termini „isik“ asemel soovitakse küberturvalisuse seaduses kasutusele võtta seni õigusaktides mittekasutatav ja äärmiselt küsitavalt määratletud termin. Seletuskirjas tuleks selgitada vähemalt seda, mis kehtivas õiguses füüsilise ja juriidilise isiku termini määratluses eelnõus soovituga võrreldes puudu jääb ja miks ei saa eelnõus pidada piisavaks määratlust, et tegemist on füüsilise või juriidilise isikuga. Eespool toodust tulenevalt teeme ettepaneku eelnõus mitte kasutusele võtta terminit üksus ja kasutada selle asemel terminit „isik“ tsiviilseadustiku üldosa seaduse tähenduses.	Selgitatud Üksusteks on teiste seas sellised subjektid (nt riigiasutused), kes ei ole iseseisvalt määratletavad füüsilise, eraõigusliku, avalik-õigusliku juriidilise vm „isikuna“. Alternatiivselt võiks kõigi subjektide puhul kasutada „teenuseosutaja“ nimetajat, kuid kuna see on katustermin, mis hõlmab nii üliolulisi üksused kui ka olulised üksused, tekiks suurem segadus olukorras, kus seadus kasutaks näiteks sõnastust „üliolulise teenuseosutaja“ ja „olulise teenuseosutaja“. Seda eriti olukorras, kus mõni üksus võib nn suurusekriteeriumi kohaselt olla kas üliolluline üksus või oluline üksus. Üksuse, teenuseosutaja, üliolulise üksuse ning olulise üksuse mõistete olemuse selgitamiseks on lisatud ka seletuskirja 4. peatükki (eelnõu terminoloogia) vastav joonis. Terminoloogilisi parandusi võib kaaluda küberturvalisuse valdkonda korrastava eelnõu VTK väljatöötamise käigus.
7.3	Eelnõu § 1 punktiga 1 täiendatakse küberturvalisuse seaduse § 1 lõikega 1^2, mille	Selgitatud

	punkti 45 kohaselt kohaldatakse nimetatud seadust Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (EÜT L 31, 01.02.2002, lk 1–24), artikli 3 lõikes 2 määratletud toidukäitlemisettevõtja suhtes, kes tegeleb hulgimüügi, tööstusliku tootmise ja töötlemisega. Juhime tähelepanu, et nimetatud määruse artikli 3 lõikes 2 kasutatud termini „toidukäitlemisettevõtja“ puhul on tegemist tõlkeveaga. Nii nimetatud määruse artikli 3 lõikes 2 kui NIS2 direktiivi lisa 2 punkti 4 eestikeelses versioonis on „*food business*“ tõlgitud „toidukäitlemisettevõtjaks“, mis ei ole õige. Termini õige tõlge on „toidukäitlemisettevõte“. Toidukäitlemisettevõtja ehk toidu käitleja on inglise keeles „*food business operator“* ja selle määratlus on sätestatud Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002 artikli 3 lõikes 3 (vt ka toiduseaduse § 6 lõige 1). Tagamaks õigete terminite kasutus, mis oleks kooskõlas nii Eesti kui Euroopa Liidu õigusega, palume sõnastada küberturvalisuse seaduse § 1 lõike 1^2 punkt 45 järgmiselt: „45) toidu käitleja, kes tegeleb Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (EÜT L 31, 01.02.2002, lk 1–	KüTS § 3 lg 5 p 3 sõnastuses on pärast kaalumist otsustatud jääda termini „toidukäitlemisettevõtja“ juurde. Eelnõus on läbivalt käsitletud oluliste üksustena isikuid, kes tegutsevad direktiivi lisas II nimetatud valdkondades, milleks on mh toidukäitlemine. „Toidukäitlemisettevõtja“ on isik. Ettevõte ei ole isik, ettevõte on tsiviilseadustiku üldosa seaduse tähenduses majandusüksus, mille kaudu isik tegutseb. Kommenteeritud väljaande kohaselt „on ettevõte teatud otstarbeks mõeldud varakogum.“ Seetõttu ei oleks eelnõu autorite hinnangul selguse huvides täpne viidata siin „ettevõttele“. Ühtlasi ei anna NIS2 direktiiv paraku liikmesriikidele diskretsiooni diferentseerida antud valdkonda kuuluvaid subjekte toidugruppide kaupa. KüTSi kohaldamisalas oleva üksuse sõnastuse täpsustamine arvestades tema tegevuse olulisust – siin vt Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust. KüTSi teenuseosutaja sõnastuse täpsustamine ministri määrusega – eelnõus taolist lahendust ei looda, kuna soov on KüTSi teenuseosutajad kindlaks määrata seaduse, mitte määruse tasandil.

	24), artikli 3 lõikes 2 määratletud toidukäitlemisettevõttes toidu hulgimüügi, tööstusliku tootmise või töötlemisega;“. Palume eelmainitud terminitega seotud parandused teha ka seletuskirjas. Samas on nimetatud määratlus ka täpsustatud kujul liiga lai, eriti arvestades kui lai on termin „toit“, ja seetõttu oleme seisukohal, et seda määratlust tuleb olulisel määral kitsendada erinormide abil, mis määratleks selgelt nii toidu hulgimüügi, toidu tööstusliku tootmise kui toidu tööstusliku töötlemise termini selle seaduse tähenduses. Selge määratlus on vajalik selleks, et seaduse mõju täpsemalt hinnata ja kavandada seaduses ettevõtjatele üksnes vajalikud ning otstarbekad meetmed. Näiteks maisipulkade ning kartulikrõpsude tootja võib osutuda keskmise suurusega või sellest suuremaks ettevõtjaks, kuid kahtlemata ei ole selle valdkonna ettevõtja puhul tegemist riigi ja ühiskonna toimimiseks või elanikkonna kaitseks kriitilise tähtsusega valdkonnaga. Ka ülevõetav direktiiv toob välja olulisuse elanikkonnakaitsele. Seega oleks sellise ettevõtja suhtes ka E-ITSi järgimise kohustuse kehtestamine tema suhtes ilmselgelt ebaproportsionaalne. Seda eeldusel, et direktiivi ülevõtmisel on eesmärk tagada nende oluliste ettevõtjate toimepidevuse kasv, kelle töö jätkumine on riigi ja ühiskonna toimimiseks või elanikkonna kaitseks kriitilise tähtsusega. Kõnealuste terminite määratlemine nõuab aga kauem aega, kui eelnõu kooskõlastamiseks antud aeg. Regionaal- ja	

	Põllumajandusministeerium jätkab siiski selle teema analüüsimist. Kui üldjuhul tuleb terminid määratleda seaduses, siis seaduses antud piirides võib seda tegema volitada ka ministri. Seetõttu teeme alternatiivselt ettepaneku täiendada eelnõu volitusnormiga, mille kohaselt kehtestab valdkonna eest vastutav minister, kelleks käesoleval juhul on regionaal- ja põllumajandusminister, käesoleva seaduse § 1 lõike 1^2 punktis 45 sätestatud üksuse täpsema toidu käitlemise valdkonna arvestades käesoleva seaduse § 1 lõikes 1^4 sätestatud tingimusi, tehes seda vajaduse korral toidugruppide või tegevuse liikide kaupa.	
7.4	Mis puudutab seletuskirjas küberturvalisuse seaduse § 1 lõike 1^2 punkti 45 selgitustes esitatud termini „hulgimüük“ sisustamist, siis jääb arusaamatuks, miks on peetud vajalikuks selle asemel selgitada terminit „jaemüük“. Eelnõu kontekstis puudub justkui selleks vajadus. Pigem peaks piirduma selgitustega termini „hulgimüük“ kohta ja käsitlema seda nii nagu on seda tehtud tootmise ja töötlemise puhul ehk rääkida suuremahulisest turustamisest ning selguse huvides võib lisada, et hulgimüügi korral ei peeta silmas turustamist lõpptarbijale. Samuti võib viidata ka Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 853/2004, millega sätestatakse loomset päritolu toidu hügieeni erieeskirjad (ELT L 139, 30.4.2004, lk 55–205), lisa I punktile 8.2, mis käsitleb hulgimüüki kui müüki teistele toidu käitlejatele. Eespool toodust nähtub seega, et nii toidu hulgimüügi, toidu tööstusliku tootmise kui ka toidu töötlemise tegevusala on küberturvalisuse seaduse	Selgitatud Terminoloogilised selgitused „hulgimüügi“ puhul on „jaemüügi" kaudu antud seetõttu, et viimane on määruses 178/2002 defineeritud mõiste (art 3 p 7), mille poolt mitte hõlmatud osas müük kvalifitseerub hulgimüügiks. Kui hulgimüügi osas tuua paralleeli Eesti õigusaktidest, siis hulgimüük on müük isikule, kes ei ole tarbija tarbijakaitseseaduse tähenduses. Vt siin alkoholiseaduse § 3 lg 1 punkti 4: „*Alkoholi käitlemiseks loetakse selle toidugrupi suhtes teostatavad järgmised toimingud: müügiks pakkumine või müük ühelt ettevõtjalt teisele ettevõtjale või muule isikule, kes ei ole tarbija tarbijakaitseseaduse tähenduses (edaspidi hulgimüük)“*. Sama lõike punkti 5 kohaselt on jaemüügiks „*müügiks pakkumine, müük või mis tahes võlaõigusliku lepingu sõlmimine või mis tahes õiguslikul alusel majandustegevuse raames kättesaadavaks tegemine või üleandmine tarbijale tarbijakaitseseaduse tähenduses (edaspidi jaemüük)“*. Turupraktikast tulenevalt tuleb täiendavalt arvestada, et hulgimüügi puhul ei saa tegemist olla ka igasuguse juriidilisele isikule/asutusele suunatud müügiga, vaid eelkõige edasimüügi ja vahendusega tööstus- ja kaubanduslikele tarbijatele, asutustele ja organisatsioonidele. Seletuskirja on ka vastavalt täiendatud.

	rakendamiseks eelnõus sätestatud kujul piisavalt määratlemata. Vältimaks mitmeti mõistmist teeme ettepaneku esitada terminite „toidu hulgimüük“, „toidu tööstuslik tootmine“ ja „toidu töötlemine“ määratlused küberturvalisuse seaduse tähenduses eelnõus. Lisaks on seletuskirjas välja toodud, et esialgsel hinnangul on kommenteeritava punkti sõnastusele vastavaid üksusi 50 ja nendest 10 lähevad ka suuruse kriteeriumi alla, kuid subjektide arvu osas ei ole viidatud, millise andmestiku põhjal sellise arvuni on jõutud ja seetõttu ei saa Regionaal- ja Põllumajandusministeerium selle kohta arvamust esitada. Subjektide arvu on toidu hulgimüügi tegevusvaldkonna, aga ka teiste tegevusvaldkondade puhul, keeruline välja selgitada, kuna siin tuleb arvestada lisaks tegevusalale ka töötajate arvu ja aasta bilansimahu või aastakäibe suurust (sealjuures vajab täpsustamist, kas üldine või üksnes toidu käitlemisega seotud käive). Näiteks riigi toidu ja sööda käitlejate registri (edaspidi *RTSR*) andmete põhjal tegeleb Eestis hetkel hulgimüügiga umbes 1300 käitlejat[1]. Kui palju töötajate arvu, aasta bilansimahu või aastakäibe suuruse kriteeriumide arvestamine nende puhul seda numbrit väiksemaks muudab, on keeruline öelda, sest RTSRis selliseid andmeid ei töödelda. Andmeid ettevõtja müügitulu suuruse kohta erinevate tegevusvaldkondade lõikes on võimalik saada ettevõtja majandusaasta aruandest, mida saab pärida Registrite ja Infosüsteemide Keskuse e-äriregistri portaali kaudu ettevõtja kaupa. Toidu varustuskindluse valdkonna elutähtsate teenuste osutajate väljaselgitamiseks on seejuures	Lisaks märgime, et Euroopa Komisjoni soovituse 2003/361/EÜ alusel väikese- ja keskmise suurusega ettevõtjate töötajate ning finantsnäitajate arvestamise ning arvutamise metoodikat on seletuskirjas selgitatud eelnõu KüTS § 3 selgituste juures.

	kavas arvesse võtta elutähtsate teenuste osutajaks määramise aastale eelneva kahe majandusaasta aruandeid, et välistada andmete liigset kõikumist aastate lõikes. Veelgi keerulisem on subjektide väljatoomine toidu tööstusliku tootmise ja töötlemise puhul, sest toidualastes õigusaktides ei ole tööstuslikku tootmist ja töötlemist eraldi määratletud ning seega ei ole selge, millised käitlejad just tööstusliku tegevusega on hõlmatud. Kui RTRSist teha väljavõte toidu tootjate ja töötlejate (välja arvatud käitlejad, kes tegelevad esmatootmise, toidu külmutamise või toidu pakendamisega või tegelevad toidu käitlemisega eraelamus) kohta, siis selliseid subjekte on RTSRis umbes 1600, aga kui palju neist vastab eespool mainitud kriteeriumidele, ei ole RTSRi andmete põhjal võimalik öelda.	
7.5	Regionaal- ja Põllumajandusministeerium leiab, et ühistranspordiseaduse §-s 6 sätestatud vedajatele kavandatava püsiva kriisiülesande kohustusega seotud täiendused tuleks teha küberturvalisuse seadusesse eraldi seaduse muutmise seaduse eelnõuga.	Arvestatud – siinse eelnõuga neid muudatusi ei tehta.
7.6	Eelnõu § 1 punkti 19 kohaselt täiendatakse küberturvalisuse seaduse § 3 lõikega 3^1 ning sätestatakse, et teenuse osutaja ja domeeninimede registreerimise teenuseid osutav üksus esitab Riigi Infosüsteemi Ametile vähemalt järgmise teabe: „1) nimi ja registrikood; 2) aadress ja ajakohased kontaktandmed, sealhulgas e-posti aadressid, interneti protokolli aadresside vahemikud ja telefoninumbrid; …“.	Selgitatud NIS2 direktiivi artikli 3 lõikest 4 ega põhjenduspunktist 18 ei tulene täpsemaid juhiseid selle kohta, missugust aadressi on spetsiifiliselt silmas peetud ega sellest lähtuvaid täpsemaid eesmärke. Samas on Euroopa Komisjoni suunistes NIS2 direktiivi artikli 3 lõike 4 kohaldamise kohta (2023/C 324/02 - https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0914%2801%29&qid=1747382459870), konkreetsemalt selle p-des 3 ja 4 kirjas, et aadressi puhul on pigem mõeldud peamise

	Juhime tähelepanu, et viidatud [KüTS] § 3 lõike 3^1 punkti 2 kohaselt tuleb teenuse osutajal ja domeeninimede registreerimise teenuseid osutaval üksusel Riigi Infosüsteemi Ametile esitada teave aadressi kohta. Eelnõust ega seletuskirjast ei selgu, kas selliseid andmeid oleks võimalik saada ka ristkasutuse teel ja ilma isikult neid pärimata ning millist aadressi on mõeldud. Kas soovitakse teavet näiteks teenuse osutaja asukoha aadressi (nt äriregistrijärgne aadress), tsiviilseadustiku üldosa seaduse kohast tegevuskoha aadressi või ühe või mõlema eelnevalt mainitud koha postiaadressi. Teeme ettepaneku eelnõu sõnastust selles osas täpsustada (vaata ka eelnõu § 1 punkti 21, millega muudetakse § 4 lõike 1 punkti 3).	tegevuskoha aadressi (või ka muude tegevuskohtade aadressi). Seetõttu on eelnõus lähtutud peamise tegevuskoha aadressist. Edaspidiselt on võimalik analüüsida, kuidas ning milliseid andmeid on võimalik saada riiklikest andmekogudest. Siiski peab arvestama asjaoluga, et kõiki andmeid ei ole võimalik andmekogudest ei ole võimalik saada – nt üksus internetiprotokolli aadresside vahemikke.
7.7	Eelnõu § 1 punktiga 52 täiendatakse KüTSi § 14 ning selle lõike 9 punkti 2 kohaselt on Riigi Infosüsteemi Ametil riikliku ja haldusjärelevalve läbiviimisel õigus teha teenuse osutaja suhtes sihipäraseid turvaauditeid, mis põhinevad Riigi Infosüsteemi Ameti või auditeeritava teenuse osutaja tehtud riskihindamisel või muul kättesaadaval riskialasel teabel; lõike 10 punkti 4 kohaselt kannab auditeeritav teenuse osutaja sihipärase turvaauditi kulud, juhul kui Riigi Infosüsteemi Amet otsustab põhjendatud juhul teisiti. Palume eelnõu seletuskirjas selgitada turvaauditi seost korrakaitseseadusega. Riiklik ja haldusjärelevalve on korrakaitse ja selle tegemisel tuleb lähtuda korrakaitseseadusest või juhul, kui see on sätestatud eriseaduses, eriseadusest.	Selgitatud Riiklik järelevalve toimub korrakaitseseaduse alusel, kuid haldusjärelevalve toimub Vabariigi Valitsuse seaduse, mitte korrakaitseseaduse alusel. Avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17. Sihipärase turvaauditi teemad on edaspidiselt riikliku järelevalve korral KüTS § 16 lõike 1^1 punkti 2 ja lõikesse 1^2 ning § 17 lõike 1^1 punkti 2 ja lõikesse 1^2. Mõlema paragrahvi lõike 1^2 alusel kehtestatakse ka ministri määrus, mis sihipärase turvaauditi temaatikat täpsustab. Seoses võimalike avalik-õiguslike ülesannete delegeerimisega selgitame, et sihipärane turvaaudit on välise osapoole (IT-audiitori) hinnang auditeeritava üksuse küberturvalisuse meetmetele. Selle läbiviimise korraldus on paika panemisel, kuid kui see peaks lahenduma nii, et Riigi Infosüsteemi Amet tellib selle hinnangu audiitorilt, kuid see hinnang ei ole Ametile siduv. Amet kasutab seda hinnangut enda edasises järelevalve menetluses ja otsustab selle pinnalt nt ettekirjutuse tegemise vajaduse, kuid järelevalve teostamise õigus ja pädevus, mis kujutab endast avaliku ülesande täitmist, jääb siiski Ametile. Seega avaliku ülesande delegeerimist välisele osapoolele ei toimu. Seetõttu ei toimu IT-audiitoritega ka halduslepingu sõlmimist, vaid need audiitorid,

	Korrakaitseseaduses on sätestatud üldmeetmed, mida korrakaitseorgan võib kohaldada, ja erimeetmed, mida korrakaitseorgan võib rakendada juhul, kui seda näeb ette eriseadus, ning selle seaduse § 24 kohaselt on korrakaitseorganil lubatud kohaldada riikliku järelevalve erimeedet ohu ennetamiseks, kui ohuprognoosile tuginedes saab pidada võimalikuks olukorda, mille realiseerumisel tekib oht. Riikliku järelevalve erimeetmena tuleb ilmselt käsitada ka turvaauditit. Samas korrakaitseseadus sellist meedet ette ei näe. Seega tuleb turvaaudit selgesõnaliselt erimeetmena eelnõus välja tuua ja selle kohaldamise õiguslikke aluseid eelnõus korrakaitseseaduses sätestatud teiste erimeetmete eeskujul oluliselt täpsustada. Samuti tuleb kooskõlas korrakaitseseadusega sätestada, et eelnõus sätestatud riskihindamine või muu kättesaadav riskialane teave on ohuprognoos ja selle koostamisel tuleb järgida korrakaitseseaduse asjakohaseid nõudeid. Lisaks palume asjakohaselt kas seletuskirjas või eelnõus täpsustada, kas tegemist on riikliku järelevalve käigus kasutatava sellise erimeetmega, mille puhul kaasatakse kolmas isik (Riigi Infosüsteemi Amet ostab turvaauditi tegemise audiitorilt) või teeb turvaauditi Riigi Infosüsteemi Amet ise. Esimesel juhul on oluline, et kolmandal isikul (audiitoril) oleksid meetme kasutamiseks järelevalveametnikuga samad õigused. Nendeks õigusteks on ilmselt dokumentidega tutvumine (§ 30) ja valdusesse	kelle teenuseid Amet hakkab tulevikus kasutama, leitakse riigihanke teel, ning nendega sõlmitakse eraõiguslikud teenuse osutamise lepingud.

	sisenemine (§ 50) jmt ning need õigused tuleks eelnõus ka ette näha. Audiitori tehtava turvaauditi puhul on oluline ka see, et kui eelnõu ja direktiivi (EL) 2022/2555 artiklitest 32 ja 33 võib järeldada, et turvaauditi tegemine on avalik-õiguslik ülesanne, siis tuleb eelnõus muu hulgas täpsustada audiitori valimise korraldust ja turvaauditi tegijaga halduslepingu sõlmimisega seonduvat. Lisaks, kui turvaaudit on iseloomult avalik-õiguslik ülesanne, siis tuleks seaduse tasandil kehtestada ka selle eest tasutava avalik-õigusliku tasuga seonduv, et eelnõu oleks põhiseadusega kooskõlas. Selgete aluste sätestamine on oluline õigusselguse saavutamiseks ning annab normiadressaadile aimu, millal tekib talle rahaline kohustus, kui suur see on ning ühtlasi on tal võimalik vastavad vahendid kavandada enda eelarves.	
8. Siseministeerium kooskõlastab märkustega 10.02.2025 kiri nr 1-7/279-5		
8.1	Eelnõu sätestab teenuse osutaja juhtorganile kohustuse läbida korrapäraselt erikoolitusi. Siseministeeriumi hinnangul on juhtorgani liikmete koolituste kohustus samm õiges suunas, kuid koolituste sisu ja kvaliteet on jäetud määratlemata. Samuti puudub selgus, kuidas koolituste läbimist jälgitakse. Tekib küsimus, mida tähendab, et teenuse osutaja juhtorgani liige peab läbima korrapäraselt erikoolitusi, mille õpiväljunditeks on piisavate teadmiste ja oskuste omandamine, et mõista ja hinnata küberturvalisuse riske, nendest tulenevat	Vt Rahandusministeeriumi kommentaari 6.1 vastust.

	mõju teenuse osutaja osutatavatele teenustele ning viise riskide käsitlemiseks? Siseministeeriumi hinnangul peab juhtorgani kohustuste osas olema seletuskirjas erikoolituse õpiväljundid detailsemalt lahti kirjeldatud.	
8.2	Samuti ei ole välja toodud erikoolituse vajaduse ajaline kriteerium. Kuivõrd NIS2 direktiiv ei määratle, mis on erikoolituste läbimise välp ehk mis aja tagant tuleks taolisi koolitusi teha, siis õigusselguse tagamiseks teeb Siseministeerium ettepaneku määrata koolituse läbimise välbaks 3 aastat, kuna ka E-ITSis (Eesti infoturbestandard) määratletud audititsükkel on käesolevalt 3 aastat.	Vt Rahandusministeeriumi kommentaari 6.1 vastust.
8.3	Eelnõu § 7 lg 2 punktid 1-3 näevad ette teenuse osutajale kohustused turvameetmete rakendamisel. Käesolevalt on turvameetmete rakendamine kirjeldatud E-ITSis, mis annab juhtkonnale kaalutlusõiguse erinevate meetmete rakendamise ulatuses. Palume eelnõu seletuskirjas välja tuua hinnang kõigi turvameetmete rakendamisega lisanduvate kulude osas, et oleks võimalik planeerida eelarvelisi kulutusi.	Selgitatud Eelnõu ei eelda ega tekita kohustust kõiki turvameetmeid rakendada. Valitakse ja rakendatakse need turvameetmed, mis on konkreetsel juhul asjakohased. Pealegi, kui tegemist on avaliku sektori asutusega, siis siin ei saa tekkida vastavale asutusele kui Eesti infoturbestandardi kohuslasele kulutusi, kuna eelnõuga ei tekitata võrreldes kehtivate nõuetega uusi nõudeid turvameetmete kontekstis. Kui asutus ei ole senini järginud kehtivat õigust (st KüTSi ja selle alusel antud määrusi), siis see ei ole siinse eelnõuga kaasnev mõju. Vt ka Rahandusministeeriumi kommentaari 6.5 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust.
8.4	Siseministeerium nõustub, et subjektide laiendamine on vajalik, kuid suurenev subjektide hulk toob kaasa järelevalve ja nõustamise mahu kasvu, mis võib ületada RIA võimekuse. On risk, et järelevalve ja toe pakkumise võimekus väheneb. Tekib küsimus, kas RIA-l on piisavalt ressursse uute nõuete täitmise tagamiseks? Kuidas planeerib RIA teha nii suurele subjektide arvule järelevalvet? Nimelt on täna subjektide arv väga suur ja	Selgitatud Riigi Infosüsteemi Ametile avalduvate mõjude ja vajaduste osa on kirjeldatud Ameti enda sisendi põhjal ning see on leitav eelnõu seletuskirjast. Eelnõu näeb ette, et Amet teostab järelevalvet riski- ja ohuprognoosipõhise lähenemisviisi alusel (vt eelnõu KüTS § 14 lg 6 punkti 1). Eesti infoturbestandardi auditeerimise ja audiitorite võimaliku vähesuse osas vt ka Rahandusministeeriumi kommentaari 6.5 vastust ning Sotsiaalministeeriumi kommentaari 9.1 vastust.

	audiitorid ei jõua E-ITSi auditeid teha, siis kuidas on tagatud efektiivne ja pidev järelevalve tegevus? Siseministeerium teeb ettepaneku hinnata nimekirja laiendamise tegelikku mõju järelevalveasutusele.	
8.5	Eelnõu [KüTS] § 8^1 lõike 1 ja 2 kohaselt Riigi Infosüsteemi Ametile (edaspidi RIA) võib: 1) teenuse osutaja teavitada küberintsidendist, nõrkusest ja küberohust; 2) muu isik kui teenuse osutaja teavitada olulise mõjuga küberintsidendist, nõrkusest ja küberohust. Sätte sõnastusest jääb ebaselgeks, miks on vabatahtliku teavitamise võimalus sätestatud seaduses just RIA suunal. Kui eesmärgiks on teadlikult luua konkreetne teabevahetuse ahel, tuleks kaaluda ka võimalusi, kuidas RIA saaks kogutud informatsiooni edastada asjakohastele partnerasutustele, nagu Politsei- ja Piirivalveamet (edaspidi PPA), Kaitsepolitseiamet või Andmekaitse Inspektsioon.	Selgitatud NIS2 direktiivi artikli 30 lõike 2 kohaselt peavad liikmesriigid vabatahtliku teavitamise puhul järgima direktiivi artiklis 23 sätestatud menetluskorda. Kuna viimane on lahutamatult seotud pädeva asutuse e Riigi Infosüsteemi Ameti ülesannetega, on tegemist ilmselt ainsa mõistliku lahendusega. KüTS § 8^1 alusel esitatud teave kantakse KüTS §-ga 13 asutatud küberintsidentide registrisse. Sama registri põhimääruses on sätestatud, kuidas ja kellele vastavat teavet edastatakse. Siin vt ka eelnõu seletuskirja lisaks oleva määruste kavandite puhul küberintsidentide registri põhimääruse muudatuste kavandit.
8.6	NIS2 direktiivi põhjenduspunktis 106 sätestab, et direktiivi alusel nõutava teabe esitamise lihtsustamiseks ja üksuste halduskoormuse vähendamiseks peaksid liikmesriigid asjakohase teabe esitamiseks ette nägema tehnilised vahendid, nagu ühtne kontaktpunkt, automatiseeritud süsteemid, veebipõhised vormid, kasutajasõbralikud liidesed, teatevormid, spetsiaalsed platvormid, mida üksused saavad kasutada, olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse. PPA on täna	Selgitatud Kommentaari puhul jääb segaseks, mil moel Politsei- ja Piirivalveamet saab küberintsidentide osas kontaktpunktiks, kuid Riigi Infosüsteemi Amet on ja jääb peamiseks kontaktpunktiks Euroopa Liidu Küberturvalisuse Ameti ehk ENISA suhtes.

	koos RIA-ga saamas küberintsidentide osas kontaktpunktiks. Antud kontekstis tekib küsimus, et kuidas ja mismoodi oleks mõistlik ühtset kontaktpunkti Eestis luua ja lisaks ei selgu, et mis õigusnormid juurde tulevad, mis täpsed kohustusi, mis mahus ja mis eelarvelisi vahendeid see asutuselt nõuaks PPA küberüksuselt. Siseministeerium teeb ettepaneku, et juhtivaks kontaktiks ENISA-le jätta RIA. PPA oleks toetav osapool ning protseduurid lepitakse eraldi kokku.	
8.7	Eelnõu [KüTS § 8 lõikes] 4^2 on edaspidi vaja RIA taotlusel esitab teenuse osutaja vahearuande olulise mõjuga küberintsidendi lahendamise seisu kohta. Siseministeerium teeb ettepaneku täiendada seletuskirjas vahearuande eesmärki, sisu, ajalist raami (nt nädala jooksul pärast intsidenti) ja kirjutada soovitud sisu lahti sarnaselt intsidenditeatele.	Selgitatud NIS2 direktiivi artikli 23 lõike 4 punkti c kohaselt tuleb asjakohasel üksusel teavitada CSIRTile või asjakohasel juhul pädevale asutusele CSIRTi või selle pädeva asutuse taotlusel vahearuande „vaatlusaluste asjade seisu kohta“. Selle esitamise ajaraam on sama artikli lõike punktide c-e kohaselt üks kuu pärast küberintsidendist teavitamist (eeldusel, et pädev asutus või CSIRT ei ole vahearuannet ise küsinud), kuna selleks tähtajaks peaks esitama lõpparuande. Vahearuande sisu on oma olemuselt sama, mis on lõpparuanne (eelnõus raport), kuna kui intsidendi lahendamine kestab, siis direktiivi kohaselt on lõppraport käsitatav vahearuandena. Sarnane loogika on ka eelnõus. Eelnõu on ka täiendatud, et Riigi Infosüsteemi Ameti taotlusel esitab teenuseosutaja enne lõppraporti esitamist vahearuande olulise mõjuga küberintsidendi lahendamise seisu kohta. Vahearuandes esitatakse samad andmed, mis esitatakse esmases teavituses ja asjakohasel juhul Riigi Infosüsteemi Ameti taotletud lisateave.
8.8	Eelnõus on välja toodud, et mõju majandustegevusele ja riigiasutustele on teatav ja sellest tulenevalt palume veelkord mõelda ja kaaluda täiendavaid rahastusallikaid NIS2 rakendamisele, sest varasemalt Eesti infoturbe standardi rakendamisel on MKM öelnud, et mõju puudub, kuid tegelikkuses on auditi hind märkimisväärselt kõrgem eelnõu seletuskirjas	Selgitatud Sellekohane teave on leitav seletuskirja 7. peatükis. Vt ka Rahandusministeeriumi kommentaari 6.5 vastust, Siseministeeriumi kommentaari 8.3 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust.

	pakutuga ja infoturbe personali halduskoormus ebamõistlikult suur.	
8.9	Juhime tähelepanu asjaolule, et kolme aasta jooksul ei ole lahenenud audiitorite vähesuse probleem, mis toob tulevikus suure tõenäosusega kaasa auditi hangete ebaõnnestumisi ja märkimisväärse hinnatõusu. Lisaks ei jätku kõikidele subjektidele audiitoreid, sest E-ITS auditeid peab tegema 3 aastase tsükliga ja iga aasta peaks pea kõikidele subjektidele tegema auditi. Riigil ei ole mõistlik tekitada olukorda, kus subjektid rikuvad tahtmatult seadust (ei suuda auditi kohustust täita endast mitteolenevatel põhjustel).	Vt Rahandusministeeriumi kommentaari 6.5 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust.
9. Sotsiaalministeerium kooskõlastab märkustega 20.02.2025 kiri nr 1.2-3/3139-4		
9.1	Nõustume, et küberturvalisus on tähtis komponent nii tervishoiuteenuste osutamise toimepidevuse tagamisel kui ka patsientide andmete kaitsmisel. Viimastel aastatel oleme oma haldusalas põhjalikult tegelenud tervisesüsteemi, sealhulgas esmatasandi toimepidevuse tugevdamise ning teenuste osutamise jätkusuutlikkusega. Elutähtsa teenuse osutajaks saavad mõned perearstid, nii et kõigile perearstidele samaväärsete küberturvalisuse nõuete kehtestamine ei ole mõistlik. Seega palume eemaldada küberturvalisuse seadusest kohustused perearstide kohta, kes ei ole elutähtsa teenuse osutajaks. 2024. aasta oktoobris jõustunud hädaolukorra seadusega laiendati elutähtsa teenuse osutajate ringi ning tervishoiuteenuste toimimise tagamise kohustusele lisandus ka ravimitega varustatuse	Mittearvestatud 26.05.2025. a toimus Justiits- ja Digiministeeriumi, Sotsiaalministeeriumi ning Eesti Perearstide Seltsi vahel kohtumine, kus selgitati ja lepiti kokku, et siinset muudatust (jätta välja need perearstid, kes ei ole elutähtsa teenuse osutajad) ei tehta. Samal kohtumisel selgitati, et siinse eelnõuga paralleelselt on Justiits- ja Digiministeeriumil ettevalmistamisel ka KüTS § 7 lõike 5 alusel kehtestatud „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruse muudatus, mis muudab ka kriteeriume, millal mingi üksus peab kohaldama Eesti infoturbestandardit või selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001 (vt eelnõude infosüsteemi toimikut 25-0715). Kui üksus ei pea kumbagi standardit rakendama, siis on tal jätkuvalt vajalik täita üldisemad ehk esmased nõuded, mis ei ole niivõrd detailsed kui eelmainitud standardid. Neid nõudeid (esmased turvameetmed) peavad ära täitma kõik KüTSi teenuseosutajad. Eelnõuga täiendatakse KüTSi subjektide ringi ainult nende üksustega, kes on NIS2 direktiivis nimetatud. Täiendavate teenuseosutajate lisandumist (või isegi nende välja võtmist) KüTSi saab analüüsida KüTSi muutva väljatöötamiskavatsuse käigus.

	kindlustamine. Seega kavandatakse elutähtsa teenuse osutajana hõlmata lisaks kiirabidele ja haiglavõrgu arengukava haiglatele nii teatud perearstid, üldapteegid kui ka ravimite hulgimüüjad. Praegu puudub vajadus nimetada küberturvalisuse seaduses elutähtsa teenuse osutajatele lisaks veel perearstiabi pakkujaid, kes elutähtsa teenuse osutajateks ei ole. Seega palume eelnõust välja jätta neid puudutavad sätted (§ 1 lg 1^5 p 9 ja § 3 lg 1^3 p 3, eelnõu § 1 p 1 ja 16). Tervishoiusüsteemi toimepidevus põhineb kinnitatud ning ajas täieneval elutähtsa teenuse osutajate võrgustikul. Seejuures jääb kõigile perearstiabi osutajatele endiselt senine kohustus kehtima - järgida kokkulepitud infoturbe baasnõudeid. Nimelt on Tervisekassa üldarstiabi rahastamise lepingu tingimustes toodud nõue, et tervishoiuteenuse osutajad (siinkohal perearstiabi osutajad) lähtuvad infoturbe korraldamisel juhendist „Baasturbe meetmed perearstidele“, mis tehakse kättesaadavaks Tervisekassa kodulehel. Kindlasti jäävad toimima ka senised muud meetmed, nagu teenuse osutajate teadlikkuse tõstmine läbi täiendavate koolituste ja valdkondlike juhiste.	
10. Välisministeerium 07.02.2025 kiri nr 15.1-3/7613-1		
10.1	Eelnõu § 1 punktiga 26 muudetakse küberturvalisuse seaduse(edaspidi *KüTS*) § 7 lõiget 2. KüTS § 7 lg 2 punkti 7 kohaselt on teenuse osutaja turvameetmete rakendamisel kohustatud tagama süsteemi hankimise, arendamise ja	Selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid).

	hooldamise turvalisuse, sh nõrkuste käsitlemise ning avalikustamise. Sellises sõnastuses võib sätet mõista kui kohustust avalikustada süsteemi nõrkused, mis viib olukorrani, kus on avalikustatud teave, mis võimaldab teostada asutuse vastu edukat küberrünnet. Palume muuta sätte sõnastust selliselt, et teabe avalikustamise kohustus ei tekitaks või lisaks juurde otsest ohtu teenuse osutaja süsteemidele. Pakume välja järgmise sõnastuse: „7) tagama süsteemi hankimise, arendamise ja hooldamise turvalisuse, sh nõrkuste käsitlemise ning avalikustamise selliselt, et ei lisandu juurde uusi ohtusid;“. Ühtlasi juhime tähelepanu, et eelnõu § 1 punktiga 26 muudetakse KüTS § 7 lõiget 2 tervikuna, mitte üksnes lõike 2 punkte 1-3 nagu on kirjas muutmiskäsus.	Kommentaaris mainitud p 7 osas selgitame, et tolle sõnastamisel lähtuti lähtutud NIS2 direktiivi artikli 21 lõike 2 punkti e sõnastusest ja mõttest. Eelnõu KüTS § 7 lõike 2 muutmiskäsu sõnastus on üle vaadatud ja muudetud.
10.2	Eelnõu § 1 punktiga 33 täiendatakse KüTS § 8 lõikega 4^1, milles sätestatakse, millised andmed tuleb võimaluse korral olulise mõjuga küberintsidendi teavituses esitada. KüTS § 8 lg 4^1 punkti 1 kohaselt on selleks mh teave olulise mõjuga küberintsidendi sisu ja toimumise põhjuse kohta, sh asjakohasel juhul teave turvarikkemärgi kohta. Termin „turvarikkemärk“(inglise keeles *Indicator of Compromise*) ei ole defineeritud ning selle tähendus on ebaselge. Teeme ettepaneku sõnastada säte selliselt, et oleks üheselt arusaadav, mida sisuliselt soovitakse. Pakume välja järgmise sõnastuse: „1) teave olulise mõjuga küberintsidendi sisu ja toimumise põhjuse	Selgitatud Turvarikkemärgi (inglise keeles *indicator of compromise*) puhul on tegemist igasuguse tunnusega, mis viitab rikkumise toimumisele. NIS2 direktiiv ei tekita vastavat mõistet, mistõttu seda eraldi ei defineerita eelnõuga. Selle asemel on seda selgitatud seletuskirjas vastava sätte juures.

	kohta, sealhulgas asjakohasel juhul teave küberintsidenti tuvastada võimaldavate märkide kohta;“.	
10.3	Eelnõu § 1 punktiga 39 täiendatakse KüTSi §-ga 8^1, mis puudutab küberintsidendist, nõrkusest ja küberohust vabatahtlikku teavitamist. Kavandatava KüTS § 8^1 lõike 2 teise lause kohaselt on anonüümselt esitatud teate esitaja isik asutusesiseseks kasutamiseks mõeldud teave. Lause sellise sõnastuse puhul ei ole arusaadav, mida on mõeldud teate anonüümselt esitamise all, sest teate esitaja isik on teada. Palume sõnastada säte selgemalt. Pakume välja järgmise sõnastuse: „(2) Potentsiaalsest nõrkusest või nõrkusest teavitav füüsiline või juriidiline isik võib esitada teate anonüümselt. Seejuures tuleb kasutusele võtta piisavad meetmed, mis tagavad teate esitaja anonüümsuse.“.	Selgitatud Siin ei ole eesmärk tekitada olukorda, kus vastavaid teateid saaks esitada ainult anonüümselt. Siin vt ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.55 vastust.
10.4	Juhime tähelepanu, et direktiivi 2022/2555 preambuli punkti 8 kohaselt ei kohaldata direktiivi liikmesriikide diplomaatiliste ja konsulaaresinduste suhtes kolmandates riikides ega nende võrgu-ja infosüsteemide suhtes, kui sellised süsteemid asuvad esinduse ruumides või kui neid käitatakse kolmanda riigi kasutajate jaoks. Palume nimetatud erisus viia sisse ka KüTSi, täiendades eelnõuga vastavalt KüTS § 1 lõiget 2.	Arvestatud
10.5	Direktiivi 2022/2555 preambuli punkt 9 kohaselt ei tohiks direktiivist tulenevalt kohustada liikmesriike esitama teavet, mille avalikustamine on vastuolus nende riigi julgeoleku, avaliku julgeoleku või kaitse oluliste huvidega. Kõnealuses kontekstis	Selgitatud Kui kommentaar on mõeldud selle kohta, mida Riigi Infosüsteemi Amet võib teiste riikide partnerasutustele, Euroopa Liidu Küberturvalisuse Ametile või Euroopa Komisjonile esitada, siis kommentaaris viidatud põhjenduspunktiga seonduvalt on ette nähtud KüTS § 12 lg 4. Lisaks märgime, et tol teemal parandatakse eelnõuga ka KüTS

	tuleks arvesse võtta salastatud teabe kaitset käsitlevaid riigisiseseid ja liidu norme, ametlikke ja mitteametlikke mitteavaldamise kokkuleppeid, nagu fooritulede analoogial põhinev fooriprotokoll teabe tundlikkuse märgistamiseks. Leiame, et on oluline vältida võimalikku vastuolu KüTSi ja avaliku teabe seaduse (edaspidi *AvTS*) vahel. Välisministeeriumi hinnangul võib see tekkida nt AvTS§ 35 lg 1 punktis 3 kehtestatud kohustuse (tunnistada asutusesiseseks kasutamiseks mõeldud teabeks teave, mille avalikuks tuleks kahjustaks riigi välissuhtlemist) ning KüTSis kehtestatud teabe esitamise ja avalikustamise kohustuste puhul. Tulenevalt eeltoodust teeme ettepaneku sätestada eelnõuga teabe esitamist ja avalikustamist puudutav erisus avaliku teabe seaduse §-s 34 nimetatud teabe osas.	§ 12 lõike 5 sõnastust. Kui kommentaar on mõeldud KüTS § 17[5] alusel toimuva küberturvalisuse alase teabevahetuse kokkuleppe osas, siis juhime tähelepanu, et too teabevahetus toimub vabatahtlikkuse alusel. Samuti on avaliku teabe seaduses ette nähtud, et teabevaldaja juht saab ise otsustada, kellele asutusesiseseks kasutamiseks mõeldud teavet jagatakse - vt tolle seaduse § 38 lõiget 4.
11. Eesti Linnade ja Valdade Liit kooskõlastab märkuste ja ettepanekutega 04.02.2025 kiri nr 5-1/511-2		
11.1	Seletuskirjas lk 135 on kirjutatud, et on võimalik, et auditeerimiskulud on majanduslikult koormavamad subjektidele, kelle IKT korraldus on oluliselt väiksema mahuga, kuivõrd ühine lävend ja seega ka minimaalne kulu auditi teenuse läbiviimises tuleneb protseduurist auditi läbiviimisel, kvalifikatsiooninõuetest auditi läbiviijale ning auditi käigus koostatava dokumentatsiooni nõuetest ning selgitatakse, et erand on kavandatud konkreetselt auditite läbiviimise kohustuse suhtes, mitte Eesti infoturbestandardi järgimise kohustuse suhtes.	Võetud teadmiseks ja selgitatud Kuna esitatud ettepanek on seotud KüTS § 7 lõike 5 alusel antud määrusega, mitte seaduseelnõuga, siis võtame ettepaneku teadmiseks. Siinse eelnõuga paralleelselt on Justiits- ja Digiministeeriumil ettevalmistamisel ka KüTS § 7 lõike 5 alusel kehtestatud „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruse muudatus (vt eelnõude infosüsteemi toimikut 25-0715), mis muudab ka kriteeriume, millal mingi üksus peab kohaldama Eesti infoturbestandardit või selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001. Kui üksus ei pea kumbagi standardit rakendama, siis on tal jätkuvalt vajalik täita üldisemad ehk esmased nõuded, mis ei ole niivõrd detailsed kui eelmainitud standardid. Neid nõudeid (esmased turvameetmed) peavad ära täitma kõik KüTSi teenuseosutajad.

	Eelnõu üheks lisaks on ka Vabariigi Valitsuse määruse muutmise kavand, mille puhul on võimalik tolle määruse avalikul kooskõlastusringil anda tagasisidet, kas ja kuidas tuleks Eesti infoturbestandardi auditi tegemise kohustust või selle vabastust sõnastada. Juhime tähelepanu, et täna kehtiv VV määrus Võrgu- ja infosüsteemide küberturvalisuse nõuded (09.12.2022 nr 121) § 4 lg 4 p 2 nimetab organisatsioonid, millele ei kohaldata E-ITS auditeerimise kohustus: *„ 2) riigimuuseumile, avalik-õigusliku isiku muuseumile,* ***valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavalla või linnaosa ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele ning kohaliku omavalitsuse üksuste ühisametile ja -asutusele****, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga;“.* Esitatud punktis rõhutatud tekst kordab otseselt KüTS § 3 lg 4 p 13 sätestatut. Teeme ettepaneku lisada VV määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (09.12.2022 nr 121) § 4 lg 4 p 2 nimekirja ka **kohaliku omavalitsuse üksuste liit** ehk punkt sõnastada järgmiselt: *2) riigimuuseumile, avalik-õigusliku isiku muuseumile, valla või linna ametiasutusele, valla või linna ametiasutuse hallatavale asutusele, osavalla või linnaosa ametiasutusele, osavalla või linnaosa ametiasutuse hallatavale asutusele,*	Eelnõuga täiendatakse KüTSi subjektide ringi ainult nende üksustega, kes on NIS2 direktiivis nimetatud. Täiendavate teenuseosutajate lisandumist (või isegi nende välja võtmist) KüTSi saab analüüsida KüTSi muutva väljatöötamiskavatsuse käigus.

	*kohaliku omavalitsuse üksuste ühisametile ja -asutusele **ning kohaliku omavalitsuse üksuste liidule**, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga.* Seda põhjusel, et kui kohaliku omavalitsuse üksuste liit ei ole andmekogu vastutav töötleja või volitatud töötleja ehk tema IKT korraldus on oluliselt väiksema mahuga, pole vajadust liitu E-ITSi rakendamisel auditeerida, sest auditeerimisprotsessid nõuavad ülemäärast ressursi ja aja kulutamist. Kohaliku omavalitsuse üksuste liidu peamine eesmärk on olla tugiorganisatsiooniks ja esindada kohalike omavalitsuste ühishuve, mitte hallata andmekogusid. Kui nad viimast teevad, siis põhjusel, et kohalikud omavalitsused on liidule vastava ülesande andnud ja sel juhul on auditeerimine põhjendatud.	
11.2	Ühtlasi teeme ettepaneku jätta sama punkti lõpust välja lauselõpp: „kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga“. Selline muudatus vähendaks oluliselt auditikohuslaste hulka. Praegu teadaoleva info kohaselt ei jätkuks kõigi auditikohuslaste auditeerimiseks audiitoreid ja auditeerimise nõuet pole kõigil võimalik täita. Lisaks võib algne sõnastus soodustada määruse täitmisest kõrvale hoidmist selliselt, et muudetakse asutuse põhimääruses asutus andmeandjaks või lepinguliseks töötlejaks, kuigi tegelikult ollakse vastutav töötleja.	Võetud teadmiseks ja selgitatud Kuna esitatud ettepanek on seotud KüTS § 7 lõike 5 alusel antud määrusega, mitte seaduseelnõuga, siis võtame ettepaneku teadmiseks. Vt ka eelmisele märkusele antud selgitust.

	Väljajäetav tekstiosa muudaks auditeerimise kohustuse selgemaks ja reaalselt täidetavaks ning nõuetest kõrvalehoidmine oleks ebavajalik.	
11.3	Samuti teeme ettepaneku lisada seletuskirja näiteid, millisel puhul on asutus „volitatud töötleja“ ja millisel „andmeandja“, nii nagu andmeandja mõistet on mõtestatud AvTS § 43^5 lõikes 2.	Võetud teadmiseks ja selgitatud Kui esitatud kommentaar on esitatud seaduseelnõule, siis seletuskirjas on uuendatud eelnõu KüTS § 3 selgitustes kirjeldatud, mida selle all mõeldakse, sh keda peetakse avaliku teabe seaduse tähenduses „volitatud töötlejaks“. Samuti ka seda, kuidas see erineb isikuandmete kaitse valdkonnas olevast isikuandmete volitatud töötlejast. Andmeandja osas annab selgituse KüTS § 13 lõikega 1^1 lisatav täiendus. Kui esitatud kommentaar on KüTS § 7 lg 5 alusel antud Vabariigi Valitsuse määruse muutmise kavandile, siis esitatud märkus on võetud teadmiseks.
12. Riigikogu Kantselei 30.01.2025 nr 1-6/24-151/2		
12.1	Riigikogu Kantseleil ei ole eelnõu kohta sisulisi märkusi. Juhime tähelepanu, et KüTS-i § 7 lõike 2 muutmisel ei muudeta vaid lõike esimest kolme punkti, nagu eelnõus ekslikult sätestatud, vaid kogu lõiget, milles on muudatuse järel 14 punkti.	Võetud teadmiseks
12.2	Küsitud tagasiside osas KüTS-i § 17^1 muudatuse kohta (sunniraha) toetame eelnõus sätestatud varianti.	Võetud teadmiseks
13. Riigikohus ei soovinud arvamust avaldada 27.01.2025 e-kiri		
14. Andmekaitse Inspektsiooni arvamus 23.01.2025 kiri nr 2.3-4/25/3148-2		
14.1	Eelnõu seletuskirja KüTS § 19 lg 2 puudutavas osas ootavad eelnõu koostajad tagasisidet, kas sarnane teavitus peaks olema ka KüTS §-des 18^5 ja 18^6 sätestatud väärtegude korral või mitte. AKI mõistab eelnimetatud koosseise selliselt, et ka nende väärtegude puhul, kus on tegemist piiriüleste	Arvestatud

	elektrivoogude olukorraga, võib kaasneda isikuandmetega seotud rikkumine, millest tuleb AKI-t teavitada IKÜM art 33 kohaselt. Kui see nii on, siis võiks NIS2 direktiivi art 35 lg-ga 1 sarnane teavitus toimuda ka KüTS §-des 18^5 ja 18^6 sätestatud väärtegude puhul. Kuigi vastutav töötleja on kohustatud isikuandmetega seotud rikkumisest AKI-it IKÜM art 33 järgi teavitama, ei pruugita seda igakord teha.	
14.2	Seletuskirja p-s 7.4 on märgitud, et ettevalmistamisel on analüüs intsidentidest teavitamise kohta mitmele pädevale asutusele nö ühe akna kaudu. Palume selle analüüsi valmimisel seda kindlasti jagada ka AKI-ga.	Võetud teadmiseks
15. Finantsinspektsiooni arvamus 28.01.2025 kiri nr 5-8/6699-2		
15.1	*KüTS-i kohaldumine ja mõju FI-le* Kehtiva KüTS § 3 lõike 4 punkti 3 kohaselt kohaldatakse KüTS-is teenuse osutaja kohta sätestatut Eesti Pangale. Finantsinspektsiooni ei ole KüTS § 3 lõikes 4 nimetatud. Eelnõu § 1 punktiga 20 tunnistatakse viidatud lõige kehtetuks, kuna kehtetuks tunnistatava lõike punktide sisu on viidud Eelnõuga KüTS § 1 lõike 1^3 punkti 7 (KüTS-i kohaldatakse keskvalitsuse avaliku halduse üksusele) kui ka lõikesse 1^5. Eelnõu § 1 punktiga 7 täiendatakse KüTS §-i 2 muu hulgas punktiga 1^2, mille kohaselt keskvalitsuse avaliku halduse üksus on üksuse üldnimetus, mille puhul on mõeldud üksustest Eesti Panka (edaspidi *EP*), Finantsinspektsiooni, kohtuasutust, riigi valimisteenistust, Riigikogu Kantseleid,	Selgitatud Uuendatud eelnõus on „keskvalitsuse avaliku halduse üksuse“ loetelust eemaldatud Finantsinspektsioon, mistõttu siinne kommentaar võetakse teadmiseks. Finantsinspektsiooni lisamist KüTSi teenuseosutajate, konkreetsemate nõuete ja sellega seotud võimalikke mõjusid on võimalik analüüsida KüTSi korrastamiseks kavandatava VTK raames.

	Riigikontrolli, Vabariigi Presidendi Kantseleid, valitsusasutust, valitsusasutuse hallatav riigiasutust ja Õiguskantsleri Kantseleid. Seletuskirja kohaselt on Eelnõu punkti 7 puhul tegemist ka kehtiva õiguse säilitamisega, kuna see mõiste hõlmab kehtiva KüTS § 3 lõike 4 punktides 3, 5, 6, 7, 8, 11, 12 ja 14 ning lisanduvalt nimetatakse siin ka Finantsinspektsioon, kelle puhul ei ole otseselt niivõrd selge, kas hetkel tema suhtes kehtib KüTS, mistõttu sarnaselt teiste üksustega on ta eraldi nimetatud siinse Eelnõuga. Täiendavalt on seletuskirjas selgitatud, et Finantsinspektsioon ei ole eraldiseisev juriidiline isik, vaid ta on Finantsinspektsiooni seaduse (edaspidi *FIS*) § 4 lõike 1 kohaselt „autonoomse pädevusega ja oma eelarvega EP juures asuv asutus, mille juhtimisorganid tegutsevad ja esitavad aruandeid FIS-is sätestatud korras. Eelnõu eesmärk on tagada Finantsinspektsiooni tegevuses kasutatavate võrgu- ja infosüsteemide ja andmete turvalisus, mistõttu on õigusselguse huvides eraldi välja toodud ka Finantsinspektsioon kui EP juures asuv asutus. Eelduslikult kohaldatakse küberturvalisuse nõudeid kõikide subjektide kõikidele struktuuriüksustele või nende juures asuvatele asutustele, kuid see punkt loetelus on loodud õigusselguse tagamise eesmärgil, sest Finantsinspektsioon on finantsjärelevalve teostamisel ja kriisilahendusülesannete täitmisel sõltumatu. Seletuskirja lk 130 kohaselt on Finantsinspektsioon täiesti uueks subjektiks KüTS-i tähenduses.	

	Eeltoodu valguses juhime tähelepanu, et seletuskirjas ei ole KüTS-i Finantsinspektsioonile kohaldamise mõjuanalüüsi, muuhulgas on seega jäetud hindamata Finantsinspektsiooni eripärane funktsioon finantsjärelevalve teostajana kui ka kriisilahenduse asutusena. Nimetatu on oluline, kuna Finantsinspektsioon kuulub neid funktsioone täites nii Euroopa ühtsesse järelevalvemehhanismi (SSM1) kui Euroopa ühtsesse kriisilahenduse korda (SRM2). Sellest tulenevalt ei ole lõpuni selge, kuidas kohalduvad KüTS-i nõuded nendele Finantsinspektsiooni tegevuses kasutatavatele võrgu- ja infosüsteemidele, mis on seotud Euroopa pangandusjärelevalve süsteemiga, kuhu ka Finantsinspektsioon kuulub. Märgime siinjuures, et KüTS-i nõuded ei saa hakata takistama järelevalve teostamist ja infovahetust SSM-i, SRB kui ka Euroopa järelevalveasutustega (edaspidi *ESA-d*: EBA3, EIOPA4 ja ESMA5). See puudutab muuhulgas ESA-de tasemel tsentraalselt ehitatavate andmekeskuste arendustegevust ja nendega seotud andmevahetust FI ja ESA-de vahel. Samuti ei nähtu, milline võib olla Finantsinspektsiooni täiendav kulu uute nõuete rakendamisel.	
15.2	Eelnõu § 1 punkti 1 kohaselt hakkab KüTS kohalduma kesksele vastaspoolele Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.07.2012, lk 1–59), artikli 2 punkti 1	Selgitatud Eelnõuga on soov lähtuda võimalikult suures ulatuses Euroopa Komisjoni suunistest direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta 2023/C 328/02. Seetõttu tehaksegi KüTS § 1 lõikes 4 muudatus. Need KüTSi kohaldamisalas olevad üksused, kellele kohaldub DORA määrus, lähtuvad DORA määrusest, sh siin ei teki ka seetõttu järelevalve osas topelt pädevusi Riigi

	tähenduses (KüTS § 1 lõike 1^2 punkt 28). Juhime tähelepanu, et Eestis neid subjekte hetkel ei ole, aga kui oleks, siis DORA määruse järgi oleks järelevalvemandaat FI-l. Seega tekiks KüTS-i alusel topeltjärelevalve. Samuti tekib KüTS-i kohaselt topeltjärelevalve krediidiasutuste suhtes (Eelnõu § 1 lõike 1^2 punkti 26 alusel) ja kauplemiskoja korraldajale väärtpaberituru seaduse tähenduses (Eelnõu § 1 lõike 1^2 punkti 27 alusel).	Infosüsteemi Ameti ja Finantsinspektsiooni vahel. Seda isegi siis, kui konkreetne üksus on elutähtsa teenuse osutajast krediidiasutus.
15.3	KüTS § 1 lõike 1^3 punkti 8 kohaselt kohaldatakse KüTS-i elutähtsa teenuse osutajale. KüTS § 3 lõike 1^2 punkti 6 kohaselt elutähtis üksus on elutähtsa teenuse osutaja. KüTS § 14 lõike 13 punkti 2 kohaselt on RIA-l õigus nõuda ettekirjutusega elutähtsa üksuse nõukogult või osanikelt juhatuse liikme volituste ajutist piiramist. Kuna elutähtsad üksused on ka krediidiasutused, tekib RIA ja FI pädevuste kattuvus nende krediidiasutuste suhtes (vt KAS § 104 lõige 1 punkt 9). RIA poolt vastavasisulise ettekirjutuse tegemine krediidiasutusele võib negatiivselt mõjutada krediidiasutuse tegevust ja juhtimist ning tervikuna võib omada olulist mõju riigi finantsstabiilsusele. Palume selgelt sätestada KüTS-is, et selle ettekirjutuse tegemise õigus kuulub FI-le ja RIA-l on õigus teha FI-le vastav ettepanek ettekirjutuse tegemiseks.	Vt Finantsinspektsiooni kommentaari 15.2 vastust.
15.4	Eelnõu § 1 punktiga 6 täiendatakse KüTS-i §-ga 1^1, mille lõike 5 kohaselt kui digitaalse teenuse osutajal on kohustus määrata digitaalse teenuse osutaja esindaja, kuid ta pole seda määranud	Selgitatud Eelnõu struktuuri on asjassepuutuvas osas muudetud ning varasema lõike 5 tekst üle vaadatud. NIS2 direktiivi pädevate asutuste (sh Riigi Infosüsteemi Ameti) järelevalvevolitused on praktikas seotud ennekõike Eesti territooriumiga, kuid järjest

	Euroopa Liidus, võib KüTS-is sätestatud nõudeid rikkuva digitaalse teenuse osutaja vastu õiguslikke meetmeid iga Euroopa Liidu liikmesriik, kus digitaalse teenuse osutaja enda teenuseid osutab. Eelkõige lauses on puudu tegusõna. Lisaks, kui eelduslikult peab õiguslikke meetmete rakendamine käima selle liikmesriigi kaudu, kus digitaalse teenuse osutaja esindaja on määratud, on küsitav, kas Eelnõuga pakutud sätte alusel saab, näiteks, Eesti RIA rakendada meetmeid Amazoni suhtes, kui Amazon ei ole määranud digitaalse teenuse osutaja esindajat Euroopa Liidus ja rikub KüTS-ist tulenevaid nõudeid?	enam on Euroopa Liidu õigusakte, mis seda järelevalvepädevust laiendavad (nt kui tuua paralleel isikuandmete kaitse üldmäärusega). Eelnõu KüTS §-s 4 toodud nn „jurisdiktsiooni ja territoriaalsust“ puudutavad sätted on üle võetud vastavalt NIS2 direktiivi artiklile 26 ning neis küsimustes Euroopa Liidu seadusandja liikmesriikidele paraku diskretsiooniõigust (mh osas, mis puudutab digitaalse teenuse osutaja peamise tegevuskoha tuvastamist ja sellest lähtuvalt meetmete võtmist) jätnud ei ole.
16. Maa- ja Ruumiameti arvamus 08.01.2025 kiri nr 1-10/24/15606-2		
16.1	Eelnõu punkti 19 kohaselt täiendatakse paragrahvi 3 lõikega 3^1 järgmises sõnastuses: *„(3^1) Teenuse osutaja ja domeeninimede registreerimise teenuseid osutav üksus esitab Riigi Infosüsteemi Ametile vähemalt järgmise teabe:* *1) nimi ja registrikood;* *2) aadress ja ajakohased kontaktandmed, sealhulgas e-posti aadressid, interneti protokolli aadresside vahemikud ja telefoninumbrid;* *…* Juhime tähelepanu, et paragrahvi 3 lõike 3^1 punkti 2 kohaselt tuleb teenuse osutajal ja domeeninimede registreerimise teenuseid osutaval üksusel Riigi Infosüsteemi Ametile esitada info aadressi suhtes. Eelnõust ega seletuskirjast ei selgu, millist aadressi on mõeldud. Kas soovitakse infot näiteks teenuse osutaja asukoha aadressi (nt äriregistri järgne	Vt Regionaal- ja Põllumajandusministeeriumi kommentaari 7.6 vastust.

	aadress), tegutsemiskoha aadressi või postiaadressi suhtes. Võimalusel palume eelnõu sõnastust selles osas täpsustada (vaata ka eelnõu punkti 21, § 4 lg 1 p 3 sõnastust).	
17. Riigi Infosüsteemi Ameti arvamus 31.01.2025 kiri nr 1.1-20/251955		
17.1	Eelnõu üleselt teeb Riigi infosüsteemi Amet ettepaneku kirjutada seaduses kasutatavad mõisted ja terminid lahti. Terminoloogiat puudutav osa tuleks esitada võimalikult selgelt seaduses ühes kohas ja üks kord. Euroopa Liidu õigusaktidele viitamise asemel palume kõik olulised terminid defineerida läbi Eesti õiguse vastava mõiste või seaduses lahti seletada. See lihtsustab teksti mõistmist ning sellisel juhul ei ole lugejal vajalik vasteid otsida Euroopa Liidu õigusaktidest.	Selgitatud Kui tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.2	Teeme ettepaneku läbivalt eelnõu [KüTS] § 1 lg 1 p 1^2 ja § 2 lg p 4^5 ning § 9 p 10 kasutavate mõistete „üksus“ ja „organ“ asemel kasutada näiteks tsiviilseadustiku üldosa seaduses (TsÜS) välja toodud isikute mõisteid – füüsiline, eraõiguslik ja avalik-õiguslik juriidiline isik või teenuse osutaja.	Vt Regionaal- ja Põllumajandusministeeriumi kommentaari 7.2 vastust.
17.3	Eelnõu [KüTS] § 1 lg 1^2 p 7 mõistet „laadimispunkti käitaja“ ei ole kehtivas elektrituruseaduses. Elektrituruseaduse (edaspidi ELTS) § 3 p 13^1 avab laadimispunkti mõiste. Laadimispunkti temaatikat on lisaks kirjeldatud ELTS §-s 74^{15}. Seega palume defineerida mõiste	Selgitatud Elektrituruseaduse muudatust siinse eelnõuga ei tehta. Too seadus defineerib ära „laadimispunkti“ ning „laadimispunkti käitaja“ ongi see üksus, kes käitab viidatud seaduse definitsiooni kohast laadimispunkti.

	„laadimispunkti käitaja“ läbi ELTS tähenduse, võimalusel ELTS muudatusena.	
17.4	Eelnõu [KüTS] § 1 lg 1^2 p 8 mõisteid „kaugkütte pakkuja“ ja „kaugjahutuse pakkuja“ ei eksisteeri kaugkütteseaduses. Seni on antud teenuse osutajaid nimetatud kaugkütteseaduse § 4 kohaselt mõistega „soojusettevõtja“.	Mittearvestatud ja selgitatud Soojusettevõtja" hõlmab kaugküttesaduse järgi ainult soojuse tootmise, jaotamise või müügi. Kaugjahutuse pakkujad peavad NIS2 direktiivi I lisa punkti 1 (b) kohaselt kohaldamisalasse kuuluma ning meile teadaolevalt on selline teenus juba täna Eesti turul olemas, olgugi et seda ei ole eriseadusega reguleeritud. Isegi juhul, kui mõni NIS2 direktiivis nimetatud subjekt/sektor täna Eesti kontekstis relevantne ei ole(ks), ei jäta direktiiv paraku liikmesriikidele diskretsiooniõigust selliseid subjekte kohaldamisalast välistada - seda näiteks juhuks, kui tulevikus peaks mõni vastav teenuseosutaja ka Eesti turul tegevust alustama.
17.5	Eelnõu [KüTS] § 1 lg 1^2 punktid 10-15 on võimalik läbivalt asendada maagaasiseaduse § 4 välja toodud „gaasiettevõtja“ mõistega.	Mittearvestatud ja selgitatud Eelnõus on võimalikul määral kasutatud NIS2 direktiivi lisades kasutatud sõnastusi.
17.6	Eelnõu [KüTS] § 1 lg 1^2 p 18 välja toodud „lennuettevõtja“ mõiste võiks olla defineeritud seaduses. Näiteks pakume definitsioonina: „Lennuettevõtja on kehtiva lennutegevusloaga või samaväärse loaga õhuveoettevõtja, kes tegeleb kommertsvaldkonnas.“.	Mittearvestatud ja selgitatud Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.7	Eelnõu [KüTS] § 1 lg 1^2 p-s 19 on välja toodud „lennujaama haldaja“ mõiste. Lennujaama haldaja on lennundusseaduses (edaspidi LennS) olemas, kuid teisi mõisteid pole. Mõiste „lennujaamas olevad abirajatised või abirajatis“ palume	Selgitatud Kommenteeritava sõnastuse puhul on võetud eeskuju NIS2 direktiivi lisast I. Vt ka Kliimaministeeriumi kommentaari 3.1 vastust.

	defineerida eelnevalt LennS-s, et tagada õigusselgus. Samuti palume seletuskirjas välja tuua kaalutlused, miks just need isikud/ettevõtted loetakse mõiste alla kuuluvaks.	
17.8	Eelnõu [KüTS] § 1 lg 1^2 p 20 välja toodud „lennuliikluskorraldusettevõtja“ mõistet täna Eesti õiguses sätestatud ei ole. Palume kaaluda selle asemel mõistet „lennujuhtimisteenust pakkuv ettevõtja“, mis mõiste sisu selgemalt avab.	Mittearvestatud ja selgitatud Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.9	Eelnõu [KüTS] § 1 lg 1^2 punktid 22-23 välja toodud „meretranspordi ettevõtja“ definitsiooni täna Eesti õiguses ei ole. Teeme ettepaneku kasutada terminit, mis on juba kehtivas õiguses olemas. Mõisted „sadama pidaja“ ja „sadamarajatis“ on sadamaseaduse § 2 p 3 ja p 9 defineeritud. Seega ei pea me vajalikuks lisada Euroopa Liidu õiguse viidet.	Mittearvestatud ja selgitatud Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.10	Eelnõu [KüTS] § 1 lg 1^2 punktid 48-50 ning eelnõu § 1 lg 1^3 p 1 võiks kaaluda näiteks „internetipõhise	Mittearvestatud ja selgitatud

	kauplemiskoha pakkuja“ asemel „internetipõhise teenuse osutaja“ kasutamist. Sama analoogiat võiks kasutada ka teiste välja toodud punktide subjektide osas.	Pärast kaalumist on eelnõu autorid seisukohal, et ettepaneku järgne muudatus tekitaks täiendavat õigusselgusetust (nt EL digiteenuste määruse kontekstis).
17.11	Eelnõus defineeritakse mõiste „nõrkus“ läbi nõrkuse (IKT-toote või-teenuse nõrkus). Palume defineerida mõiste „nõrkus“ eraldi. Näiteks infoturbestandardi ISO/IEC 27000 järgi defineeritakse seda kui vara või meetme nõrk koht, mille saab ära kasutada üks või mitu ohtu. Seega tuleks eelnõu [KüTS] § 2 punktides 3^1-3^9 teised mõisted üle vaadata ja ümber sõnastada, et ei tekiks uusi mõisteid, vaid kasutataks ja täiendatakse valdkonda reguleerivates õigusaktides juba kehtivaid samatähendusega mõisteid. Uue mõiste defineerimine võib tekitada segadust aastaid kehtinud ja juurutatud organisatsioonide infoturbe korraldustes.	Osaliselt arvestatud ja selgitatud Eelnõus on kooskõlastusringil saabunud tagasisidega ja sellele järgnenud arutelude tulemustega arvestades termin „nõrkus“ muudetud terminiks „turvahaavatavus“, kuid termini definitsioonis on kasutatud NIS2 direktiivi artikli 6 punktiga 15 rohkem kooskõlas olevat sõnastust.
17.12	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 2 p [1^1]. Eelnõu sõnastuse kohaselt on ka füüsiline isik asutatud.	Arvestatud
17.13	Teeme ettepaneku vaadata üle, kas on eraldi vaja mõistetena tuua eelnõu [KüTS] § 2 p 1^2 ning p 1^3 „keskvalitsuse avaliku halduse üksus“ ning „kohaliku tasandi avaliku halduse üksus“. Antud mõisteid on kasutatud eelnõu [KüTS] § 1^1 lg 2 p 3, § 3 lg 1^2 p 4, 5 § 14 lg 14 punktis 2 ning § 17^5 lg 4. Antud punktides saaks kasutada meie hinnangul ka loetelu asutustest, mille mõistet keskvalitsuse avaliku halduse üksus ja kohaliku tasandi avaliku halduse üksus koondab.	Mittearvestatud ja selgitatud – pärast kooskõlastusringil saabunud tagasiside kaalumist on eelnõu autorite hinnangul kõnealuste terminite kasutamine põhjendatud. Seletuskirja täiendatud: *“Termini „keskvalitsuse avaliku halduse üksus“ kasutamise võimalikkust ja mõistlikkust on eelnõu koostamise käigus korduvalt kaalutud ning otsitud sobivamaid alternatiive, kuna antud eelnõu kontekstis on tegemist NIS2 direktiivist pärit terminiga, mis on mõeldud ülevõtmiseks kõigile liikmesriikidele ja mis grammatiliselt ja tunnetuslikult eelkõige seondub föderatiivsete riikide õigusterminoloogiaga. Sellele vaatamata on kaalumise järel otsustatud hetkel parema alternatiivi puudumisel termin sellisel kujul säilitada, arvestades mh, et sarnast sõnastust („keskvalitsus“ koos seaduse puhul asjaomase täiendiga) kasutatakse ka*

		arvukates teistes Eesti õigusaktides - nende seas näiteks riigieelarve seaduses, riigivaraseaduses ja krediidiasutuste seaduses.”.
17.14	Teeme ettepaneku eelnõu [KüTS] § 2 p 4^7 defineerida kvalifitseeritud usaldusteenuse osutajat läbi E-identimise ja e-tehingute usaldusteenuse seaduse. Kuna seal on kvalifitseeritud usaldusteenuse osutaja nõuded siseriiklikult sätestatud täpsemalt.	Mittearvestatud ja selgitatud Vastav mõiste on defineeritud Euroopa Liidu õiguses (vt Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 3 punkti 20), mitte e-identimise ja e-tehingute usaldusteenuste seaduses. Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.15	Palume eelnõu [KüTS] § 5 lg 4 p-s 2 või selle mida on mõeldud “nõrga lüli” all, et seda oleks võimalik vältida.	Selgitatud NIS2 direktiivi tekstis on selle sisu inglise keeles „*single point of failure*“, mis on ka eelnõus sisalduva eestikeelse sätte mõte. Kõigile NIS2 direktiivis ja siseriiklikus õiguses, iseäranis haldusesisest korraldust puudutavate sätete kontekstis esitatud terminitele ja fraasidele ei ole võimalik anda legaaldefinitsiooni ning need tuleb sisustada praktikas. Kõnealune säte on Riigi Infosüsteemi Ameti ülesandena viidud asutuse põhimääruse koosseisu.
17.16	Teeme ettepaneku selgitada täpsemalt, mida peetakse silmas eelnõu [KüTS] § 5 lg 5 p 7 mõiste „reaalajalähedase seire“ all.	Selgitatud NIS2 direktiiv ei määratle täpsemalt selle sisu, kuid tuginedes valdkondlikule praktikale saab olla tegemist ennekõike automatiseeritud monitooringu või seirega, mille suhtes kohaldub ka teatav viiteaeg ehk see seire võib toimuda tagantjärgi, kuid ajalikult võimalikult reaalse aja lähedaselt.
17.17	Teeme ettepaneku sõnastada eelnõu [KüTS] § 5 lg 5 p 9 järgmiselt:	Selgitatud

	„9) käsitleb küberintsidente ja asjakohasel juhul abistab asjaomaseid teenuse osutajaid.“. Teeme ettepaneku selles kontekstis läbivalt asendada termin „lahendamine“ terminiga „käsitlemine“. Selgitame, et NIS2 ingliskeelse versiooni järgi on CSIRT ülesanne “responding to incidents” ja vajadusel teenuse osutajatele abi pakkumine (ingliskeelne NIS2 artikkel 11 lõige 3 punkt c), mitte aga “*resolve incidents*” ehk lahendamine. Ka põhjenduspunkt 42 viitab: „*The CSIRTs are tasked with incident handling*.“.	Vastav säte on viidud Riigi Infosüsteemi Ameti põhimääruse täiendamise kavandisse (vt vastavat seletuskirja lisa).
17.18	Teeme ettepaneku sõnastada [KüTS] eelnõu § 5 lg 5 p 10 järgmiselt: „10) kogub ja analüüsib digitaalkriminalistika-andmeid, analüüsib järjepidevalt riske ja küberintsidente, ning tagab küberturvalisuse alast olukorrateadlikkust.“.	Arvestatud ja selgitatud Vastav säte on viidud Riigi Infosüsteemi Ameti põhimääruse täiendamise kavandisse (vt vastavat seletuskirja lisa).
17.19	Teeme ettepaneku selgitada eelnõu [KüTS] § 5 lg 8 p 6 sõnaühendit „hoolas järelmeede“. Kas siin peetakse silmas seaduslikku ja proportsionaalset, mida ei ole vaja eraldi rõhutada? Samuti palume täpsustada seletuskirjas, kuidas saab küberturbe intsidentide käsitlemise üksus seda tagada. Alternatiivselt palume kaaluda, kas sättes on puudu tegusõna: „6) tagab, et teatatud nõrkusega seoses võetakse kasutusele hoolikaid järelmeetmeid.“.	Selgitatud Vastav säte on viidud Riigi Infosüsteemi Ameti põhimääruse täiendamise kavandisse (vt vastavat seletuskirja lisa). Tegemist on määratlemata õigusmõistega, mis tuleb sisustada juhtumipõhiselt. Tegusõna puudu ei ole (võetakse järelmeetmeid) – vt: https://sonaveeb.ee/search/unif/est/eki/meetmeid%20v%C3%B5tma/1/est.
17.20	Kavandatava [KüTS] eelnõu § 7 lg 2^1 p 5-s kasutatakse mõistet „riskidele avatuse määr“. Palume selgitada, kas silmas on peetud “*entity's exposure to risks*”. Palume hoida seaduse nõuded kooskõlas infoturbe standardiga ja lisada selgitus terminite loetelusse.	Selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Seetõttu on avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2^1 sisu edaspidi sama paragrahvi lõikes 2.

		Tolle punkti puhul on jah mõeldud NIS2 direktiivi artikli 21 lõike 1 teise tekstilõike teises lauses olevat „*entity's exposure to risks*“. Eraldi mõistet sel teemal ei tekitata. Siinse kommentaari teine lause viitab eelduslikult standardi puhul Eesti infoturbestandardile. Esitatud seisukoht on vastupidine Riigi Infosüsteemi Ameti kommentaaris 17.41 esitatud seisukohale.
17.21	Kavandatava eelnõu [KüTS] § 8 lg 2 p 6 viitab mõistele „oluline küberintsident“. Kuivõrd eelnõu täiendatakse § 2 p 3^5 terminiga „oluline küberoht“, on mõistlik, et selguse huvides oleks välja toodud mõlema termini selgitused.	Selgitatud „Olulise küberohu“ osas vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.32 vastust. Algselt oli eelnõus kasutatud sõnastust „oluline küberintsident“, kuid eelnõu teksti ülevaatamise käigus jõuti järelduseni, et siin tuleb kasutada sõnastust „oluline intsident“, kuna sama sõnastust kasutab NIS2 direktiiv ja selle artikli 23 lõike 5 alusel antud rakendusakt. Seetõttu on ka eelnõu KüTS § 8 lg 2 punkti 6 tekst sama sõnastusega, et tekiks selgem arusaam, et rakendusaktis olev „oluline intsident“ on see olukord, mille puhul on tegemist KüTSi mõttes „olulise mõjuga küberintsidendiga“, millest tuleb pädevat asutust teavitada. Seletuskirjas on eelnõu KüTS § 8 lg 2 punkti 6 selgitust ka vastavalt täiendatud.
17.22	Teeme ettepaneku tuua terminite loetelus välja “turvarikkemärk”, mida kasutatakse kavandatava eelnõu [KüTS] § 8 lg 4^1 p-s 1.	Vt Välisministeeriumi kommentaari 10.2 vastust.
17.23	Palume vaadata üle mõisted „IKT-toode“, „IKT-teenus“, „IKT-protsess“, „küberturvalisus“, „ohuprognoos“, „riskiprognoos“. Näiteks „oht“ on E-ITSis defineeritud/selgitatud järgmiselt: „Oht on olukord või sündmus, mis võib tekitada või võimaldada kahju.“ Infotehnoloogia maailmale ülekantuna on see olukord või sündmus, mis võib kahjustada teabe käideldavust, terviklust või konfidentsiaalsust, tekitades seeläbi kahju teabe omanikule või kasutajale. Risk on ohu võimekus tekitada organisatsioonile kahju.	Mittearvestatud ja selgitatud Mõisted „IKT-toode“, „IKT-teenus“, „IKT-protsess“, „küberoht“ ja „küberturvalisus“ on EL õiguses defineeritud. Eelnõus on siin tegemist viitega EL õigusele ja seal defineeritud vastavale mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd

		viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Riski- ja ohuprognoosi olemust on juba selgitatud seletuskirjas. NIS2 direktiivis toodud mõisteid ei saa erinevalt üle võtta (nt „risk“ või „(küber)oht“) - see tooks kaasa ka direktiivist erinevad tõlgendused kohustuste täitmisel.
17.24	Teeme ettepaneku kaaluda terminite esitamist tähestikulises järjekorras, et hõlbustada lugemist.	Arvestatud
17.25	Eelnõu seletuskirjas (vt lk 16) soovitatakse subjektsuse kindlaks tegemisel loogikat, mille kohaselt tuleb tuvastada sektor ning seejärel vaadata, kas tegu on keskmise suuruse ettevõtjaga. Eelnõu tekstis on järjekord esitatud vastupidises järjekorras. Teeme ettepaneku viia eelnõu tekst kooskõlasse seletuskirja soovitusega.	Selgitatud Seletuskirjas olev selgitus on abistav info selgitamaks (avalikul kooskõlastusringil olnud) eelnõu ühe paragrahvi kahe lõike omavahelist seost. Eelnõu ülevaatamisel on eelnõu KüTS §-de 1 ja 3 struktuur ja sisu olulisel määral muutunud.
17.26	Teeme ettepaneku koondada kõik [KüTSi] subjektid ühte paragrahvi, lisades selged kriteeriumid, kellele seadus kehtib. Näiteks saab subjektid jagada sektorite ja üksuste kaupa ning esitada Eesti konteksti arvestades. Eelnõu tekstis Euroopa Liidu õigusaktidele viitamine raskendab eelnõu lugemist, mistõttu ei pruugi subjektidele olla selge, kas neile KüTS kohaldub. Teeme samuti ettepaneku määratleda arusaadavuse huvides ja võimalusel üksused, kellele seadus kohaldub ning seejärel tuua välja eraldi paragrahvidena lisaks erisused (hetkel kavandatava eelnõu § 1 lõiked 1^3, 1^4, 1^5). Seejärel saaks järgnevas §-s välja tuua teenuse osutajat puudutav osa (kavandatava eelnõu § 3 lõiked 1^1-1^4).	Osaliselt arvestatud ja selgitatud Eelnõu ülevaatamisel on eelnõu KüTS §-de 1 ja 3 struktuur ja sisu olulisel määral muutunud. Eelnõu KüTS §-s 3 on üliloluliste üksuste ja oluliste üksuste nö grupid sätestatud, st on määratletud millised üksused ühe või teise grupi alla kuuluvad. Eelnõus on tehtud viiteid EL õigusele ja seal defineeritud mõistetele - neid ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
17.27	Seletuskirjast ei tulene, mis kaalutlustel on [KüTSist] välja jäetud erakapitalil põhinev	Selgitatud

	tervishoiuteenus ja nt hambaarstid. Täna kasutavad nt Confido, Fertilitas jmt tervishoiuteenuse osutajad täpselt samadel alustel eriliigilisi isikuandmeid ja ollakse liidestunud samade andmekogudega nagu HVA haiglad. Lisaks - tervishoiuteenuse osutajate tegevuslubasid on MEDRES (Tervishoiutöötajate registris) 2756, kuid praeguses KüTSis on vaid perearstid (u 800 perearsti/400 keskust) ja HVA haiglad (19). Seega on väga suur hulk tervishoiuteenuse osutajaid seadusest väljas.	Ka seletuskirjas on selgitatud, et soov on NIS2 direktiiv üle võtta kitsalt, sh tervishoiu puhul säilitada kehtiv olukord. Täiendavate teenuseosutajate lisandumist (või isegi nende välja võtmist) KüTSi saab analüüsida KüTSi korrastamiseks kavandatava väljatöötamiskavatsuse raames.
17.28	Teeme ettepaneku lisada [KüTSi] subjektide hulka tervishoiuteenuse osutajate sektorisse kuuluvad erahaiglad, kliinikud, laboriteenuse osutajad jmt, kellel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või aastakäive ületab 10 miljonit eurot. Palume vastavalt täiendada kavandatava eelnõu [KüTS § 1 lg 1^2] või alternatiivselt avada seletuskirjas üheselt arusaadavad kaalutlused, miks tehakse eelnõus erisus erinevate tervishoiuteenuse osutajate vahel.	Selgitatud Täiendavate teenuseosutajate lisandumist (või isegi nende välja võtmist) KüTSi saab analüüsida KüTSi muutva väljatöötamiskavatsuse käigus.
17.29	Teeme ettepaneku sõnastada eelnõu [KüTS] § 1 lg 1^5 järgmiselt: „(1^5) Arvestades käesoleva paragrahvi lõike 1^4 sätestatut, kohaldatakse...“. Kuna lõike 1^4 viide hõlmab kõiki selles asuvaid punkte, saab viitamisel piirduda lõike 1^4-le viitamisega.	Mittearvestatud ja selgitatud Uuendatud eelnõus on KüTS §-de 1 ja 3 sõnastust muudetud, sh on ka eemaldatud § 1 lõige 1^4 tervikuna. Selle asemel selgitatakse seletuskirjas konkreetse üksuse juures, kas ja kuivõrd kohaldub selle üksuse puhul NIS2 direktiivi artikli 2 lõike 2 punktides b–e sätestatud kriteeriumid.
17.30	Teeme ettepaneku sõnastada eelnõu [KüTS] § 1 lg 1^6 järgmiselt: „(1^6) Vabariigi Valitsus võib käesoleva paragrahvi lõike 1^4 kriteeriumitest lähtuvalt määrata määrusega valdkonna või sektori, milles oleva	Mittearvestatud - vastava määruse volitusnorm on eemaldatud eelnõust.

	üksuse suhtes kohaldatakse teenuse osutaja kohta sätestatut olenemata tema suurusest.“. Kui jäädakse üksuse sõnastuse juurde, siis siin on ilmselt silmas peetud üksust, mitte isikut.	
17.31	Teeme ettepaneku ühildada omavahel eelnõu [KüTS] § 1 lõiked 1^3 ja 1^5. Mõlemas lõikes teenuse osutajate suhtes kohaldatakse käesolevat seadust olenemata nende suurusest.	Osaliselt arvestatud ja selgitatud Eelnõu teksti uuendamisel on KüTS § 1 teksti muudetud, mistõttu esitatud ettepanekut ei ole sellisel kujul võimalik täita. Eelnõu ülevaatamisel on eelnõu KüTS §-de 1 ja 3 struktuur ja sisu olulisel määral muutunud.
17.32	Pöörame tähelepanu, et eelnõu [KüTS] § 2 p 4^6, 4^7, § 17^4 lg 5 viidatud määrust on muudetud. Seega tuleks viitele lisada määruse „Euroopa Parlamendi ja nõukogu määrus (EL) 2024/1183, 11. aprill 2024, millega muudetakse määrust (EL) nr 910/2014 seoses Euroopa digiidentiteedi raamistiku kehtestamisega“ viide.	Mittearvestatud ja selgitatud Viidatakse EL määrusele, mitte seda muutvale määrusele. Vastasel juhul tuleks seadusi muuta iga kord, kui muutub viidatav (otsekohalduv) EL õigusakt.
17.33	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 3 lg 1^2 p 10 sõnastus. Bilansimaht peaks ületama 43 miljonit eurot ning aastakäive 50 miljonit eurot ehk vastupidi eelnõus sõnastatule.	Arvestatud Märkus õige, sh muudatus on sisse viidud arvestades ka struktuursete muudatustega eelnõu KüTS §-des 1 ja 3.
17.34	Palume eelnõu [KüTS] § 3 lg 3^1 ja lg 3^2 selgitustes seletuskirjas täpsustada, mis tagajärg võib kaasneda, kui RIA-le viidatud punktides nimetatud teavet ei esitata. Kui seaduses ei ole kirjeldatud, milline on tagajärg teenuse osutajatele teabe esitamata jätmisel või mil viisil selle järgimist saaks kontrollida, on antud sätte sisuline mõju väga küsitav. Samuti palume seletuskirjas selgitada, kas vastava sätte täitmata jätmise korral on RIA-l võimalik järelevalvemeetmeid kasutada ning kuidas on RIA-l võimalik teada saada teabe esitamata jätmisest. Sama küsimus tekib kavandatava [KüTS] § 4 lg 1 p 1-6 nimetatud	Selgitatud Riigi Infosüsteemi Amet peab tegema kaalutluse, millist meedet (järelevalvelist meedet, turuseire või nt selgitus- ja nõustamistegevuse vahendusel) on võimalik ning sobiv kasutada, kui üksus ei ole kommentaarides olevat teavet esitanud. Muud mehhanismid selleks puuduvad ja see on järelevalveasutuse positsioonilt kohustatud isikute vaates tavapärane. NIS2 direktiiv ei nõua andmete esitamise nõuete täitmata jätmise eest teenuseosutaja karistamist - seetõttu seda ka ülevõtmise eelnõus ei sisaldu.

	andmete esitamise ning § 4 lg 1^2 tuleneva RIA-le pandud kohustuse täitmise korral.	
17.35	Palun täpsustada eelnõu [KüTS] § 4 lõige 1 p 2 mõistet „asjakohasel juhul“. Hetkel jääb sättes ebamääraseks, mida täpsemalt teenuse osutajalt nõutakse.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.41 vastust.
17.36	Teeme ettepaneku jätta välja eelnõu [KüTS] § 5 lg 4 p 1-9 sätestatu ning lisada see Riigi Infosüsteemi Ameti põhimäärusesse, kuna sätted loetlevad RIA struktuuriüksuse ülesandeid.	Arvestatud
17.37	Teeme ettepaneku sõnastada eelnõu [KüTS] § 5^2 lg 2 järgmiselt: „Valdkonna eest vastutav minister võib volitada Riigi Infosüsteemi Ametit käesoleva paragrahvi lõikes 1 nimetatud ülesande täitmist edasi volitama, arvestades Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 artikli 4 lõikes 3 ja halduskoostöö seaduses sätestatud nõudeid.“ Samuti palume seletuskirjas põhjendada kaalutlusi, miks valitsusasutuse hallataval asutusel saab olla konkreetse ülesande edasivolitamise õigus.	Mittearvestatud ja selgitatud Eelnõu KüTS § 5^2 sõnastust on muudetud ning selle kaks esimest lõiget on seotud kommentaaris mainitud delegeeritud määruse artikli 4 lõikega 1. Uuendatud eelnõus ei ole konstruktsiooni, et minister volitab Riigi Infosüsteemi Ametit edasi, vaid tolle ülesande täitja määrab minister.
17.38	Teeme ettepaneku sõnastada eelnõu [KüTS] § 6^1 lg 2, lg 3 järgmiselt: „(2) Teenuse osutaja juhtorgani liige peab läbima regulaarselt/vähemalt kord x aasta jooksul koolitusi, mille õpiväljunditeks on piisavate teadmiste ja oskuste omandamine, et mõista ja hinnata küberturvalisuse riske, nendest tulenevat mõju teenuse osutaja osutatavatele teenustele ning viise riskide käsitlemiseks. (3) Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud saavad	Mittearvestatud - vt Rahandusministeeriumi kommentaari 6.1 vastust.

	regulaarselt/vähemalt kord x aasta jooksul sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“.	
17.39	Teeme ettepaneku sõnastada eelnõu [KüTS] § 7 lg 2 p 1-3 ja 9-14 järgmiselt: „(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud: 1) koostama ja rakendama infoturvariskide haldamise metoodika ja protseduurid; 2) koostama ja kehtestama infoturbe eesmärgid ja infoturvapoliitika; 3) tagama küberintsidentide avastamise ja halduse protseduuride toimimise; 8) turvameetmete regulaarse läbivaatuse, turvameetmete tõhususe hindamise ja infoturbe parendamise; 9) koolitama regulaarselt kõiki teenuse osutaja ametnikke ja töötajaid küberturvalisuse tagamise osas; 10) asjakohasel juhul kasutama ajakohaseid krüptograafilisi meetmeid; 11) välja töötama ja teostama pääsuhalduse põhimõtted ja protseduurid; 12) teostama varade halduse; 13) asjakohasel juhul kasutama mitmik- või pidevautentimise meetodit või lahendust, turvalist hääl-, video- ja tekstiside sidelahendust, ning kriisiolukorras kasutatavat turvalist sidelahendust; 14) viima läbi süsteemi riskihalduse protseduurid, mille käigus koostatakse süsteemi turvalisust mõjutavate riskide loetelu, määratakse riskide raskusaste ning kirjeldatakse ja rakendatakse	Osaliselt arvestatud ja selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on detailses osas viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Tolle määruse puhul on veel eraldiseisvalt ettevalmistamisel eelnõu, mis muudab ka kriteeriume, millal mingi üksus peab kohaldama Eesti infoturbestandardit või selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001 (vt eelnõude infosüsteemi toimikut 25-0715). Kui üksus ei pea kumbagi standardit rakendama, siis on tal jätkuvalt vajalik täita üldisemad ehk esmased nõuded, mis ei ole niivõrd detailsed kui eelmainitud standardid. Neid nõudeid (esmased turvameetmed) peavad ära täitma kõik KüTSi teenuseosutajad. Määruse eelnõu tekst vastavas osas: ***§ 4[1]. Alalised turvameetmed*** *(1) Teenuseosutaja on alaliste turvameetmete rakendamisel kohustatud:* *1) koostama ja rakendama infoturvariskide haldamise metoodika ning protseduurid, sealhulgas analüüsima süsteemi riske, mille käigus koostatakse süsteemi turvalisust ja selle toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu, määratakse riskide realiseerumise tagajärgede raskusaste ja kirjeldatakse riskijuhtimismeetmeid;* *2) koostama ja kehtestama infoturbe eesmärgid ning infoturvapoliitika;* *3) tagama küberintsidentide käsitlemise protseduuride toimimise;* *4) võtma kasutusele abinõud küberintsidendi mõju ja leviku vähendamiseks, sealhulgas vajaduse korral piirama süsteemi kasutamist või juurdepääsu süsteemile;* *5) tagama süsteemi toimepidevuse ja kriisihalduse, sealhulgas süsteemi varundus- ja taasteprotseduuride toimimise;* *6) tagama süsteemi tarneahela turvalisuse, sealhulgas teenuseosutaja ja tema koostööpartnerite vahelistes lepetes sisalduvate turvameetmetega seotud aspektide regulaarse ülevaatamise ning ajakohastamise;*

	riskikäsitlusmeetmed vastavalt rakendamise tähtaegadele. Selgitame: 1) p 8 osas: parenduse eesmärk on, et tegevused tehtud saaks. Protseduuri väljatöötamine pole siinkohal esmane vajadus; 2) p 9 osas: küberturvalisus hõlmab antud kontekstis ka küberhügieeni; 3) p 10 osas: krüptograafia kasutamisel on oluline ka selle ajakohasus, eriti PQ (*post-quantum*) ajastu kontekstis; 4) p 11 osas: siin pole oluline niivõrd juhendite olemasolu, kuivõrd nende ellu rakendamine; 5) p 12 osas: on hädavajalik, et varadest omataks ettekujutust. Detailsetest protseduuride kasutegur on väike, kui varad ise pole hallatud. Väljend "Koostama ja kehtestama" on seotud plaani loomise ja ametliku kehtestamisega. Sõna "Teostama" viitab sellele, et varade haldamine toimub praktikas, järgitakse kehtestatud juhiseid ja toimingud viiakse ellu; 6) p 14 osas: antud paranduse eesmärk on parandada arusaadavust. Lisaks palume kaaluda punkti 1) asendamist siinse punktiga, kuna antud punkt juba katab ära 1) sisu, milles nõutav protseduur peaks seisnema. Vältimaks turvameetmete jäämist vaid plaanimise tasemele, siis on soovitav lisada ka rakendamise nõue. Seda viimast eriti olukorras, kus rakendusplaan riskikäsitlusmeetmetega saab olema võimalik koostada automaatselt. Sellisel juhul nõue saaks	*7) tagama süsteemi hankimise, arendamise ja hooldamise turvalisuse, sealhulgas turvahaavatavuste käsitlemise ning avaldamise;* *8) kehtestama turvameetmete regulaarse läbivaatamise, turvameetmete tõhususe hindamise ja infoturbe parendamise protsessi;* *9) koolitama regulaarselt kõiki teenuseosutaja ametnikke ja töötajaid küberturvalisuse tagamise osas;* *10) kasutama asjakohasel juhul ajakohaseid krüptograafilisi meetmeid;* *11) töötama välja ja rakendama personali turvalisuse ning pääsuhalduse põhimõtted ja sellega seotud protseduurid;* *12) rakendama varade haldust;* *13) kasutama asjakohasel juhul mitmik- või pidevautentimise meetodit või lahendust, turvalise hääl-, video- ja tekstside lahendust ning kriisiolukorras kasutatavat turvalist sidelahendust.*

	justkui täidetud, kuid turve ei paraneks, kui meetmete rakendamist ei toimu.	
17.40	Teeme ettepaneku kustutada eelnõu [KüTS] § 7 lg 2^1 p 2 ja sõnastada p 1 järgmiselt: „(2^1) Käesoleva paragrahvi lõikes 2 nimetatud turvameetmete rakendamisel arvestatakse: 1) kaitsetarvet, mis võtab arvesse teenuse osutaja eriomaseid vajadusi ja turvanõudeid.“. Selgitame, et punktide 1 ja 2 sisu kattub ning seetõttu oleks soovituslik sõnastada senised kaks punkti üheks punktiks, vastasel juhul tekib arusaamatus, miks nad lahus on.	Osaliselt arvestatud ja selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on detailses osas viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Seetõttu on avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2^1 sisu edaspidi sama paragrahvi lõikes 2. Tollest punktis on eemaldatud sõna „kaitsetarve“ ning selle punkti (vt eelnõu KüTS § 7 lg 2 p 1) sõnastus on „teenuseosutaja vajadusi ja turvanõudeid“. Siin vt ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaare 24.3 ja 24.49 ning Eesti Energia kommentaari 36.13. Vt ka Riigi Infosüsteemi Ameti kommentaari 17.39 juures esitatud selgitusi.
17.41	Teeme ettepaneku sõnastada eelnõu [KüTS] § 7 lg 2^1 p 3 järgmiselt: „3) kaasaegseid ja asjakohasel juhul Euroopa ning rahvusvahelisi standardeid;“. Selgitame, et kehtiv KüTS võimaldab rakendada kas Eesti Infoturbestandardit või ISO/IEC 27001. Antud sätte sõnastusest jääb ebaselgeks, kas see laiendab rahvusvahelise standardite kasutamise võimalust KüTS raames. Palume üle hinnata et antud sätte sõnastust ja vajadusel kitsendada antud sätte mõistet.	Mittearvestatud ja selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on detailses osas viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Seetõttu on avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2^1 sisu edaspidi sama paragrahvi lõikes 2. Antud punkt on sõnastatud NIS2 direktiivi artikli 21 lõike 1 teise tekstilõigu esimese lause üle võtmiseks. Kui seda lauset kitsendada, siis see tooks kaasa NIS2 direktiivi ebaõige üle võtmise. Eelnõu autorid märgivad, et näiteks NIS2 direktiivi põhjenduspunktid 79–81 sisaldavad viiteid Euroopa ja rahvusvahelistele standarditele ning nende kasutamisele. Ka NIS2 direktiivi artikli 21 lõike 5 alusel antud Komisjoni rakendusaktis (Komisjoni rakendusmäärus (EL) 2024/2690) on teatud üksuste puhul ette nähtud konkreetsed turvameetmed (tolles rakendusmääruses „küberturvalisuse riskijuhtimismeetmed“), mida selles rakendusaktis nimetatud üksused peavad järgima. Selle rakendusakti lisas olevad turvameetmed põhinevad „*Euroopa ja rahvusvahelistel standarditel, nagu ISO/IEC 27001, ISO/IEC 27002 ja ETSI EN 319401, ja tehnilistel nõuetel, nagu CEN/TS 18026:2024, mis puudutavad võrgu- ja infosüsteemide turvalisust“* (vt määruse (EL) 2024/2690 põhjenduspunkti 3). Samas rakendusaktis on märgitud ja selgitatud ka muude standardite seoseid. Seega, kui EL õigusakt näeb mõne üksuse puhul ette konkreetse EL või rahvusvahelise standardi kasutamise, siis võib tekkida

		olukord, et need üksused ei pea järgima KüTS § 7 lõike 5 alusel kehtestatud Eesti infoturbestandardit või selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001. Siin vt ka eelnõu KüTS § 7 lõiget 7 ning selle selgitusi.
17.42	Teeme ettepaneku sõnastada eelnõu [KüTS] § 7 lg 2^1 p 6 järgmiselt: 6) ohte süsteemselt ja terviklikult hõlmavat lähenemisviisi, mille eesmärk on kaitsta süsteeme ja nende süsteemide füüsilist keskkonda küberintsidentide eest. Selgitame, et seega on ettepanek asendada "kõiki ohte" väljendiga "ohte süsteemselt ja terviklikult". Vastasel juhul tekib seaduse täitmises võimatu olukord (kõiki ohte pole võimalik hõlmata). Samas oluline on ohtude hõlmamisel võimalikult terviklik ja süsteemne vaade, mida toetab nt E-ITSi alusohtude kataloog.	Arvestatud ja selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on detailses osas viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Seetõttu on avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2^1 sisu edaspidi sama paragrahvi lõikes 2. Vt ka Riigi Infosüsteemi Ameti kommentaari 17.39 juures esitatud selgitusi. Kommentaaris viidatud säte asub aga eelnõus KüTS § 7 lg 2 punktis 5 järgmises sõnastuses: „ohte süsteemselt ja terviklikult hõlmavat lähenemisviisi, mille eesmärk on kaitsta süsteeme ja nende süsteemide füüsilist keskkonda küberintsidentide eest“. Teisisõnu - uuendatud eelnõus kasutatakse ettepanekus esitatud sõnastust.
17.43	Teeme ettepaneku sõnastada eelnõu [KüTS] § 7 lg 2^2 p 1 järgmiselt: „(2^2) Käesoleva paragrahvi lõike 2 punktis 6 nimetatud tarneahela turvalisusega seotud turvameetmete asjakohasust kaaludes võtab teenuse osutaja arvesse: 1) koostööpartnerile eriomaseid nõrkusi, koostööpartneri toote üldist kvaliteeti, elutsüklihaldust ja küberturvalisuse tavasid, sealhulgas toote turvalise arenduse korda;“. Selgitame, et ettepanek lisada sõna "elutsüklihalduse" annaks arusaamise taakvara tekke riskidest juba toote kasutamise plaanimise etapis.	Mittearvestatud ja selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2^2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Eesmärk on NIS2 direktiivi minimaalse ülevõtmise huvides lähtuda art 21 lõike 3 sõnastusest ja seda mitte laiendada.
17.44	Teeme ettepaneku sõnastada eelnõu [KüTS] § 7 lg 2^3 järgmiselt: „(2^3) Kui teenuse osutaja tuvastab, et	Mittearvestatud ja selgitatud

	ta ei rakenda käesoleva paragrahvi lõikes 2 sätestatud turvameetmeid, teostab ta põhjendamatu viivituseta kõik vajalikud, asjakohased ja proportsionaalsed parandusmeetmed turvameetmete rakendamiseks.“. Selgitame, et ettepanek asendada sõna "võtab" sõnaga "teostab" suurendab selgust rakendaja jaoks. Parandusmeetmete võtmine ülesandena jääb rakendaja jaoks ebaselgeks. Antud juhul on eesmärgiks meetmete ellu rakendamine.	Vastav lõige on eelnõust eemaldatud, kuna kohustus turvameetmeid rakendada tuleneb juba eelnõu KüTS § 7 lõikest 1. Seetõttu puudub vajadus seda kehtestada sama paragrahvi kahes erinevas lõikes.
17.45	Teeme ettepaneku täpsustada eelnõu [KüTS] § 8 lg 7 osas. Kelle tegevuse osas sisuline raport esitatakse – kas CSIRT intsidendi lahendamise tegevuste (juhul kui intsidendi lahendamisega tegeleb CSIRT) osas või teenuse osutaja enda tegevuste osas või mõlema osapoole tegevuse osas korraga. [NIS2 direktiivi] art 23 annab selged juhised olulise intsidendiga seotud raporteerimise ajaraamist ning nii intsidendiga seotud osapoole kui CSIRT kohustustest. Meie parema arusaamise kohaselt ei kajasta eelnõu tekst art 23 raames seatud juhiseid piisava täpsusega.	Selgitatud Kommenteeritud lõike kohaselt esitab raporti KüTSi teenuseosutaja Riigi Infosüsteemi Ametile. Siin vt ka Advokatuuri 20.8 kommentaari vastust.
17.46	Teeme ettepaneku, et intsidendist teavitamise kohustuse täitmata jätmine peaks olema üks väärteokoosseisudest. Haldusmenetluse raames soovitud tulemust ei saavuta, kuivõrd RIA ei saa teha tulevikku suunatud abstraktseid ettekirjutusi (edaspidi teavitage). Kuivõrd tulevikus on paljude üksuste üle võimalik teostada vaid ex-post järelevalvet, siis üks peamisi viise järelevalvet teostada ongi intsidendijärgselt.	Selgitatud Vastavad väärteokoosseisud on juba eelnõus ette nähtud (vt KüTS §-e 18^2 ja 18^3), mistõttu puudub vajadus eelnõud täiendada.

17.47	Teeme ettepaneku sõnastada eelnõu [KüTS] § 8 lg 10 järgmiselt: „(10) Julgeolekuasutus teavitab küberintsidendist asjakohast julgeolekuasutust, arvestades käesolevas paragrahvis sätestatud nõudeid.“;	Arvestatud
17.48	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 6 p 2 sõnastus, mis puudutab haldusjärelevalvet „põhjaliku ennetava- või järelkontrollina“. Riiklikku ja haldusjärelevalvet teostatakse KorS'i ning VVS'i alusel, mis tagab asjaolu, et kõik riigi poolt teostatavad riiklikud ning haldusjärelevalved oleksid teostatud põhjalikult.	Arvestatud – sõna „põhjalik“ eemaldatud.
17.49	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 6 p 3, kus on välja toodud „...,ennekõike käesoleva seaduse §-ides 7 ja 8, sätestatud nõudeid;“. Teeme ettepaneku antud osa eelnõu tekstist välja jätta, kuivõrd teenuse osutajad peavad järgima kõiki seaduses sätestatud nõudeid ning antud juhul ei ole vajalik tuua eraldi välja §-ides 7 ja 8 sätestatud nõudeid.	Mittearvestatud ja selgitatud Viidatud lauseosa on lisatud NIS2 direktiivi artikli 33 lõike 1 esimese lause tõttu. Vastav lauseosa rõhutab nende sätete erilist tähtsust, kuid ei tähenda, et teisi sätteid ei peaks järgima ning kontrollima.
17.50	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 6 p 4. Antud õigus on korrakaitseorganil ka kehtivas õiguses.	Mittearvestatud ja selgitatud See säte on mõeldud toimima koos eelnõukohase KüTS § 14 lg 6 p-ga 1. See toetab p-s 1 sätestatud prioriseerimisõiguse teostamist ja on seega endiselt vajalik. Lisaks juhime tähelepanu asjaolule, et kommenteeritav lõige kehtib ka haldusjärelevalvemenetluse suhtes, mitte ainult riiklikus järelevalves, mida viiakse läbi korrakaitseseaduse alusel.
17.51	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 7 ja 8 vajalikkus, kuivõrd antud põhimõtted tulenevad KüTS'i jaoks eriseadustest. Näiteks haldusmenetluse seadus, väärteomenetluse seadus jne.	Mittearvestatud ja selgitatud Eelnõukohased KüTS § 14 lg-d 7 ja 8 teenivad NIS2 direktiivi artikli 32 lõike 7 (ja artikli 33 lõike 5, mis viitab artikli 32 lõikele 7) ülevõtmise eesmärki riiklikus ja haldusjärelevalve menetluses. NIS2 direktiivi artikli 32 lõikes 7 on ette nähtud küberturvalisuse valdkonna jaoks spetsiifilised reeglid, mis küll haakuvad Eestis ette nähtud üldiste haldusmenetluslike reeglitega, kuid on siiski NIS2 direktiivist

		tulenevateks erireegliteks. Seetõttu tuleb direktiivi artikli 32 lg 7 täpseks ülevõtmiseks need ka eraldiseisvalt sätestada – eelnõus tehakse seda KüTSis. NIS2 direktiivi ülevõtmise tabelis on ka täpsemalt selgitatud, milline on NIS2 direktiivi artikli 32 lõigete 7 ja 8 seos väärteomenetluse kontekstis.
17.52	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 9 p 1, p 4-9. Tegemist on sätetega, mille teostamise õigus on juba kehtivate seadustega RIA-l olemas.	Mittearvestatud ja selgitatud. Eelnõu esialgses versioonis sätestatud KüTS § 14 lg 9 punkt 1 ja punktid 4-9 (eelnõu kooskõlastamise järgselt muudetud versioonis KüTS § 16 lg 1^1 punkt 1 ja punktid 4-9) teenivad NIS2 direktiivi artikli 32 lõike 4 ja artikli 33 lõike 4 ülevõtmise eesmärki. Eelnõu autorid peavad vastavate reeglite sätestamist KüTS-is kui vastava valdkonna eriseaduses vajalikuks ja põhjendatuks.
17.53	Teeme ettepaneku sõnastada eelnõu [KüTS] § 14 lg 9 p 10 järgmiselt: „(10) Riigi Infosüsteemi Ametil on riikliku ja haldusjärelevalve läbi viimisel õigus nõuda elutähtsalt üksuselt, vastavushalduri määramist, kes jälgib, käesoleva seaduse §-ides 7 ja 8 ning nende alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõuete täitmist.“	Mittearvestatud ja selgitatud Pakutud sõnastus ei lähe kokku kommenteeritava lõike sissejuhatava lausega. Samuti ei ole pakutud sõnastuse puhul aru saada, mis õigusliku instrumendi (meetme) vahendusel toimuks vastava „nõude“ tegemine - eelnõus on selleks ettekirjutus. Lisaks eeltoodule märgime, et avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17.
17.54	Teeme ettepaneku sõnastada eelnõu [KüTS] § 14 lg 10 p 2 järgmiselt: „2) viib läbi sõltumatu organisatsioon või Riigi Infosüsteemi Amet;“.	Arvestatud ja selgitatud Esitatud ettepanek on arvestatud, kuid see muudatus on viidud KüTS § 16 lõike 1^2 ja § 17 lõike 1^2 alusel antava ministri määruse kavandisse.
17.55	Teeme ettepaneku vaadata üle eelnõu [KüTS] § 14 lg 11 ja lg 12 vajalikkus. Antud õigus on korrakaitseorganil ka kehtiva õiguse alusel.	Mittearvestatud ja selgitatud Tegemist on reeglitega, mis on vajalikud NIS2 direktiivi korrektseks ülevõtmiseks. Esiteks. Lõikega 11 (eelnõu uues versioonis KüTS § 16 lg 1^3 ja 17 lg 1^3) soovitakse üle võtta NIS2 direktiivi artikli 32 lõike 4 punkt b ja selles sisalduv täpsustus selle kohta, et ennetavalt saab ettekirjutuse teha üliolulise üksuse suhtes. Ilma selle sätteta ei oleks artikli 32 lg 4 punkt b korrektselt üle võetud. Teiseks. Lõikes 12 (eelnõu uues versioonis KüTS § 16 lg 1^4) soovitakse ette näha NIS2 direktiivi artikli 32 lõike 5 sissejuhatavast osast tulenev täiendava tähtaja andmise reegel. See on omakorda tugevalt seotud sama paragrahvi järgmiste lõigetega - 13 ja 14

		(eelnõu uues versioonis KüTS § 16 lg 1^5 ja lg 1^6), mis näevad n-ö viimase võimalusena ette tegevuse loa või sertifikaadi kehtivuse ajutise peatamise ja juhtimisülesandeid täitva isiku volituste peatamise. Lõige 12 (eelnõu uues versioonis KüTS § 16 lg 1^4) toimib koos nende lõigetega ja see rõhutab nende n-ö viimaseks meetmeks olemise iseloomu. Avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17.
17.56	Teeme ettepaneku eelnõu [KüTS] § 18^4 täiendamiseks. Teeme ettepaneku laiendada seaduse nõuete rikkumisel teenuse osutaja juhtorgani või juhtorgani liikme poolset vastutust. Kehtiva [KüTSi] § 18 lg 1 ning § 18^1 lg 1 nõuete rikkumise korral on võimalik vastutusele võtta ka füüsiline isik. Palume täiendada eelnõu teksti viisil, mis jätaks kehtiva [KüTSi] § 18 lg 1 nõuete rikkumise korral analoogse karistuse määramise võimaluse. Hetkel on selline võimalus sätestatud piiratult eelnõu [KüTS] § 18^4 kontekstis eelnõu § 6^1 nõuete rikkumise eest.	Mittearvestatud Kehtiva KüTS § 18 lg 1 ning § 18^1 lg 1 nõuete rikkumise korral ei ole võimalik vastutusele võtta juhatuse liiget või infoturbejuhti kui füüsilist isikut. Avalikul kooskõlastusel olnud eelnõu KüTS § 18^4 eemaldati uuendatud eelnõust, sest NIS2 direktiiv ei nõua karistusõigusliku vastutusrežiimi loomist (piisab ka tsiviilõiguslikust vastutusest) mistõttu esitatud ettepanekut ei ole võimalik täita.
17.57	Teeme ettepaneku eelnõu [KüTS] § 18^5 lg 1 muutmiseks. Asendada eelnõu lõikes 1 „füüsilisest isikust üksuse poolt“ sõnastusega „füüsilise isiku poolt, kes tegutseb piiriüleste elektrivoogudega seotud üksuse nimel“. Vastasel juhul meil ei ole uue KüTSi eelnõu järgi alust võtta väärteomenetluse raames vastutusele füüsiline isik, kui ta ei ole juhtkonna liige (nt infoturbejuht). Praegu kehtiva KüTS järgi on see võimalus olemas § 18 lg 1 alusel ja see tuleb säilitada.	Mittearvestatud Kõnealune koosseis ei ole mõeldud teenuseosutaja juures tegutseva füüsilise isiku, vaid kohustusi rikkuva teenuseosutaja karistamiseks. Vt ka Riigi Infosüsteemi Ameti kommentaari 17.56 vastust.
17.58	Teeme ettepaneku eelnõu [KüTS] § 18^6 lõiked 1 ja 2 asendada „füüsilisest isikust seadusliku esindaja	Arvestatud ja selgitatud Kõnealune koosseis ei ole mõeldud teenuseosutaja juures tegutseva füüsilise isiku, vaid kohustusi rikkuva teenuseosutaja nimel määratud „seadusliku esindaja“ karistamiseks.

	poolt „seadusliku esindaja poolt“. Seaduslik esindaja saab olla ainult füüsiline isik.	Too esindaja on sarnane konstruktsioon nagu on digitaalse teenuse osutaja esindajaga. kuid tegemist on Euroopa Komisjoni delegeeritud määruses (EL) 2024/1366 oleva olukorraga. Tolle väärteokoosseisu puhul mainitud „seaduslik esindaja“ võib olla kas füüsiline isik või juriidiline isik Seda on selgitatud eelnõu KüTS § 18^5 juures seletuskirjas.
17.59	Teeme ettepaneku täiendada eelnõu [KüTS] § 19 lg 2 sõnastust. Kuivõrd antud ülesanne on Andmekaitse Inspektsiooni pädevuses. Seega peaks antud juhul kohtuväliseks menetlejaks olema Andmekaitse Inspektsioon.	Arvestatud
17.60	Palume seletuskirjas selgitada, kuidas Eesti (RIA) hakkab teavet saama organisatsioonidest, mille peamine tegevus toimub nt Lätis, kuid turvaalane tegevus käib Eestis, kuigi teenuseid osutatakse üle maailma.	Selgitatud Näiteks on võimalus seda teavet saada turujärelevalve kui ka järelevalvemenetluse käigus, sh kasutades piiriülest järelevalveasutuste koostööd. Samuti on võimalik uurida konkreetse riigi avalikke andmekogusid (nt äriregistreid) kui ka nende üksuste endi võrgukodudes olevat infot, et seda teavet saada. Riigi Infosüsteemi Amet peab olema siin proaktiivne.
17.61	Palume eemaldada seletuskirja leheküljelt 86 järgnev lause: “Testkeskkonna link https://mass.cloud.ut.ee/test-massui/ ja töökeskkonna link https://mass.cloud.ut.ee/massui/. ” See testkeskkond on enesehindamise mõõdiku kohta, mitte RIAs arendatava terviklahenduse kohta.	Arvestatud
18. Tarbijakaitse ja Tehnilise Järelevalve Ameti arvamus 31.01.2025 kiri nr 2-2/2024/0121		
18.1	TTJA toetab küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga kavandatavaid muudatusi, võtmaks üle Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, 14. detsember 2022, mis käsitleb meetmeid, millega tagada	Võetud teadmiseks

	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 (küberturvalisuse 2. direktiiv, edaspidi NIS2 direktiiv).	
18.2	Eelnõu § 1 punktiga 49 nähakse ette küberturvalisuse seaduse (KüTS) täiendamine §-ga 13^3, mis puudutab Euroopa küberturvalisuse sertifitseerimise kavade kasutamist. Säte on seotud NIS2 direktiivi artikli 24 üle võtmisega ja sellel on ka seos NIS2 direktiivi põhjenduspunktidega 80–82 ja 138. TTJA peab oluliseks märkida sättega seonduvalt järgmist. 1. KüTS §-ga 13^1 on Eestis määratud riiklikuks küberturvalisuse sertifitseerimise asutuseks TTJA. 2. Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881, 17. aprill 2019, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) artikli 58 lõike 5 kohaselt tagavad liikmesriigid, et riiklikel küberturvalisuse sertifitseerimise asutustel on piisavad ressursid oma volituste rakendamiseks ning oma ülesannete tulemuslikuks ja tõhusaks täitmiseks. Seejuures on riiklikul küberturvalisuse sertifitseerimise asutusel küberturvalisuse määruse artikli 58 lõike 7 punkti 1 kohaselt muu hulgas kohustus teha järelevalvet Euroopa küberturvalisuse sertifitseerimiskavade täitmise ja rakendamise üle.	Mittearvestatud ja selgitatud Eelnõust on vastav paragrahv välja jäetud, et võtta üle NIS2 direktiiv minimaalses mahus. Seetõttu ei ole võimalik ka eelnõu seletuskirja täiendada Tarbijakaitse ja Tehnilise Järelevalve Ameti mõjudega. See siiski ei välista võimalust, et vastaval Ametil on tekkinud vajadus kommentaaris mainitud lisaressurssi ühe ametikoha täiendamise kaudu, kuid ka kommentaaris on kirjeldatud, et tegemist on teiste õigusaktide kui NIS2 direktiiviga, mis selle ressursivajaduse on tekitanud.

	3. Lisaks on riikliku küberturvalisuse sertifitseerimise asutuse ülesandeid täpsustatud ja täiendatud Komisjoni rakendusmäärusega (EL) 2024/482, 31. jaanuar 2024, millega kehtestatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 rakenduseeskirjad seoses Euroopa ühiskriteeriumidel põhineva küberturvalisuse sertifitseerimise kava (EUCC) vastuvõtmisega. Viidatud rakendusmääruse IV peatükk käsitleb mh riikliku sertifitseerimisasutuse kohustusi seoses Euroopa küberturvalisuse kava rakendamisega ja teatamiskohustusega. Rakendusmääruse artiklid 25-31 täpsustavad seejuures, millises osas on riiklikul sertifitseerimisasutusel kohustus teha järelevalvet seoses sertifitseerimise kava rakendamisega. Lisaks on rakendusmääruse artiklis 48 sätestatud EUCC haldamise nõuded. Seega kuulub riikliku küberturvalisuse sertifitseerimisasutuse ülesannete hulka ka Euroopa küberturvalisuse sertifitseerimise rühma (ECCG) töös osalemine. 4. Küberturvalisuse määruse alusel on hetkel avaldatud rakendusmäärus (EL) 2024/482, analoogsed rakendusmäärused on plaanis avaldada kõikide Euroopa sertifitseerimise kavade kohta. Seejuures on hetkel aktiivselt väljatöötamisel Euroopa küberturvalisuse sertifitseerimise kava pilveteenuste jaoks (EUCS), 5G teenuste Euroopa küberturvalisuse sertifitseerimise kava (EU5G) ja Euroopa digitaalse identiteedi rahakott (EUID Wallet). Eestil on huvi kõikide viidatud arenduste vastu ning nende rakendamine avaldab ka mõju	

	TTJA ülesannete suurenemisele. Lisaks on ECCG töörühmas ettevalmistamisel rakendusmääruse väljatöötamine, millega täpsustatakse küberturvalisuse määruse artiklis 59 viidatud vastastikuse eksperdihinnanguga seonduvat ning mis algse ajakava kohaselt on planeeritud jõustuma käesoleva aasta lõpus. 5. Eelnevat arvesse võttes on ette nähtav TTJA koormuse tõus KüTS § 13^3 jõustumisega, kuivõrd TTJA ressursivajadus suureneb iga Euroopa sertifitseerimise kava rakendamisega. 6. Täiendavalt märgime, et ehkki KüTS § 13^3 lõike 1 kohaselt võib Vabariigi Valitsuse määrusega kohustada teenuse osutajat järgima küberturvalisuse sertifitseerimise kava, ei ole TTJA hinnangul välistatud, et teenuse osutajad võtavad vastu otsuse kava järgida ka vabatahtlikult. Näiteks võib selline vajadus tekkida mõne koostööpartneri nõudmisel, kes soovib, et teenuse osutajal oleks KüTS §-s 7 sätestatud nõuetele vastavuse tõendamiseks kasutusel teatavad IKT-tooted, IKT-teenused ja IKT-protsessid. 7. Lähtudes TTJA-le lisanduvatest tegevustest seoses sertifitseerimise kavadega, teeme ettepaneku täiendada eelnõu seletuskirja peatükki 7, tuues välja seaduse rakendamisega kaasnevad mõjud ka TTJA-le. Eelkõige palume välja tuua, et **seadusest tulenevate uute ülesannete täitmiseks on riiklikul küberturvalisuse sertifitseerimise asutusel vaja luua üks täiendav ametikoht. Ametikoha töövaldkond on küberturvalisuse sertifitseerimise kavade täitmise ja rakendamise**	

	üle järelevalve teostamine. Loodava ametikoha abil on võimalik TTJA-l rakendada temale määratud volitusi ning täita ülesandeid tulemuslikult ja tõhusalt.	
	19. Transpordiameti arvamus 21.01.2025 e-kiri	
19.1	Merenduse kommentaar: Sadamate osas on KüTS muudatus sadamate osas vähemkoormavas suunas – kui varasemalt pidid kõik turvaülesandeid täitvad sadamad kohaldama KüTSi sätteid, siis nüüd välistatakse need sadamad, kus ei ole töötajaid üle 50 ja käive üle 10 milj euro. RIA nimetab iga kahe aasta järel need sadama pidajad, kes peavad nõudeid täitma. Selline 2-aastane intervall võib aga nö piiripealsete ettevõtete puhul olla häiriv ja segadust tekitav (nt sadam määratakse oluliseks üksuseks, 2 aasta pärast jäetakse nimistust välja ja 2 aastat hiljem jälle lisatakse nimistusse) – küberturvalisuse tagamisel on oluline pigem stabiilsus, mis võimaldab juurutada korrektseid organisatsiooni põhiväärtuseid ja kvaliteedi tagamise süsteemi. TRAM peab koostama turvanõudeid täitvate sadamate turvalisuse alaseid riskianalüüse (iga 5 aasta järel), mistõttu võib analüüsides olla keeruline hinnata ja viidata, kas sadamal on kohustus KüTS täita või mitte, kuna tegemist on muutuva asjaoluga. Selgusetuks jääb ka see, kui sadam enam ei ole oluline üksus KüTS tähenduses, siis kas ja milliseid küberturvalisuse tagamise nõudeid sadam sellest hoolimata täitma peaks ja kes selle üle järelevalvet peaks teostama –	Selgitatud Seoses hädaolukorra seaduse muudatustega (jõustusid oktoobris 2024) on elutähtsate teenuste hulgas uuesti ka sadamate toimimine (vt tolle seaduse § 36 lg 1^1 punkti 8). Seega, kui kommentaaris mõeldud sadamad on samad sadamad, kes on või saavad olema elutähtsa teenuse osutajad, siis need sadamad on ka KüTSi kohaldamisalas olenemata nende suurusest. Piiripealsete juhtumite puhul tuleb üksusel oma kohustusi ja riske hinnates lähtuda võimalusest, et ta võib suure tõenäosusega kvalifitseeruda KüTS-i kohuslaseks ja sellest tulenevalt ka tegevusi ja meetmeid planeerida. Vt Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.

	hetkel TRAMil puudub pädevus oma riskianalüüside käigus kübernõrkuseid tuvastada.	
19.2	Lennunduse kommentaar: Küberturvalisuse seaduse muutmise puhul on tegemist NIS2 (Euroopa Parlamendi ja nõukogu küberturvalisuse 2. direktiivi) kohustusliku (ja hilinenud) ülevõtmisega. Kuigi ka NIS2 käsitleb lennundust ja paljud küberturvalisuse nõuded on Part-IS'ga sarnased, siis fookuspunktiks on oluliste teenuste püsimajäämine, Part-IS puhul on aga fookuspunktiks lennuohutus. Küberturvalisuse seaduses on pädevaks asutuseks määratletud RIA, seega peame asuma RIA-ga sel teemal koostööd tegema.	Võetud teadmiseks
20. Eesti Advokatuuri arvamus 03.02.2025 kiri nr 1-8/982-1		
20.1	Eelnõu kohaldamisala on ebaselge Õigusselguse[1] huvides peab olema tagatud, et seaduse eelnõus on üheselt ja selgelt sedastatud kohustatud isikud ja puutumust omavad valdkonnad. KüTSi eelnõu kohaldamisala reguleeriv sõnastus on niivõrd ebaselge, et ei ole võimalik aru saada, mis on seadusandja eesmärgiks ning kes ja milliste kriteeriumite alusel on kohustatud isikud.	Selgitatud Eelnõu koostades on kasutatud võimalikul määral NIS2 direktiivi sõnastust või seal viidatud õigusakti sõnastust. Eelnõu ülevaatamisel on eelnõu KüTS §-de 1 ja 3 struktuur ja sisu suures ulatuses ümber kujundatud, seda mh parema õigusselguse saavutamise eesmärgil.
20.2	Eelnõu normatiivtekst ei ole loetav Eelnõu ei ole kooskõlas HÕNTE § 15 lg-ga 2. Nimelt ei toeta eelnõu ülesehitus ja sõnastus teksti loetavust ja seadusest arusaamist. Antud mahus ülamärgete kasutamine osutab, et põhjendatud on	Selgitatud Eelnõud läbivalt (iseäranis KüTS §-de 1 ja 3 osas) muudetud. Tõsi on, et eelnõus on tehtud viiteid EL õigusele ja seal olevatele mõistetele - neid ei ole võimalik Eesti õiguses taasesitada või korrata . Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse

[1] PS § 13 lg-s 2 toodud õigusselguse põhimõte nõuab, et õigusaktid oleksid sõnastatud piisavalt selgelt ja arusaadavalt, et isikul oleks võimalik piisava tõenäosusega ette näha, milline õiguslik tagajärg kaasneb teatud tegevuse või tegevusetusega (RPJKo 3-4-1-23-15, p 98; 5-19-38/15, p 68; 5-22-4/13, p 62).

	uue KüTSi väljatöötamine. Sarnased teemad on killustatult käsitlemist leidnud erinevates sätetes ja jaotistes. HÕNTE näeb ette, et teemasid tuleb käsitleda eraldi ja vastavasisulised paragrahvid tuleb rühmitada nende sisu järgi peatükkides ja osades (vt HÕNTE § 7 jj). Eelnõus kasutatud viitamine on ebaselge ja ei taga õigusselgust. Eelnõus on väga suures mahus viiteid Euroopa Liidu õigusaktidele. Kui eelnõu koostajad jäävad seisukohale, et selline viitamine on mõõdapääsmatu, siis tuleb seletuskirjas vastavad viited Euroopa Liidu õigusaktidele sisuliselt lahti seletada.	ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Seletuskirjas on selgitatud EL õigusele tehtud viite korral, mida konkreetne viide tähendab, sh oli seda tehtud juba avalikule kooskõlastusele esitatud eelnõu seletuskirjas.
20.3	Seletuskiri ei vasta HÕNTE nõuetele ja ei täida eesmärki Seletuskiri ei vasta HÕNTE § 39 jj nõutele. Seletuskiri on küll mahukas aga norme selgitatakse seletuskirjas valikuliselt. Seletuskirjas tuleb eelnõu sätted lahti selgitada ja vajadusel põhistada või näidetega ilmestada. Vältida tuleb formalistlikku käsitlust, kus norm on kopeeritud seletuskirja ja puuduvad igasugused muud selgitused. Lisaks tuleb arvestada, et kui normatiivtekstis on nõnda palju sisemisi viiteid kui ka viiteid teistele õigusaktidele, sh Euroopa Liidu õigusaktidele, siis tuleb seletuskirjas selliste viidete sisu põhjalikult lahti selgitada. Märkida tuleb, et keerulise ülesehituse ja sõnastusega seaduse eelnõu seletuskiri peab toetama normatiivtekstist arusaamist. Kahjuks tuleb möönda, et KüTSi eelnõu seletuskiri ei täida vajaliku abimaterjali rolli.	Arvestatud ja selgitatud Nii eelnõud kui seletuskirja on läbivalt täiendatud ja korrigeeritud. EL õigusele viite teemal vt Advokatuuri kommentaari 20.2 vastust.

20.4	Mõjude analüüsid on tegemata või mõjusid on käsitletud puudulikult ja ühekülgselt HÕNTE § 39 sätestab, et seletuskirja eesmärgiks on mh anda ülevaade seaduse jõustumisega kaasnevatest mõjudest. Eelnõu seletuskirjas ei analüüsita kõiki asjakohaseid mõjusid. Käsitlemist leidnud mõjusid on kirjeldatud äärmise pealiskaudsusega ja ainult positiivses võtmes. Kui eelnõuga kasvavad kohustatud isikute arv ja järelevalve mahud ning samuti on ettenähtav mõju kõigile turuosalistele ja lõpptarbijale, siis on küüniline sedastada, et mõjusid ei ole või need on juba direktiivi väljatöötamisel käsitlust leidnud. Eesti poliitikakujundajal ja seadusandjal on kohustus hinnata igakülgselt kõiki mõjusid, mis võivad Eestile osaks langeda. Soovitused: 1. Viia eelnõu kooskõlla HÕNTE-ga. 2. Kaaluda KüTSi eelnõu uue tervikteksti väljatöötamist.	Osaliselt arvestatud ja selgitatud - Mõjude analüüs on üle vaadatud ja võimaluse korral täiendatud. - Siinse eelnõuga ei tehta uut tervikteksti, kuid selle koostamist võib tulevikus analüüsida.
20.5	Käesoleva eelnõu puudujäägid viitavad üheselt, et poliitikakujundaja ei ole saanud turuosalistelt sisendit. Sellise sisu ja mõjuga õigusaktide väljatöötamisel on oluline kaasata erinevad huvigrupid. Enne eelnõu väljatöötamist peab poliitika olema kujundatud. Ebapiisav kaasamine võib olla juurpõhjuseks, miks eelnõu ei vasta HÕNTE-le.	Võetud teadmiseks
20.6	Eelnõu [KüTS] § 1 lg 1^6 annab Vabariigi Valitsusele volituse määrata Vabariigi Valitsuse määrusega valdkonna või sektori, milles oleva isiku suhtes kohaldatakse teenuse osutaja kohta sätestatut	Mittearvestatud ja selgitatud. Kommentaaris mainitud määruse volitusnorm on eelnõust eemaldatud, mistõttu esitatud soovitust ei ole võimalik täita.

	olenemata tema suurusest vastavalt eelnõu § 1 lg 1^4 punktides 1, 2, 3 ja 4 kriteeriumitest. Viidatud volitusnormis tuleb konkretiseerida volituse sisu ja ulatust. Nimelt on sedastatud kriteeriumid liiga laiad ning annaksid Vabariigi Valitsusele põhjendamatult suure diskretsioonivabaduse. Seletuskirjas ei ole selgitatud sellise volitusnormi võimalikku negatiivset mõju (nt omavoli, poliitilist kallutatust vms). Nii suure mõjuga ettevõtlusvabadust piirav volitusnorm ei ole põhjendatud. Konkretiseerida tuleb volitusnormi sisu ja ulatust. Täpsustamist vajavad eelkõige kriteeriumid. Soovitus: muuta eelnõu § 1 lg 1^6 sõnastust selliselt, et Vabariigi Valitsuse volitusnormi sisu ja ulatus on konkretiseeritud täpsustatud kriteeriumitega.	
20.7	**KüTS § 6^1 lg 3 ja § 18^4 sõnastust seoses juhtorganite kohustuste ja sunnimeetmetega tuleks muuta** KüTS § 6^1 lg-s 3 on sätestatud: (3) *Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“* Kommenteeritud väljaandes puudub aga selgitus KüTS § 6^1 lg 3 osas. Täpsemalt, seletuskirjas on välja toodud vaid teenuse osutaja juhtorgan, kui koolituse läbija : *„Taolise koolituse läbija ehk teenuse osutaja juhtorgani liige teab: etc.“.* Lõike enda tekst hõlmab aga ka teenuse osutaja töötajaid ja ametnikke: *„Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud*	Arvestatud osaliselt ja selgitatud. Eelnõus KüTS § 6^1 sõnastust on muudetud ning sellest on eemaldatud juhatuse liikme(te) kohustus tagada, et tema üksuse töötajad ja ametnikud saaksid sisuliselt samu koolitusi, mida juhatuse liige (liikmed) peavad ise läbima. Samuti on eelnõust eemaldatud kommentaaris mainitud väärteokoosseis. Vt ka Rahandusministeeriumi kommentaari 6.1 vastust.

	saavad korrapäraselt sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“ NIS2 artikli 2 lg 2 eestikeelses versioonis on sätestatud: „*Liikmesriigid tagavad, et elutähtsate ja oluliste üksuste juhtorganite liikmed on kohustatud läbima korrapäraselt erikoolitusi, ning ergutavad elutähtsaid ja olulisi üksusi pakkuma sarnaseid koolitusi korrapäraselt oma töötajatele, et nad saaksid omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja nende juhtimise tavasid ning nendest tulenevat mõju üksuse osutatavatele teenustele.“* NIS2 artikli 2 lg 2 ingliskeelses versioonis on sätestatud: *Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.* Lause ülesehitusest nähtub, et ergutustööd peab tegema just riik, mitte üksus. Ühtlasi pole võimalik sõnast „ergutama“ lugeda välja teenuse osutaja juhtorgani kohustust, mida peaks trahviga survestama. Mõttekäigu toetuseks räägib ka sõnakasutus *tagavad, et … on kohustatud vs. ergutavad … pakkuma; Shall ensure that … are required vs. shall encourage … to offer.* Esimene versioon on ilmselgelt karmim kui teine.	

	Juhtorgani liikmed on kohustatud läbima erikoolitusi, kuid töötajate koolituste osas on rõhk ergutamisel, mitte kohustusel. Seega ei saa töötajate koolituste pakkumist käsitleda juhtorganite kohustusena, mida peaks trahviga survestama. KüTS § 18^4 on lausa eraldi mainitud vastutust töötaja koolitamata jätmise osas: *"Kommenteeritava paragrahviga ette heidetav tegu on seotud KüTS §-s 6^1 sätestatud nõuete rikkumisega, mida teenuse osutaja juhtorgan või juhtorgani liige peab täitma, et tagada KüTSi nõuete täitmine. Näiteks turvameetmete heaks kiitmine, nende järgimise jälgimine ja kontroll, vajalikel erikoolitustel osalemine ning tagada, et teenuse osutaja töötajad ja ametnikud saavad küberturvalisuse valdkonnaga seotud koolitusi."* Soovitus: muuta KüTS § 6^1 lg 3 ja § 18^4 sõnastust, et töötajate koolitamise kohustus ei oleks seotud trahviga, vaid jääks ergutuse tasandile vastavalt NIS2 direktiivi artikli 20 mõttele.	
20.8	**KüTS § 8 lg 4^1 ja 4^2 puhul jääb arusaamatuks, miks seadusandja ei kirjuta ümber NIS2 teksti seoses varajase hoiatuse, intsidenditeate, vahearuande ja lõpparuandega** Eelnõu [KüTS] § 8 lõiked 4^1 ja 4^2 käsitlevad varajase hoiatuse, intsidentide teavitamise, vahearuande ja lõpparuande nõudeid. Siiski on arusaamatu, miks seadusandja ei ole ülevõtmisel järginud NIS2 direktiivi teksti võimalikult täpset sõnastust. NIS2 direktiivi eesmärk on tagada ühtne ja harmoneeritud lähenemine liikmesriikides,	Osaliselt arvestatud ja selgitatud Eelnõud on muudetud viisil, et see oleks sarnasem NIS2 direktiivi artiklile 21. Eelnõus ei ole kasutatud NIS2 direktiivi sõnastust üks-ühele olukordades, kus see ei ole tingimata vajalik ehk olukordades, kus direktiivist tulenev nõue oleks võimalik lugeda täidetuks ka Eestis juurdunud praktikat ja terminoloogiat järgides. Direktiivist tulenevad nõuded säilitatakse, aga need asetatakse (võimaluste piires) ülevõtmise käigus liikmesriigi õiguse terminoloogiasse, traditsiooni ja konteksti. (ELTL art 288 lg 3: „*Direktiiv on saavutatava tulemuse seisukohalt siduv iga liikmesriigi suhtes, kellele see on adresseeritud, kuid jätab vormi ja meetodite valiku selle riigi ametiasutustele.*").

	mistõttu ühtlustatud sõnastuse kasutamine aitaks vältida võimalikke tõlgendamisprobleeme ning tagada õigusselgus. Seletuskirjas viitab seadusandja sellele, et teavituse liigid on sisu ja tingimuste mõttes erinevad, mistõttu on otsustatud säilitada osaliselt kehtiv õigus (näiteks teavituste tähtaja osas) ja ühtlustada teavituste sisu. Siiski ei ole seletuskirjas selgitatud, miks ei ole direktiivi teksti sõnastust täpsemalt järgitud ning miks valiti selline erinev lähenemine. Probleemid ja tähelepanekud: 1. Intsidentide teavituse tähtaeg: NIS2 direktiiv sätestab selgelt, et intsidentidest tuleb teavitada hiljemalt 72 tunni jooksul. Eelnõus puudub konkreetne säte selle tähtaja kohta, mis loob õigusselgusetuse ja võib viia tähtajast erinevate tõlgendusteni. 2. Teavituse ulatus ja sisu: Eelnõus on kirjas vaid kohustus esitada teave intsidenti puudutava sisu ja toimumise põhjuste kohta. Samas NIS2 direktiiv nõuab lisaks hinnangut, kas intsident oli ebaseaduslik või pahatahtlik, mis on oluline intsidentide tõsiduse hindamiseks ja riskide maandamiseks. Sellise teabe lisamine aitaks paremini täita direktiivi eesmärke. 3. Varajane hoiatus, vahearuanne ja lõpparuanne: Eelnõu reguleerib teavituste liike, kuid nende sisulised nõuded ja tingimused jäävad ebaselgeks. See jätab liiga palju ruumi tõlgendustele, mis võib viia liikmesriikide praktikas oluliste erinevusteni, mida NIS2 direktiiv just ühtlustada püüab. Soovitused:	

	1. Ülevõtmise täpsus: Viia KüTS vastavusse NIS2 direktiiviga, kasutades võimalikult täpselt direktiivi sõnastust. See tagaks õigusselguse ning ühtlustatud praktika nii Eestis kui ka teistes liikmesriikides. 2. Intsidentide teavituse tähtaeg: Lisada eelnõusse selge viide, et intsidentidest tuleb teavitada hiljemalt 72 tunni jooksul vastavalt NIS2 direktiivi nõuetele. See aitab vältida olukordi, kus teavituse õigeaegsuse osas tekivad vaidlused või erisused. 3. Teavituse sisu täiendamine: NIS2 direktiivis nõutud teave, näiteks hinnang intsidentide ebaseaduslikkuse või pahatahtlikkuse kohta, tuleks lisada eelnõusse, et see vastaks direktiivi eesmärgile ja standarditele. 4. Seletuskirja täiendamine: Lisada seletuskirja selgitus, miks on mõni osa direktiivi sõnastusest üle võetud teisiti, kui otsustatakse mitte järgida direktiivi täpset sõnastust. See parandab läbipaistvust ja aitab selgitada seadusandja kaalutlusi.	
20.9	Ebaselgus juhtorgani definitsiooni osas Eelnõu [KüTS] § 6^1 ja § 18^4 kasutavad mõistet „juhtorgan“, kuid eelnõu tekstis ega seletuskirjas ei ole täpsustatud, kas see hõlmab juhatust, nõukogu või mõlemat. Eesti õiguses ei ole mõistet „juhtorgan“ iseseisvalt defineeritud; TsÜS eristab eraldi juhatust ja nõukogu (§ 31 lg 1 ja 2). See tekitab tõlgendamisprobleeme, eriti olukordades, kus juhtorgani kohustuste rikkumine toob kaasa rahatrahvi (kavandatav § 18^4).	Arvestatud Eelnõu KüTS § 6^1 sõnastust on muudetud ning „juhtorgan“ asendatud „juhatuse liikme“ lähenemisega või kui üksuses juhatuse liiget pole üksuse enda struktuuri loogika tõttu, siis kellele selle paragrahvi nõudeid kohaldatakse. Samuti on eelnõust eemaldatud kommentaaris mainitud väärteokoosseis. Kõnealust küsimust on loodava KüTS § 6^1 juures põhjalikumalt selgitatud ka seletuskirjas.

	Eelnõu § 6^1 võtab üle NIS2 direktiivi artikli 20, mille ingliskeelses versioonis kasutatakse mõistet „management bodies“. Direktiivi eestikeelses tõlkes on see tõlgitud kui „juhtorganid“, kuid direktiivi sisust tulenevalt viidatakse pigem juhatusele kui organile, kes vastutab igapäevaste juhtimisotsuste, sealhulgas küberturvalisuse meetmete heakskiitmise ja rakendamise jälgimise eest. Direktiivi eesmärk ei tundu hõlmavat nõukogu, kelle roll on järelevalve ja strateegiline suunamine. Ka eelnõu muud sätted viitavad juhatuse reguleerimisele, näiteks: ● [KüTS] § 6^1 lõike 2 nõuab juhtorgani liikmelt regulaarsete küberturvalisuse alaste koolituste läbimist. Seda vastutust ja oskuste vajadust seostatakse pigem juhatusega, kes vastutab operatiivjuhtimise eest, mitte nõukoguga, kelle ülesanded on strateegilisemad. ● [KüTS] § 14 lõike 13 punkt 2 kohaselt võib Riigi Infosüsteemi Amet nõuda elutähtsa teenuse osutaja nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist (vt kriitikat selle sätte kohta allpool). Ka sellest haldussunni sättest saab järeldada, et juhtorganiks saab pidada üksnes juhatust. Soovitus: täpsustada eelnõu [KüTS] § 6^1 ja § 18^4 sõnastust, et oleks selge, kas „juhtorgan“ viitab ainult juhatusele, nõukogule või mõlemale. Lähtudes direktiivi eesmärgist ja Eesti õiguse kontekstist, oleks asjakohane viidata juhatusele.	

20.10	**Elutähtsa üksuse juhatuse liikmete volituste peatamise menetluse puudulikkus** Eelnõu [KüTS] § 14 lõike 13 punkti 2 kohaselt võib Riigi Infosüsteemi Amet nõuda ettekirjutusega elutähtsa teenuse osutaja nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist. Juhatuse liikme volituste peatamise nõue on äärmuslik meede, mis mõjutab otseselt juhatuse liikme õigusi ja ettevõtte juhtimise toimimist. Sellise meetme rakendamine peab olema selgelt põhjendatud ja proportsionaalne, et vältida järelevalveasutuse meelevaldset otsustusõigust ning tagada õigusselgus ja ettevõtjate õiguskindlus. Esiteks. NIS2 direktiiv ei anna regulaatorile endale pädevust selliste meetmete rakendamiseks. Direktiivi kohaselt saab regulaator üksnes taotleda "asjaomaselt organilt või kohtult" kooskõlas liikmesriigi õigusega, et keelata füüsilisel isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, selles üksuses ajutiselt juhtimisülesannete täitmine. Seega on eelnõus pakutud lahendus vastuolus [NIS2] direktiiviga. Teiseks. NIS2 direktiiv nõuab, et "sellise ajutise peatamise või keelu kehtestamise suhtes kohaldatakse kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust." Eelnõus ja seletuskirjas puudub selgitus nende õigusriiklike menetluslike tagatiste kohaldatavusest juhatuse või	Arvestatud ja selgitatud Esiteks, nagu märkuses ka õigesti välja tuuakse, on kõnealuse sätte eesmärk NIS2 direktiivi artikli 32 lõike 5 punkti b ülevõtmine. Sellise regulatsiooni on Euroopa Liidu seadusandja direktiivis ette näinud ning liikmesriikidel puudub võimalus seda mitte rakendada. Samuti rõhutavad eelnõu autorid, et tegemist on n-ö viimase võimaluse abinõuga, mida järelevalveasutusel on võimalik rakendada üksnes juhul, kui varem rakendatud järelevalvemeetmed ei ole andnud tulemust ning ülioluline üksus ei ole ka talle antud täiendava tähtaja jooksul puudust kõrvaldanud. Riigi Infosüsteemi Amet peab hindama, kas tegemist on kõige sobivama meetmega konkreetses olukorras tekkinud probleemi lahendamiseks ehk tegemist ei saa olla kergekäeliselt kasutatava meetmega. Seetõttu ei saa ühegi realistliku stsenaariumi kohaselt olema tegemist praktikas tihedat rakendamist leidva meetmega. Samas, nagu eelnõu seletuskirjas ka selgitatud on, ei ole siiski tegemist Eesti õiguses täiesti erakordse lahendusega. Nimelt annab krediidiasutuste seaduse § 50 Finantsinspektsioonile õiguse ettekirjutusega nõuda krediidiasutuse juhi või võtmeisiku tagasikutsumist. Sarnast lahendust on kasutatud ka käesolevas eelnõus, kusjuures eelnõu on pärast avalikku kooskõlastusringi muudetud nii, et ettekirjutus tehakse konkreetsele üliolulisele üksusele, kes peab juhatuse liikme volitused ajutiselt peatama. NIS2 direktiivi tekst jätab iseenesest liikmesriikidele võimaluse juhatuse liige tagasi kutsuda „kooskõlas liikmesriigi õigusega". Eelnõu koostamisel ja kooskõlastamisejärgselt kaaluti põhjalikult, kas artikli 32 lg 5 punkti b ülevõtmiseks on alternatiivseid ja Eesti õigusesse paremini sobivaid meetmeid, ning jõuti järeldusele, et ei ole. Advokatuuri viidatud HKMS-is sätestatud haldustoimingu tegemiseks halduskohtult loa taotlemine ei sobi põhjusel, et see kohaldub üksnes haldustoimingutele HMS § 106 mõttes. Otsus nõuda juhtorgani liikme volituste peatamist on oma olemuselt haldusakt HMS § 51 lg 1 tähenduses. Sellega kehtestatakse järelevalve subjektile kohustus (ja piiratakse tema õigusi). Seega on tegemist sisuliselt ettekirjutusega, nii nagu see ongi eelnõus ette nähtud. Sellest tulenevalt ei ole HKMS § 264 sätestatud haldustoiminguks loa küsimine sellises olukorras kohaldatav (see saaks kohalduda üksnes juhul, kui tegemist oleks haldustoiminguga, aga tegemist on haldusakti andmisega). Haldusakti andmisele ei ole HKMS § 264 haldustoimingu tegemiseks loa andmisega võrreldavat regulatsiooni olemas. Samuti ei oleks selliste nõuete esitamine kohtu kaudu otstarbekas ka põhjusel,

	nõukogu liikme või osaniku kaitseks. Samuti ei täpsustata, kuidas toimub sellise erandliku ja Eesti õiguskorras ebatavalise meetme kohaldamise menetlus. Mõistlik oleks lähtuda HKMS-s sätestatud haldustoiminguks loa taotlemise regulatsioonist. Soovitused: 1. Kaaluda, kas juhatuse liikme volituste peatamise meetme kohaldamine on kooskõlas NIS2 direktiiviga ja Põhiseadusega. 2. Täpsustada meetme kohaldamise menetlust tagamaks asjaosalistele õigusriiklikud menetluslikud tagatised.	et kohtumenetlus võib võtta aastaid. NIS2 direktiivi artikli 32 lg 5 punkti b kohaldamine on aga mõeldav üksnes väga äärmuslikes olukordades, kus viimase abinõuna tuleb kiirelt ja operatiivselt tegutseda. Riigi Infosüsteemi Ameti ettekirjutus allub kohtulikule kontrollile. Üliolulisel üksusel on võimalik esitada selle peale halduskohtusse kaebus ja nõuda ka ettekirjutuse täitmise peatamist esialgse õiguskaitse korras. Üliolulisele üksusele on tagatud kõik halduskohtumenetluses ette nähtud tagatised, sellele eelnevas faasis kohalduvad Ametile kõik HMS-is ette nähtud nõuded haldusmenetluse läbiviimisele. Täiendavalt selgitame, et sarnast lahendust, kus pädev järelevalveasutus nõuab otse järelevalvesubjektilt endalt juhatuse liikme tagasikutsumist, on kasutatud ka teiste riikide NIS2 direktiivi ülevõtmiseks koostatud eelnõudes. Näiteks on see selliselt kavandatud Eesti õiguskorra kujundamisel oluliseks eeskujuks olnud Saksa Liitvabariigi vastavas seaduseelnõus. Lisaks eeltoodule märgime, et avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17.
20.11	Eelnõu rakendamise osas puudub õigusselgus Eelnõu seletuskirjas on märgitud, et [KüTSi] lisanduvatele organisatsioonidele nähakse ette kolmeaastane üleminekuaeg, mille jooksul tuleb oma tegevus viia küberturvalisuse seaduse põhiliste nõuetega kooskõlla. Samas puudub vastav teave seaduse eelnõu tekstis ning viidatud tähtaeg näib tulenevat üksnes rakendusmääruse eelnõust „Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine“. Viidatud määruse eelnõu käsitleb vaid standardite (E-ITS või ISO/IEC 27001) rakendamise kohustust, kuid küberturvalisuse seaduse eelnõuga kaasnevad täiendavad kohustused mitte ainult uutele vaid ka juba olemasolevatele subjektidele.	Arvestatud – vt eelnõu KüTS §-e 4^1 ja 28^1. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.

	Kehtiva küberturvalisuse seaduse kohaselt kohaldatakse seadust teenuse osutajale vaid ulatuses, mis puudutab võrgu- ja infosüsteeme. Eelnõu kohaselt tuleb aga seadusest tulenevaid nõudeid rakendada kogu organisatsioonile tervikuna, mistõttu peaks ilmselt olema üleminekuaeg mitte üksnes uutele subjektidele vaid ka olemasolevatele. Soovitused: 1. Eelnõus peaks ette nähtud üleminekuaeg kehtima mitte ainult [KüTSi] lisanduvatele subjektidele, vaid ka juba olemasolevatele subjektidele. 2. Arvestades, et seaduse eelnõuga laieneb [KüTSi] kohustatud subjektide ring, peaks õigusselguse tagamiseks vastav teave uutele subjektidele olema paremini kommunikeeritud, näiteks eelnõu seletuskirja lisatavate täiendavate selgituste kaudu.	
21. Tervisekassa arvamus 31.01.2025 kiri nr 1.5-1/16293-1		
21.1	Eelnõu sõnastuse kohaselt laiendatakse küberturvalisuse seaduse (KüTS) subjektide ringi. Juhime tähelepanu, et sõnastuse kohaselt kohalduks KüTS perearstiabi osutajale, kes ei ole elutähtsa teenuse osutaja, olenemata tema suurusest. Tervisekassa hinnangul on kohustusega kaasnevad nõuded enamikele perearstiabi osutajatele ebaproportsionaalsed (nt KüTS-i rakendamisega seotud kulu ning auditi kulu ca 30 000 - 50 000 eurot 3 aasta lõikes) ning ei võta arvesse perearstiabi osutaja suurust. ˇ	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

	Teeme ettepaneku kohaldada nõuet proportsionaalselt vastavalt perearstiabi osutaja suurusele.	
22. Alkoholitootjate ja Maaletoojate Liidu arvamus 11.02.2025 kiri		
22.1	Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõu (edaspidi eelnõu) seletuskirja kohaselt on eelnõu eesmärgiks võtta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555 üle kitsalt ehk minimaalsel vajalikul tasemel. Kooskõlastamisele esitatud eelnõu kohaselt on: - elutähtis üksus, kellel on majandusaasta jooksul keskmiselt 250 või rohkem töötajat ja kelle aasta bilansimaht ületab 50 miljonit eurot või aastakäive ületab 43 miljonit eurot, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ning kes on osutatud vähemalt ühes eelnõu § 1 lõike 12 punktides 1–51. - oluline üksus, kellel on majandusaasta jooksul keskmiselt rohkem kui 50 töötajat ja kelle aasta bilansimaht on vahemikus 10–43 miljonit eurot ning aastakäive on vahemikus 10–50 miljonit eurot, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ja kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 12 punktides 1–51.	Osaliselt arvestatud ja selgitatud Eelnõud on parandatud ning on selgemalt välja toodud, milliste üksuste valdkonnad on seotud NIS2 direktiivi I või II lisaga – toidu valdkonnaga seotud üksused on oluliste üksuste grupis. Seda on tehtud eelnõu KüTS §-s 3. Eelnõuga ei ole NIS2 direktiivi kohaldamisala laiendatud, sest direktiiv ei võimalda direktiivi lisas II nimetatud üksuste puhul teha erandeid nende olulisuse järgi, mh näiteks toiduainete kategooriate järgi. Siin vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.

	Punkt 45 osundab toidukäitlemisettevõtjatele, millest võib järeldada, et eelnõu loeb kõik eelnimetatud käibe ja töötajate arvu lävendit ületavad toidusektori ettevõtted vastavalt elutähtsateks või olulisteks. Direktiivi artikkel 2 lõike 1 kohaselt käsitatakse elutähtsate üksustena direktiivi I lisas osutatud liiki üksuseid, mis ületavad soovituse 2003/361/EÜ lisa artikli 2 lõikes 1 esitatud keskmise suurusega ettevõtja ülemmäärasid ning muid I ja II lisas osutatud liiki üksused, mida liikmesriik käsitab elutähtsa üksusena direktiivi artikli 2 lõike 2 punktide b–e kohaselt. Direktiivi artikkel 2 lõike 2 punktid b-e on järgmised: „b) *üksus on liikmesriigis sellise teenuse ainuosutaja, mis on kriitilise tähtsusega ühiskondliku või majandustegevuse säilitamiseks;* *c) üksuse osutatava teenuse häirel võib olla oluline mõju avalikule turvalisusele, avalikule julgeolekule või rahvatervisele;* *d) üksuse osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju;* *e) üksus on kriitilise tähtsusega oma erilise olulisuse tõttu riiklikul või piirkondlikul tasandil konkreetse sektori või teenuseliigi või liikmesriigi muude üksteisest sõltuvate sektorite jaoks*;“ Direktiivi artikkel 3 lõige 2 määratleb olulised üksused:	

	„*Käesoleva direktiivi kohaldamisel käsitatakse oluliste üksustena I või II lisas osutatud üksusi, mis ei kvalifitseeru käesoleva artikli lõike 1 kohaselt elutähtsateks üksusteks. See hõlmab üksusi, mida liikmesriigid käsitavad oluliste üksustena artikli 2 lõike 2 punktide b–e alusel*.“ Toidukäitlemisettevõtted on käsitletud direktiivi lisas II (mitte lisas I). Kooskõlastamisele esitatud eelnõu loeb seega toidukäitlemisettevõtted kaalutlemata elutähtsateks või olulisteks kuigi direktiiv seda ei nõua. Eeltoodust lähtuvalt, võime tõlgendada, et olulised ja elutähtsad üksused ei ole mitte kõik direktiivi lisas II nimetatud sektorites käibe ja töötajate arvu kriteeriumidele vastavad ettevõtted, vaid ettevõtted, mida liikmesriik otsustab direktiivi artikkel 2 lõikes 2 punktides b – e toodud kriteeriumidele vastavalt elutähtsaks või oluliseks lugeda. Leiame, et kõik toidukäitlemisettevõtted sõltumata toodangust ei ole riigi ja ühiskonna toimimiseks või elanikkonna kaitseks kriitilise tähtsusega ning alkoholitootjad ja maaletoojad, ei vasta direktiivi artikkel 2 lõikes 2 punktides b – e toodud kriteeriumidele, mistõttu ei ole põhjust ka alkoholitootjad ja maaletoojaid eelnõu subjektide hulka arvata. Peame otstarbekaks võtta direktiiv üle minimaalselt vajalikul tasemel, sh põhjendatult tarviliku subjektide nimekirjaga, et eelnõu ei kahjustaks Eesti ettevõtete konkurentsivõimet ega hoogustaks inflatsiooni.	

23. Eesti Haiglate Liidu arvamus 27.01.2025 kiri nr 116-2B		
23.1	Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 (edaspidi NIS2) artikkel 21 lõige 2 (d) käsitleb küberturvalisuse riskijuhtimise meetmeid, mida elutähtsad ja olulised üksused peavad rakendama. NIS2 kohustab elutähtsaid ja olulisi üksuseid rakendama kõiki ohte hõlmaval lähenemisviisil asjakohaseid ja proportsionaalselt tehnilisi, tegevuslikke ja korralduslikke meetmeid, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, et ennetada või minimeerida intsidentide mõju nende teenuste saajatele ja muudele teenustele. NIS2 rõhutab riskide juhtimist ja proportsionaalsust, samas kui küberturvalisuse seaduse eelnõu § 7 lõige 2 punkt 6 kehtestab turvameetmete rakendamisel üldise kohustuse *"Tagama süsteemi tarneahela turvalisuse"*. Meie hinnangul võib nõue olla ebarealistlik, sest teenuse osutajal ei pruugi olla alati täielikku kontrolli kogu tarneaheale üle, eriti kui tegemist on suuremahuliste ja keerukate tarneahelatega. Tarnijate ja koostööpartnerite regulaarne hindamine suurendab ka teenuseosutajate halduskoormust ja võib põhjustada tarnekatkestusi, kui tarnijad ei vasta kehtestatud turbenõuetele. **Teeme ettepaneku muuta eelnõu [KüTS] § 7 lõige 2 punkte 1 ja 6 alljärgnevalt:** (2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:	Selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). Avalikul kooskõlastusringil olnud eelnõus oli proportsionaalsuse ja riskipõhise lähenemisviisi temaatika sisustatud KüTS § 7 lõikes 2^1, mis oli omakorda seotud sama paragrahvi lõikega 2. Too lõige 2^1 hõlmas ka tarneahelaga seotud nõudeid, mis olid sätestatud lõikes 2. Kuna eelnõu ülevaatamise käigus on KüTS § 7 sõnastust muudetud, siis avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lg 2^1 on nüüdsest sama paragrahvi lõikes 2. Ka uuendatud sõnastuses on jätkuvalt sees proportsionaalsuse arvestamine, sh riskipõhise lähenemisviisi kasutamine.

	1) koostama ja kehtestama infoturvariskide kaalutlemise metoodika ja protseduurid (sh rakendama proportsionaalseid riskijuhtimise meetmeid süsteemi tarneahela turvalisuse tagamiseks); 6) tagama koostööpartnerite vahelistes lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise; Ettepanekus välja toodud täpsustus "proportsionaalsed riskijuhtimise meetmed" muudab nõude paindlikumaks ja võimaldab teenuse osutajatel kohandada riskijuhtimise meetmeid vastavalt oma suurusele, riskitasemele ja ressurssidele. Samuti vähendab muudatus ebarealistlikke ootusi, mille kohaselt peab teenuse osutaja turvameetmete rakendamisel "tagama süsteemi tarneahela turvalisuse". Lisaks suurendab muudatus vastavust NIS2 direktiivi artikli 21 nõuetega, mis rõhutavad proportsionaalsust ja riskipõhist lähenemist. Eelnõu [KüTS] § 7 lõike 2 punkti 6 täpsustus keskendub konkreetsele tegevusele ja vähendab üldistust ning suunab tegevust paremini.	
23.2	**Tähelepanekud seoses [KüTS] paragrahvi 14 lõigetega 9-10, mis on eelnõus sõnastatud järgmiselt:** *(9) Riigi Infosüsteemi Ametil on riikliku ja haldusjärelevalve läbi viimisel õigus teha:* *2) teenuse osutaja suhtes sihipäraseid turvaauditeid, mis põhinevad Riigi Infosüsteemi Ameti või auditeeritava teenuse osutaja tehtud*	Selgitatud Mõistame, et uute reeglitega rakendamisega kaasnevad kulud. NIS2 direktiivi artikli 32 lõike 2 kolmanda tekstilõike teine lause ja 33 lõike 2 kolmanda tekstilõike teine lause on mõlemad esitatud sõnastuses: *„Sõltumatu organi poolt läbi viidava **sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti**."*. Samas ei näe NIS2 direktiivi vastavad artiklid ette erinevate eelnõu kohaldamisalasse jäävate subjektide eristamist.

	riskihindamisel või muul kättesaadaval riskialasel teabel; *(10) Käesoleva paragrahvi lõike 9 punktis 2 nimetatud sihipärase turvaauditi:* *4) kulud kannab auditeeritav teenuse osutaja, välja arvatud juhul, kui Riigi Infosüsteemi Amet põhjendatul juhul otsustab teisiti.* Juhime tähelepanu, et eelnõu [KüTS] § 14 lõike 10 punkt 2 ei arvesta teenuse osutaja suurust ega ressursse, määrates vaikimisi kõik auditi kulud automaatselt teenuse osutaja kanda, välja arvatud juhul kui Riigi infosüsteemide Amet otsustab teisiti. Selline nõue võib olla väiksemate haiglatele või organisatsioonidele liialt koormav, eriti kui auditid on ulatuslikud ja kulukad. Kulude prognoosimatus raskendab eelarve planeerimist ja võib piirata organisatsiooni võimekust investeerida ennetusmeetmetesse.	Lisaks eeltoodule märgime, et kommentaaris olev teema on viidud KüTS § 16 lõike 1^2 ja § 17 lõike 1^2 alusel antava ministri määruse kavandisse, milles sätestatakse ka loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale sihipärase turvaauditi kulu.
23.3	**Tähelepanekud seoses [KüTS] paragrahvi 14 lõigetega 13-14, mis on eelnõus sõnastatud järgmiselt:** *(13) Kui elutähtis üksus ei kõrvalda puudusi või ei täida Riigi Infosüsteemi Ameti nõudeid käesoleva paragrahvi lõike 12 alusel määratud tähtajaks, on Riigi Infosüsteemi Ametil õigus nõuda ettekirjutusega:* *1) elutähtsa üksuse kõigi või mõnede osutatavate asjaomaste teenuste või tegevuste sertifikaadi või loa ajutist peatamist loa väljastajalt, või vastava pädevuse olemasolul teha ise nimetatud toiminguid;*	Selgitatud NIS2 direktiivi artikli 32 lõige 5 näeb ette sellised meetmed, mida Riigi Infosüsteemi Amet saab kasutada nö „viimase võimalusena“, kui muud meetmed ei ole andnud tulemust, üksusele on määratud puuduste kõrvaldamiseks täiendav tähtaeg, mis on edutult möödunud. Samuti on oluline, et meetmed on ajutised ja neid saab kohaldada üksnes nii kaua, kui ülioluline üksus puudused kõrvaldab. Riigi Infosüsteemi Amet peab hindama, kas see on kõige sobivam meede konkreetses olukorras tekkinud probleemi lahendamiseks ehk tegemist ei saa olla kergekäeliselt kasutatava meetmega. Seega võib eeldada, et nende meetmete rakendamine toimub praktikas äärmiselt erandlikel juhtudel. Mõistame küll, et teatud ülioluliste üksuste suhtes võib kommentaaris mainitud meetmete rakendamine olla suure mõjuga. Samas ei näe NIS2 siin ette võimalust teatud sektoreid või teatud subjekte selle regulatsiooni alt välistada. Seetõttu tuleb direktiivi korrektseks ülevõtmiseks sätestada vastavad sätted selliselt, et

	2) elutähtsa üksuse nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist. *(14) Käesoleva paragrahvi lõike 13 punktides 1 ja 2 sätestatud meetmeid:* *1) kohaldatakse seni, kuni kõnealune elutähtis üksus võtab kasutusele vajalikud meetmed puuduste kõrvaldamiseks või Riigi Infosüsteemi Ameti esitatud nõuete täitmiseks.* Meie hinnangul võib eelnõu [KüTS] § 14 lõike 13 punkt 1 takistada haiglate poolt osutatavate elutähtsate teenuste osutamist ja mõjutada otseselt ühiskonna toimimist. Kui tervishoiuasutuse (nt haigla) teenused peatatakse, võib see ohustada patsientide elu ja tervist. Teenuste ajutine peatamine võib põhjustada pikaajalisi häireid, mille taastamine võib olla ressursimahukas ja tuua tervishoiuasutustele kaasa ettenägematuid kulutusi. Eelnõu [KüTS] § 14 lõike 13 punkt 2 võib tekitada juhtimislünki, eriti väiksemates asutustes, kus juhtimisstruktuuride asendusmaatriks on kirjeldamata või asendusmaatriksi olemasolu ei ole võimalik tagada. Eelnõu [KüTS] § 14 lõike 14 punkt 1 võib kaasa tuua olukorra, kus teenuste ajutine peatamine võib häirida elutähtsate funktsioonide osutamist. Küberturvalisuse meetmete rakendamine (sh puuduste kõrvaldamine) võib olla tehniliselt keerukas, kulukas ja ajamahukas ning seda eriti väiksemate asutuste puhul. Piiratud ressurssidega organisatsioonidel võib puuduste kõrvaldamiseks kuluda oluliselt rohkem aega, mis pikendab	see kohaldub kõikidele üliolulistele üksustele, sh elutähtsa teenuse osutajatest tervishoiuteenuse osutajatele. Juhatuse liikme volituste ajutine peatamine ei tähenda, et vahepealsel ajal ei ole võimalik määrata uut juhatuse liiget, kes tol perioodil saab tegeleda puuduste kõrvaldamisega. Lisaks eeltoodule märgime, et avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17.

	teenuste või volituste peatamise perioodi ja võib kaasa tuua täiendavat finantskoormust ja mainekahju. Lisaks tekib ebaselgus, kuidas tagada asutuses turvameetmete rakendamine ja puuduste kõrvaldamine olukorras, kus asutuse vastutava juhi volitused on peatatud.	
24. Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu arvamus 31.01.2025 kiri nr 6.1-2/13		
24.1	**Peamised murekohad ja ettepanekud** Küberturvalisuse nõuete järgimine parandab ettevõtete ja asutuste toimepidevust ning konkurentsivõimet nii Eestis kui ka rahvusvaheliselt. Oleme üldiselt nõus, et eelnõuga laieneb kehtiva KüTS-i mõjuala kuid kohaldamisala laiendamine peab olema põhjendatud ja läbi mõeldud. ITL toetab NIS2 direktiivi eesmärke, eriti nõuete ja protseduuride ühtlustamist üle Euroopa Liidu. Leiame, et regulatsiooni eesmärk peab olema ka selle subjektidele väärtust luua, sealhulgas läbi selguse ja reaalselt parema küberturvalisuse. **Kahjuks on eelnõus väga mitmeid probleeme, millest peamised on kokkuvõtlikult järgmised:** **1) Ülevõtmise eelnõuga NIS2 direktiivi kohaldamisala põhjendamatu laiendamine** Eestis, seda nii subjektide nimekirja pikendamise kui ka kohaldamisalas olevate teenusete keskselt lähenemiselt kogu ettevõtte tegevuse hõlmamisele üleminekuga; **2) Eelnõu jõustamisega kiirustamine ettevõtetele mõistlikku rakendusaega jätmata** – üleminekuaega vajavad kõik subjektid (nii	Võetud teadmiseks, sh allpool on vastatud tõstatatud probleemidele.

	eelnõuga lisanduvad kui ka kehtiva KüTS-i subjektid selleks, et tagada võrdne kohtlemine); **3) Eelnõu madal normitehniline kvaliteet ja vastuolu hea õigusloome tavaga**, mille tagajärjeks on regulatsiooni ebaselgus. Segane sõnastus nii olulises valdkonnas viib kaugemale õigusselgusest ning vähendab seega küberturvalisust. **Järgnevalt põhjendame oma seisukohti lähemalt ning esitame ka oma ettepanekud välja toodud murekohtade lahendamiseks.**	
24.2	Eelnõu materjalidega tutvuma asudes jääb esimesena silma, et puudu on eelnõu vastuvõtmise fookus ja eesmärk, mida Eestis saavutada tahetakse. Millist probleemi selle eelnõuga lahendatakse? Seda pole välja toodud. Mõistame, et tegemist on EL-i direktiivi ülevõtmise eelnõuga ja NIS2 direktiivi eesmärke me toetame. Siiski on tegemist eelnõuga, mis sätestab mitmeid uusi kohustusi väga suurele hulgale ettevõtetele ja asutustele. Seetõttu on vajalik ka selgesõnaliselt põhjendada, miks Eestis seadus sellisel kujul kavatsetakse vastu võtta. Ühe selge eesmärgi sõnastamine aitaks kindlasti kaasa kohustatud isikute suunas vajalikule selgitustööle. See aitaks põhjendada miks selliseid kohustusi kehtestada on vaja ja mis kasu nendest kohustatud isikutele endale sünnib. ITL-i ettepanek: sõnastada selgelt, mis on eelnõu eesmärk ehk mille vastu need meetmeid kasutusele võetakse. Näiteks, et eelnõu eesmärk on kaitsta kriitiliste teenuste osutamist Eestis või et proportsionaalsed nõuded on vajalikud selleks, et	Arvestatud – seletuskirjas on eelnõu eesmärki täiendatud.

	ennetada teatud tagajärgi. Soovitame siduda eelnõu eesmärgi ka Eesti ettevõtete ja majanduse konkurentsivõime paranemisega.	
24.3	Eelnõuga laiendatakse kehtiva KüTS-i kohaldamisala väga oluliselt ja rohkem kui NIS2 direktiiv seda ette näeb. See on risti vastupidine tegevus Vabariigi Valitsuse prioriteetsele eesmärgile, mille kohaselt tuleb ettevõtete halduskoormust ja dubleerivaid tegevusi vähendada. Eelnõu jõustumine toob kaasa äärmiselt suure halduskoormuse kasvu väga suurele hulgale ettevõtetele, sealjuures võrgu - ja infosüsteemide osas ilmselt kattuvalt (üht ja sama võrku või infosüsteemi hakatakse kontrollima teenuse kasutaja ja teenuse osutaja ning vahendaja poolt). Samuti lisandub suur täiendav koormus ka erinevatele riigiasutustele, kes peaks praegu hoopis kokkuhoiu kohti leidma. Eesti õigusega NIS2 direktiivi laiendamine ei ole kooskõlas ka NIS2 eesmärgiga ühtlustada küberturvalisuse nõudeid üle kõigi EL-i riikide, sest teiste riikidega võrreldes on Eestis juba tänase KüTS regulatsiooniga saavutatud märkimisväärselt kõrge turvalisuse tase. NIS2 direktiivi KÜTS-i ülevõtmine laiendavalt on kavandatud näiteks järgmisega: - ettevõtted, kelle üks teenus kuulub NIS2 direktiivi lisades 1 ja 2 nimetatud sektoritesse, peavad eelnõus sätestatud meetmed kohaldama kogu oma tegevusele, mitte üksnes NIS2 direktiivis nimetatud teenuste osutamisele. KüTS-i kohaldamisalasse kuuluv teenus võib olla ettevõtte enda vaates kõrvaltegevus või	Osaliselt arvestatud ja selgitatud vastavalt kommentaaris esitatud ettepanekutele - Arusaamatuks jääb, milles seisneb laiendav ülevõtmine. Eelnõu koostades on üle vaadatud eelnõu sõnastust ning selles ei ole uusi KüTSi subjekte, keda NIS2 direktiiv ette ei näe (v.a näiteks üksikud avalikku sektorisse kuuluvad subjektid, kelle suhtes soovitakse ka NIS2 direktiivi üle võttes seaduse järgimise kohustus säilitada). Eelnõud koostades on lähtutud võimalikult suurel määral NIS2 direktiivi enda sõnastustest KüTSi uute subjektide sõnastamisel. - NIS2 direktiivis toodud kohaldamisala (subjektide ringi) saab kitsendada ainult direktiiviga ettenähtud määral, mitte enam ega meelevaldselt. Oleme teadlikud teatud riikide erinevast lähenemisest ja küsinud ka selgitusi, kuid täna puuduvad veenvad põhjendused, et sellised lähenemised on direktiiviga kooskõlas - pigem vastupidi võrreldes Lääne-Euroopa riikidega. Taustainfoks tasub teada, et sama küsimust on teisedki liikmesriigid põhjalikult vaaginud, kes on juba NIS2 direktiivi üle võtnud ning on andnud selle kohta välja ka selgitavaid materjale. Näiteks on soovi korral võimalik tutvuda ka Belgia kuningriigi pädeva asutuse vastavate selgitustega siin (lk 8 alajaotis B) ja siin (nt lk 8, lk 11, lk 12). Seetõttu on esimene ettepanek arvestatud ja täidetud. - NIS2 direktiiv näeb sõna-sõnalt ette üksuse (jur.isik) põhised kohustused, mitte teenuse põhised kohustused. NIS2 direktiivi kohaselt on kohustatud isikuks „üksus“, mis on direktiivis esitatud definitsiooni järgi juriidiline või füüsiline isik ehk organisatsioon tervikuna. NIS2 direktiiv ei tekita võimalust kitsendada KüTSi nõuete rakendamist kitsalt ehk konkreetse teenuse või tegevusega seonduvalt. Taoline erisus (tegemist on KüTSi teenuseosutajaga siis, kui mingi valdkonnaga seotud tegevusala on väheoluline osa tema kõikidest tegevustest) on NIS2 direktiivis ette nähtud ainult üksikute valdkondade puhul (nt reovee valdkonnas). Kui taolist põhimõtet rakendada ka muude valdkondade puhul, kus NIS2 direktiiv ise ei näe ette kitsendust, siis selline tegevus ei ole NIS2 direktiiviga kooskõlas.

	ebaproportsionaalselt väikese mahuga võrreldes KüTS-i kohaldamisega kaasnevate kohustustega. Sellisel viisil terve ettevõtte üle kontrolli teostamine ja ülemäärane reguleerimine ei ole põhjendatud; - turvanõuete koosseisu ja kohustuste vähesel määral täiendamine. Samas seda tehakse nii, et need subjektid, kes peavad oma vastavust rahvusvaheliselt tõendama, peavad eelnõu vastuvõtmisel hakkama selle protsessi käigus selgitusi jagama, millised nõuded on Eestis siseriiklikult juurde lisatud. See suurendab taaskord halduskoormust. Kehtiva KüTS-i laiendamise näite leiame eelnõu § 1 punktiga 27 **KüTS-i lisatavast § 7 lõige 2[1]. See tekitab segadust, kuna sätestab E-ITS-iga samad reeglid ja ka eelnõu seletuskirjas viidatakse otseselt E-ITS-ile. Kuivõrd KüTS § 7 lg 5 jääb samale kujule (ei plaanita eelnõuga muuta), siis tekib olukord, kus ettevõtted ja nende teenuse osutajad, kes vastavad ISO 27001 standardile, peaksid justkui hakkama rakendama lisaks ka E-ITS-i. Kuigi E-ITS koostamisel on kinnitatud, et on järgitud ISO 27001 reegleid, siis tegelikkuses ei ole seda täiesti üksühele tehtud. Näiteks standardist ISO 27001 ei tule välja samas sõnastuses mõisted ega ole reguleeritud eraldi kaitsetarbe määramise osa. Eelnõu seletuskirjas ei ole hetkel selgitatud, kuidas ISO 27001 rakendajad seda nõuet peaks täitma. Sellise tõlgenduse kohaselt tõuseksid täiendavate auditeerimise kohustustega ka**	Turvameetmete (NIS2 direktiivis riskijuhtimismeetmete) teema osas juhime ka tähelepanu Euroopa Komisjoni suunistele NIS2 artikli 4 lõigete 1 ja 2 kohaldamise kohta. Suuniste punkti 7 viimases lauses on selgitatud: „*Direktiivi (EL) 2022/2555 artikli 21 lõikes 1 sätestatud kohustus, mille kohaselt peavad [üliolulised] ja olulised üksused võtma asjakohaseid ja proportsionaalseid küberturvalisuse riskijuhtimismeetmeid, kehtib kõigi asjaomase üksuse tegevuste ja teenuste suhtes ega puuduta üksnes konkreetseid infotehnoloogia („IT“) varasid või [üliolulisi] teenuseid, mida üksus osutab.“* Seega ei oleks ka kommentaaris pakutud „vähetähtsa määra“ või „ainult KüTSis sätestatud teenusega subjektiks saamise“ variant ka kasutatav, kui Komisjoni enda suuniste kohaselt tuleb näiteks turvameetmete nõudeid kohaldada konkreetse üksuse kõikide tegevuste ja teenuste suhtes. Seetõttu ei ole võimalik kommentaaris tehtud teist ettepanekut täiel määral arvestada – vastasel juhul toimuks NIS2 direktiivi väär üle võtmine ning rakendamine. Vt siin täiendavalt ka Sotsiaalministeeriumi kommentaari 9.1 selgitust. - Kommentaaris tehtud kolmanda ettepaneku osas selgitame, et eelnõust on eemaldatud sõna „kaitsetarve“. Sellest hoolimata juhime tähelepanu asjaolule, et kuigi Eesti infoturbestandard kasutab sõnastust „kaitsetarve“, siis seda kasutab ka rahvusvaheline standard ISO/IEC 21964 – selle mõiste selgitus on AKIT-i kohaselt „*andmete ja teabe omadus, mis väljendub vajadust kaitsta teda kahju eest, mida võib tekitada konfidentsiaalsuse, tervikluse ja/või käideldavuse rikkumine; kaitsetarve on normaalne, suur või väga suur; andmekandjate hävitamisel on andmekandja kaitse klass seda kõrgem, mida suurem on andmete kaitsetarve“*. Seega ei ole kaitsetarbe puhul tegemist ainult Eesti infoturbestandardis sisustatud mõistega. Siin vt ka Riigi Infosüsteemi Ameti kommentaari 17.40 vastust.

	ettevõtetele kulud, mida hetkel ei ole arvestatud. Seletuskirjas ei ole täpsustatud ka ISO standardiga seotud osa, nt kuidas ISO 27001 rakendajad peavad vastama E-ITS või nüüd tulevikus KüTS § 7 lg 1[2] kaitsetarbe nõudele, mis on standardist õigusakti tasemele toodud. Seletuskirjas ei ole ka selgitust sellisel kujul standardi nõuete seadusesse kirjutamise kohta. ITL-i ettepanek: mitte laiendada direktiivi kohaldamisala ja selles sisalduvaid kohustusi. Ettevõtete halduskoormus ja vastavuskulud on niigi suured. Seetõttu palume: - tagada eelnõus mõistlik subjektide ring; - muuta eelnõud nii, et ettevõtted on KÜTS-i kohaldamisalas ainult oma NIS2 kohaldamisalasse jääva tegevusega; - kõrvaldada eelnõust ebaselgus seoses E-ITS standardi nõuetega ISO 27001 rakendajatele, kuna määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 3 lg 2 kohaselt loetakse ISO 27001 standardile vastavus võrdseks E-ITS-ile vastavusega. Põhjendame oma ettepanekuid järgmiselt: - Eesti on väike riik, me peame mõtlema, millised on reaalsed ohud ja millised on reaalsed riskid ning kõrvutama seda sellega, mis läheb selle haldus maksma. Meie üleskutse on läbi mõelda, kuidas teha neid asju mõistlikumalt, läbimõeldumalt ning proportsionaalsetena. - Subjektide nimekirja üle vaatamine ja sisulise kohaldamisala kitsendamine ning dubleerivate elementide eemaldamine vabastab ka	

	asutuste ressurssi. Sellisel juhul ei pea nii suure hulga asutuste ja ettevõtete üle järelevalvet teostama, neid nõustama ja juhendama olukorras, kus tegelik mõjuulatus on väike või olematu. Selle asemel saab keskenduda olulise mõjuga teenuste turvalisuse tagamisele ja tõstmisele. - NIS2 direktiivi ülevõtmisega ei tohi kaasneda näiteks turvanõuete või ainult Eestis kohaldatavate kohustuste lisamist, et mitte tekitada liiga palju riiklikke eripärasid, mis muudavad keerukamaks ja kallimaks Eesti teenused ja tooted ning annavad teistele konkurentsieelise. Kui teenuseosutajat hakatakse sertifitseerima näiteks EL-i küberturvalisuse sertifitseerimisskeemi alusel, siis KüTS-i eripärad tekitavad keerukust ja bürokraatiat, samuti ebavõrdsust erinevate riikide järelevalve alla kuuluvate teenusosutajate vahel. - Senise teenusepõhise lähenemise juurde jäämist toetab ka see, et nii või teisiti peavad seonduvad süsteemid ja tegevused, sh partneritega seonduv olema riskihinnangus kajastatud, hinnatud ja turvalisus tagatud. Ettevõte tervikuna ei peaks siiski olema Riigi Infosüsteemi Ameti (RIA) poolt kontrollitav. RIA kontroll võib olla ebaproportsionaalne ja ülemäärane ettevõtte üle tervikuna, kui KüTS kohaldamisala alla jääv teenus ei ole ettevõtte põhitegevus.	
24.4	Eelnõu jätab KüTS kohuslaste nimekirja lahtiseks, kuna kehtestab Vabariigi Valitsuse jaoks volitusnormi (eelnõu § 1 p 1 - KüTS § 1 lg 1^6) uute kohuslaste lisamiseks määrusega. Näeme seoses sellega mitmeid olulisi probleeme:	Arvestatud – vastavad sätted on välja jäetud.

	— Kavandatav volitusnorm on liiga lai. See on seotud eelnõu § 1 punktiga 1 KüTS § 1 lisatavas lg 1^4 toodud kriteeriumitega, kuid siiski jääb ebaselgeks, millistel alustel uusi subjekte lisama hakatakse ning kas seejuures saab olema tagatud võrdne kohtlemine. — Volitusnormi lisamise põhjus on arusaamatu. Miks see on lisatud ja mis mõju sellest oodatakse? Eelnõu seletuskirja lugedes jääb mulje nagu oleks see säte lisatud igaks juhuks, kui keegi eelnõust kogemata välja on jäänud. Samal ajal on subjektide ring juba eelnõus toodud loetelu kohaselt väga laiaulatuslik ja ebamäärane (ei saa aru, kellele see kohaldub). — Volitusnormi lisamise põhjendus jääb arusaamatuks ka seetõttu, et eelnõu seletuskirjas (lk 53-54) juba kirjeldatakse võimalikke uusi sektoreid kes võiksid saada KÜTS-i kohuslasteks, kuid hiljem (lk 129) öeldakse, et volitusnormi ei plaanita siiski kohe kasutada ehk tegu on tuleviku jaoks mõeldud paindlikkust lisava võimalusega. — Volitusnormi lisamine läheb vastuollu seaduse mõttega. Osa subjekte määratakse kohe seadusega ja teised hiljem rakendusaktiga. Leiame, et subjektide lisamine peab toimuma kõigi jaoks sama õigusakti (ehk siis seaduse) tasemel. ITL-i ettepanek: jätta eelnõu § 1 punktiga 1 KüTS §-i 1 lisatav lõige 1^6, millega antakse Vabariigi Valitsusele õigus määrata määrusega valdkonna või sektori, milles oleva isiku suhtes kohaldatakse teenuse osutaja kohta sätestatut olenemata tema	

	suurusest, eelnõust välja. Samuti jätta eelnõust välja seotud säte KüTS § 3 lg 1^4.	
24.5	Eelnõust jääb ebaselgeks, kuidas kohuslaseks olevad isikud teada saavad, et nad eelnõus sisalduvaid kohustusi täitma peavad. Eelnõu § 1 punktiga 18 muudetav KüTS § 3 lg 3 sätestab, et RIA tuvastab iga kahe aasta tagant KüTS-i kohaldamisalas olevad teenuse osutajad. Selleks peavad teenuse osutajad hakkama ise RIA-le infot edastama ja RIA omakorda teavitab Eesti teenuse osutajatest Euroopa Komisjoni. Sellest protsessist on puudu osa, kuidas teenuse osutajad ise saavad teada, et neile võib kohalduda või RIA neile kinnitab, et nad on tõepoolest KüTS-i kohaldamisalas. ITL-i ettepanekud: - Lisada eelnõusse järgmine protsess: - RIA kohustus teavitada võimalikuks subjektiks saamisest isikuid eelotsusena; - siis antakse ettevõttele või asutusele võimalus ise hinnata ennast (enda tegevust) vastavalt KüTS-is toodud kriteeriumitele; - seejärel väljastab RIA haldusakti, misjärel algab kaheaastane aeg ehk selliselt saaks ka kohuslaseks määramise algusaeg korrektselt fikseeritud. - Lisada eelnõusse RIA kohustus avalikustada KüTS-i subjektide nimekiri koos põhjendusega, miks seal nimekirjas ollakse (s.t viide asjakohasele KüTS-i sättele). Juhul, kui see on vajalik, siis võib anda RIA-le õiguse otsustada	Selgitatud Eelnõu autorid on subjektide ringi ja kohustuste osas viinud sisse või ette valmistamas mõningad riigisisesest õigusest tingitud korrektuurid, kuid valdavas osas tuleb lähtuda NIS2 direktiivis ettenähtud piiridest. Direktiivijärgsest (kohustuslikust) subjektide ringist ei ole võimalik erisusi luua. Pakutud ettepanek (eelotsuse ja haldusakti tegemine) sarnaneb hädaolukorra seaduse alusel toimuva elutähtsa teenuse osutajaks määramise protseduuriga, mis omakorda tugineb CER-direktiivis (direktiiv (EL) 2022/2557) sätestatud kohustuste ülevõtmisele. NIS2 direktiiv aga sellist mehhanismi ette ei näe, sh lähtub direktiiv ise põhimõttest, et KüTSi nõuete alla hõlmatud teenuseosutaja ja domeeninimede registreerimise teenuse osutaja ise annab Riigi Infosüsteemi Ametile teada enda kohta käivatest andmetest. Nende andmete *põhjal* koostab Amet nende üksuste nimekirja, mille avalikustamine ei ole mh julgeolekukaalutlustel mõeldav (viimase osas vt eelnõus KüTS § 3^1 selgitusi). Paralleelselt jätkavad nii Riigi Infosüsteemi Amet kui ka Justiits- ja Digiministeerium koolitus- ja teavitustegevustega.

	mitte kõiki subjekte avalikustada, kuid sellised erandid peavad olema põhjendatud. Samas on oluline, et mitte avalikustatud subjekti lepingupartnerid teaksid tema subjekti staatusest. Põhjendame oma käesolevas punktis tehtud ettepanekuid järgmiselt: - Subjektide nimekirja avalikustamine aitab kaasa avalikule diskussioonile teemal, kellele on mõistlik neid kohustusi kehtestada ja kellele mitte. - Subjektide nimekirja avalikustamine aitab tagada õigusselguse. Ühiskonnale peab olema mõistetav, kes ja miks subjektina KüTS-i kohaldamisalasse hõlmatud on. - Eelnõu konkreetne kohaldamisala ja subjektide avalik nimekiri tõstab riigi turvalisust, kuna võimaldab ettevõtetel ja asutustel koostöös paremini valmistuda võimalikeks kriisiolukordadeks. Näiteks nõutakse eelnõu § 1 punktiga 26 KüTS § 7 lg 2 punktis 6, et teenuse osutaja tagaks süsteemi tarneahela turvalisuse, sh teenuse osutaja ja tema koostööpartnerite vaheliste lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise. Selle kohustuse täitmiseks on abiks, kui teenuse osutaja teab, kes ta partneritest või klientidest ka KüTS-i kohuslased on.	
24.6	Eelnõust jääb ebaselgeks, kuidas hakkab toimuma subjektide lisamine nimekirja ning nende liikumine kahe nimekirja (elutähtsad ja olulised üksused) vahel. Kuna vahe tegemine on seotud ettevõtte	Selgitatud Esitatud ettepaneku lahendus on sees metoodikas, kuidas arvestatakse ning arvutatakse väikese- ja keskmise suurusega ettevõtjate töötajate ning finantsnäitajaid Euroopa Komisjoni soovituse 2003/361/EÜ kohaselt. Seletuskirjas on eelnõu KüTS § 3 juures

	suurusega, nt käibe ja töötajate arvuga, siis saab see olema dünaamiline. ITL-i ettepanek: välja mõelda ja lisada eelnõusse protsess ja mehhanismid olukordadeks, kui ettevõtte suurus muutub kahe aastase perioodi keskel. Kui otsus on, et kaheks aastaks nimekirjad külmutatakse ja liikumist ei toimu, siis selgitada seda vastava sätte juures eelnõu tekstis.	selgitatud vastavat metoodikat. Seetõttu ei ole eelnõuga eraldiseisvat metoodikat või muid nõudeid loodud.
24.7	Eelnõu jõustumisega seonduv on ebaselge. Eelnõu tutvustamisel on Justiits- ja Digiministeeriumi poolt välja öeldud, et uued subjektid saavad ülemineku aja kolm aastat. Eelnõu materjalidega tutvudes sellist sätet ei leia. Eelnõu rakendusakti kavandist (määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine) leiab üleminekuaja uutele elutähtsa teenuse osutajatele (neil on aega KüTS-i rakendamiseks tähtajani, mis määratakse nende elutähtsa teenuse osutajaks määramise haldusaktis). Lisaks on üleminekuaeg 3 aastat ette nähtud kõigile uutele KüTS-i subjektide standardi (E-ITS või ISO/IEC 27001) rakendamise kohustuse osas, kuid mitte muude kohustuste osas. Eelnõus endas rakendusaega (rakendussätteid selle kohta) ei ole. See ei ole loogiline, et eelnõu osade sätete jõustumine pannakse paika Valitsuse määrusega. Eelnõu § 11 kohaselt jõustub kogu eelnõu 1. juulil 2025. aastal ehk kohe pärast vastu võtmist.	Arvestatud – vt eelnõu KüTS §-e 4^1 ja 28^1. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
24.8	Ilmselgelt vajavad uued subjektid ülemineku aega ka muude kohustuste osas. Samuti vajavad seda olemasolevad subjektid, sest täiendavaid kohustusi	Arvestatud – vt eelnõu KüTS §-e 4^1 ja 28^1. Juhime tähelepanu asjaolule, et NIS2 direktiivi artikli 21 lõike 5 alusel kehtestatud rakendusmääruse (EL) 2024/2690 nõuete kehtivus on sõltuvuses rakendusmääruse

	ja uusi nõudeid lisandub ka neile. Näiteks tuleb mitmetel teenuse osutajatel hakata täitma mahukat Euroopa Komisjoni otsekohalduvat rakendusmäärust nr 2024/2690 täpsustatud turvanõuetega, mis suurendab halduskoormust ja tekitab nõuete rakendamisel erisusi. Laieneb kohaldamisalas olevate teenuste ulatus, näiteks usaldusteenuste ja sideteenuste osas. Vähem oluline pole, et muutub ka nõuete kohaldamisala ulatus. Kehtiva KüTS-i kohaselt on teenuse osutajatel kohustused konkreetse teenuse osutamisel süsteemi kasutamisel, eelnõuga planeeritakse kehtestada kohustused kogu ettevõtte tegevusele. Näiteks tuleb täiendada olulisel määral riskianalüüsi, sisseostu protsessi ja lepinguid, koolituspõhimõtteid, auditeerimist ja tagada, et küberturvalisuse meetmed on täidetud kogu ettevõtte puhul. ITL-i ettepanek: lisada eelnõusse rakendussäte, mille kohaselt on kõigil kohustatud subjektidel aega eelnõus sisalduvate kohustuste rakendamiseks 3 aastat alates seaduse avaldamisest Riigi Teatajas. Põhjusel, et KüTS eelnõuga kaasneb täiendavaid kohustusi, siis tuleb üleminekuaeg nende kohustuste osas anda kõigile kohustatud subjektidele, mitte üksnes uutele subjektidele. Selline lahendus tagab ka subjektide võrdse kohtlemise.	aluseks oleva direktiivi üle võtmisest, kuid see siiski ei takista rakendusmääruses nimetatud üksustel (nt usaldusteenuse osutajatel) valmistuda rakendusmääruse nõuetele vastamiseks – isegi siis, kui tegemist ei ole veel selle üksuse suhtes kohalduvate küberturvalisuse nõuetega. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
24.9	Eelnõu jõustumisega seonduvalt vajab selgitamist ka küsimus, millal muutuvad Eestis kohustuslikult täidetavaks Euroopa Komisjoni poolt kehtestatud NIS2 direktiivi otsekohalduvad rakendusaktid.	Selgitatud Kommentaaris mainitud rakendusmäärus on otsekohalduv, kuid praktikas on see otseses sõltuvuses tema volitusnormist ning sellega seotud õigusaktist ehk NIS2 direktiivist. Rakendusmäärus täpsustab NIS2 direktiivi artiklites 21 ja 23 olevaid

	Selles küsimuses esineb erinevaid tõlgendusi (s.h Euroopa Komisjoni ametnike poolt) alates sellest, et otsekohalduvaid rakendusakte peab täitma kohe, kuigi NIS2 pole veel Eesti õigusesse üle võetud kuni selleni, et rakendusaktid ei saa olla kohaldatavad kuni pole siseriiklikus õiguses alusnormi ehk rakendusakti aluseks olev NIS2 pole Eesti õigusesse üle võetud.	nõudeid ehk ta on sõltuvuses siseriiklikust õigusaktist, mis NIS2 direktiivi üle võtab. Kuna NIS2 direktiiv ei ole veel Eesti õigusesse lõplikult üle võetud, siis ei saa rakendusmääruse nõuded ka Eesti puhul ette selles ette nähtud subjektidele kehtida enne siinse eelnõu vastu võtmist ja kehtima hakkamist. See siiski ei tähenda, et rakendusmääruse kohaldamisalas olevad üksused ei saaks enne siinse eelnõu vastu võtmist teha kõik endast oleneva, et siinse eelnõu jõustumisel oleksid nad vastavuses kommentaaris mainitud rakendusmäärusega. Selleks ei pea ootama siinse eelnõu jõustumist.
24.10	Normitehniliselt on eelnõu väga raskesti loetav: — Eelnõu esimesed paragrahvid on väga pikad ja pool NIS2 direktiivist on võetud üle KüTS-i esimesse paari sättesse. Ka muudatuste kogumaht on suurem kui KüTS-i kehtival tekstil. Mitmete pikkade ülamärkega sätete lisamine teeb seaduse lugemise ja sätete seoste jälgimise väga keeruliseks. — Eelnõu sisaldab väga palju viiteid teistele (Euroopa Liidu) õigusaktidele, kusjuures ka küsimustes, mille puhul õigusselgus on äärmiselt oluline, näiteks kohaldamisala. Eelnõu seletuskiri on väga ebaühtlase kvaliteediga. See on väga mahukas, kuid väga paljude sätete selgituseks öeldakse, milline NIS2 artikkel (või põhjenduspunkti tõlgendus, mis tegelikult ei ole õigusnorm) üle võetakse ja seejuures sätte sisu ei selgitata üldse (näiteks eelnõu § 1 punkt 56 - KüTS § 17^4 lõiked 4-6 seletuskirja lk 103). On pikki paragrahve, mille puhul on valitud selgitada ainult ühte alapunkti (näiteks seletuskirja lk 77 selgitatakse eelnõu § 1 p 22 - KüTS § 5 lg 5 ainult punkti 10).	Vastused esitatakse esitatud ettepanekute järjekorras: - Eelnõu tekst on läbivalt üle vaadatud ja korrigeeritud, olulises osas (nt KüTS §-de 1 ja 3 osas) ka struktuuri muudetud. - Siinse eelnõuga ei tehta, mh tulenevalt NIS2 direktiivi ülevõtmise ajakavast, uut tervikteksti, kuid selle loomise vajadust hinnatakse paralleelselt koostamisel oleva küberturvalisuse valdkonna korrastamise VTK raames. - Mõjude analüüs on üle vaadatud ja vastavalt võimalusele ja olemasolevale teabele täiendatud.

	Eelnõu mõjuhinnang on puudulik ehk sisuliselt tegemata. Eelnõu seletuskirjas tunnistatakse otse, et majanduslik mõju subjektidele on erinev ja seda ei ole võimalik hinnata (lk 3). Eelnõu tegelik mõju on suur, kuna kohustatud isikute ring on väga suur ja kehtestavate kohustuste ulatus samuti. Samas on eelnõu seletuskirjas välja toodud ainult positiivsed mõjud. Negatiivseid mõjusid ei ole tuvastatud, kuid kas see tähendab, et neid tõesti pole? Näiteks ei ole analüüsitud mõjusid tänaste teenuste osutamisele – kindlasti kaasnevad kulud nõuete rakendamisega ja auditeerimisega, mis teeb teenused kallimaks, või et kas eelnõus sisalduvate küberturvalisuse nõuete täitmine toob kaasa ka selle, et mõni teenus läheb keerukamaks ja seega ka lõppkasutaja jaoks aeglasemaks või muutub tehnoloogilisse lahendusse lisanduva turvakomponendi tõttu mittekasutatavaks? ITL-i ettepanekud: — Palume vaadata eelnõu tekst üle ning järgida seejuures normitehnika eeskirja ja hea õigusloome tava reegleid eesmärgiga tagada eelnõu selgus ja arusaadavus ning sätete omavaheliste seoste jälgitavus. — Palume kaaluda asendusseaduse ehk uue KüTS tervikteksti tegemist, sest muudatuste maht on võrreldes kehtiva seadusega väga suur.[2] See idee on väärt kaalumist ka seetõttu, et paralleelselt on Justiits- ja Digiministeeriumis	

[2] Normitehnika eeskirja 13 sätestab järgmist: *Kui muutmisülesanne seisneb valdkonna ulatuslikus ümberkujundamises, siis on seaduse muutmise variant selleks ebasobiv, kuna tulemus ei ole ülevaatlik ega tõsta esile muudatuse õiguspoliitilist olemust ja tähendust*.

	ettevalmistamisel kehtiva KüTS-i revisjon (eelnõu seletuskiri lk 11-12) ehk sama seadust ootavad lähiajal ees järgmised (ulatuslikud?) muudatused. Viia läbi korrektne ja põhjalik mõjuanalüüs. ITL on valmis kaasa mõtlema, kuidas mõjuanalüüsi kõige paremini teha, et arvestatud saaksid kõik olulised mõjud. **Eelnõu kvaliteedi teemat kokku võttes tõdeme, et eelnõu on ilmselgelt ebaküps ning vajab põhjalikke muudatusi**. Õigusakt peab olema selge ja kohustatud isikutele arusaadav, kuid praegusel kujul ei täida eelnõu seda nõuet. Seda näitab ka see, et eelnõu koostajad küsivad seletuskirjas mitmetes küsimustes huvigruppide arvamust, mis oleks pidanud olema tehtud enne eelnõu ametlikku kooskõlastust. Seletuskirja lisatud hinnangud kohaldamisalas olevate üksuste arvude kohta on väga umbkaudsed. Võib arvata, et ka valdkondlikud erialaliidud ei oska skoopi kuuluvate ettevõtete hulka hinnata, sest kohaldamisala on ebaselge. Seega eelnõust ei ole hetkel üheselt arusaadav, mis muret sellega lahendatakse, kellele see kohaldub ja mis mõjud sel on.	
24.11	Kohaldamisala Kohaldamisala laiendamise küsimust adresseerisime oma kirja I osa punktis 2 [(siinse tabeli kommentaaris 24.1)], kuid kohaldamisala on segane ka sätete ülesehituse ja kasutatava terminoloogia tõttu. Kõigepealt sätestatakse, et eelnõu subjektid on üksused, siis loetletakse üles,	Selgitatud Eelnõu ülevaatamisel on eelnõu KüTS §-de 1 ja 3 sisu ja struktuur olulisel määral muutunud. Üksus on defineeritud NIS2 direktiivi artikli 6 punktis 38 ning eelnõuga luuakse vastav termin ka KüTS §-s 2. Ettepanekus märgitud joonis on seletuskirjale lisatud.

	milliste tunnustega üksused (lisandub suuruse aspekt) need on. Samas kohustused kehtivad teenuse osutajatele, kes on elutähtsad ja olulised üksused, kes on omakorda eraldi üles loetletud. Tekib küsimus, kas teenuse osutaja võrdub üksus. Üksuse mõiste on Eesti senist õigusruumi ja mõisteid arvestades ebaselge termin. Eelnõu lugeja peab kõvasti pingutama, et aru saada tervikpildist (kes mida tegema peab, kellele kohaldub). ITL-i ettepanek: vaadata üle kohaldamisala sätted ja tagada arusaadavus. Lisada seletuskirja jooniste kujul ülevaade, kes on subjektid ja millised kohustused neile rakenduvad. ITL-i konkreetsemad ettepanekud on leitavad käesoleva kirja lisast [(siinse tabeli kommentaarid 24.20-24.71)].	
24.12	Mõisted Eelnõu § 1 punktidega 7-14 lisatakse KüTS-i §-i 2 hulgaliselt uusi mõisteid. Mitmed neist mõistetest viitavad EL-i õigusaktidele ja on seetõttu keerulised lugeda ning aru saada, eriti just KüTS-i uute subjektide poolt. Osadest mõistetest ei saa aru ka eelnõu seletuskirja kõrvale lugedes. Näiteks hallatud teenuse osutaja ja hallatud turbeteenuse osutaja. Nende puhul on kindlasti vajalik leida arusaadavamad ehk sisu rohkem avavad mõisted eelnõusse või kasutada Eesti õigusruumis juba kasutusel olevaid mõisteid. ITL-i ettepanek: kirjutada võimalikult palju mõisteid eelnõu tekstis lahti (mitte kasutada viiteid) ja vaadata üle ka seletuskirjas olevad sõnastused. See tagab eelnõu loetavuse ilma vajaduseta termineid muudest õigusaktidest otsida. Mõistete	Selgitatud Eelnõus ongi § 2 sõnastamisel lähtutud sellest, et selles sätestatakse KüTSi tähenduses olevad mõisted, sh kui sama mõiste on kasutusel mõnes muus seaduse või EL õigusaktis, siis on viidatud vastavale mõistele. Eelnõus on tehtud viiteid EL õigusele ja seal olevatele mõistetele - neid ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.

	sätet on vaja kirjutada põhjalikumaks ja lisada sinna ka seletamata mõisteid, nt küberturvalisuse alane tegevus. ITL-i konkreetsed ettepanekud mõistete osas leiate käesoleva kirja lisast [(siinse tabeli kommentaarid 24.20-24.71)]. Erandina leiame, et usaldusteenuste ja kvalifitseeritud usaldusteenuste terminit ei ole vajadus eelnõus lahti kirjutada, kuna "kvalifitseeritud usaldusteenus" on niikuinii määratletud kui konkreetsele EU määrusele (nn eIDAS määrusele) vastav usaldusteenus. Kuigi eelnõu § 1 punktidega 7-14 muudetava KüTS §-is 2 on juba kirjas, et "käesolevas seaduses kasutatakse termineid järgnevas tähenduses", siis teeme ettepaneku ükshaaval üle vaadata kas sama terminit kasutatakse mõnes teises õigusaktis samas kontekstis erinevalt. KüTS on nii paljude valdkondadega seotud, mistõttu tuleb tagada, et ei tekiks paralleeltermineid (eelnõus siiski on palju mõisteid erineva tähendusega kui mujal – kõige lihtsam näide on üldiselt kasutatava mõiste „risk" sisustamine küberturvalisuse kontekstis). Osa termineid on ka praegu sätestatud valdkondliku õigusaktiga ja on sama tähendusega, aga siiski tuleks tagada võimalikult hea ühtlustamine. Kui termin erineb muus õigusaktis olevast siis selguse mõttes on otstarbekas konkreetse termini juurde lisada „käesoleva seaduse tähenduses".	Eelnõu koostamisel on hinnatud ja üle vaadatud, et ei tekiks sama mõiste kohta erineva definitsiooniga mõisteid ehk paralleeltermineid. Eelnõu koostamise käigus on ka üle vaadatud, et kui NIS2 direktiiv ise viitab mõne EL direktiivi mõistele, siis millise Eesti õigusaktiga on too mõiste üle võetud ning seeläbi on ka tehtud viide vastavale mõistele. NIS2 direktiivis toodud mõisteid ei saa erinevalt üle võtta (nt „risk") - see tooks kaasa ka direktiivist erinevad tõlgendused kohustuste täitmisel. Usaldusteenuste ja kvalifitseeritud usaldusteenuste mõistete osas ongi tehtud viide asjakohasele EL määrusele ehk siin ei ole korratud nende mõistete sõnastust definitsiooni, vaid viitena õigele õigusaktile ja sealsele terminile ning definitsioonile. Seletuskirjas on üle vaadatud ja võimalusel täiendatud haldusteenuse osutaja, infoturbeteenuse osutaja ning küberturvalisuse alase tegevuse selgitusi.
24.13	Pädevad asutused ja ülesanded Eelnõu § 1 punktiga 22 muudetakse KüTS §-i 5 ja kirjutatakse põhjalikult lahti RIA pädevused ja ülesanded. Seda sätet lugedes tekib küsimus, kas	Selgitused esitatakse arvestades esitatud ettepanekuid - Arvestatud - vt ka Riigi Infosüsteemi Ameti kommentaari 17.36 vastust. - Jääb selgusetuks, millise koostöökohustuse täiendav sisseviimine oleks vajalik. Märkuse esitaja on ise esile tõstnud sätted, millest tuleneb üheselt mõistetav

	see kõik peab ikka olema KüTS-is. Näiteks ei ole tavapärane kirjutada valdkonda reguleerivasse seadusesse, et asutusel peavad olema vahendid oma tegevuseks. See on nõue EL-i poolt liikmesriigile, mida liikmesriik peab täitma. KüTS-is on asjakohane reguleerida RIA õigusi sekkumiste teostamisteks teenuste osutajate üle ja ka RIA peamisi kohustusi. Teise murekohana tekitab segadust see, et RIA kohustused ettevõtetele ja asutustele abi osutamiseks ei ole üheselt selgelt kirjas. Need on eelnõus küll nn põhimääruse osas (KüTS § 5 lg 5 p 9; § 5 lg 8 p 3) kirjas, aga see pole piisav. Lisaks on ka küberturbe intsidentide lahendamise üksusel (CSIRT) paar ettevõtete ja asutuste abistamise punkti (KüTS § 5 lg 5 punktid 4, 7, 8 ja 9). Samas on ka nendes kasutatud sõnu *vajadusel*, *taotluse korral* ning *asjakohasel juhul.* Eelnõu § 1 punktiga 56 eelnõusse lisatavas KüTS §-is 17^4 on koostöö ette nähtud ainult ETO-de ning elutähtsate üksustega. KüTS-is on vastastikune abi pigem asutuste vahel (Eestis ja EL-is) järelevalve teostamisel. Meie hinnangul on KüTS-is paigast ära proportsioon ettevõtetele/asutustele abi andmise osas (mis peaks olema väga oluline ning rõhutatud) ja järelevalve osas (järelevalve kasuks). Koostöö tegemist ning näiteks vabatahtlikku teavitamist ei peaks reguleerima õigusakti tasemel. <u>ITL-i ettepanekud</u>: - Jätta kas kõik või osa RIA-t puudutav (KüTS § 5 lg 4 – 8) eelnõust välja ning lisada need punktid RIA põhimäärusesse;	koostöö- ja abistamiskohustus. Samuti on see ülesanne sätestatud Ameti põhimääruse § 13 lg 1 p-s 6. Kommentaaris mainitud Ameti ülesanded on lähtunud NIS2 direktiivi enda nõuetest ja sõnastustest ning kui eelnõus sätestada lisaks nendele ülesannetele veel muid ülesandeid, siis tegemist pole enam NIS2 direktiivi üle võtmisega.

	- kirjutada eelnõusse selgelt ühte sättesse RIA ülesanded ja kohustused ettevõtetele ja asutustele abi osutamiseks. Seejuures tuleb arvestada, et RIA põhifunktsioon olla abistaja tähendab olla peamiselt eri osapoolte info koondaja intsidentide puhul. See ei tohi kindlasti tähendada erasektori poolt pakutavate teenustega konkureerimist (näiteks riiklik SOC ja riiklik PEN-test). Riik peab valima, kus ta teenuse osutajana sekkub. Sektor kindlasti ei oota seda, et RIA pakuks kõigile tuge ja kaitset ning asutuse töötajate arv pidevalt kasvaks. RIA ülesanne on olla ühtne kontaktpunkt.	
24.14	Teenuse osutaja juhtorgani kohustused ja vastutus Eelnõu § 1 punktiga 24 lisatakse KüTS-i uus säte § 6^1, mis kehtestab ettevõtte juhtorganile ja selle liikmetele kohustused kiita heaks turvameetmed, läbida erikoolitusi ja tagada töötajate koolitamine. Eelnõu § 1 punktiga 58 lisatakse ka karistus võimaliku rikkumise eest (KüTS § 18^4). Lisaks saab RIA õiguse nõuda ettekirjutusega elutähtsa üksuse nõukogult või osanikelt juhatuse liikme(te) volituste ajutist peatamist (eelnõu § 1 punktiga 58 lisatav KüTS § 14 lg 13 p 2). Täpsustatud ei ole, kas mõeldakse juhatuse esimeest või kõiki juhatuse liikmeid. Tegemist on ühe probleemseima sättega eelnõus, mis tekitab küsimuse, kas keegi on mõelnud ka tagajärgedele, mis saab raskustes olevast ettevõttest, kelle juht ametist tagandatakse. Mõistame, et tegemist on NIS2 direktiivist tuleneva sättega, kuid sellist erasektori juhtimisse sekkumist	Osaliselt arvestatud ja selgitatud Esiteks, nagu märkuses ka õigesti välja tuuakse, on kõnealuse sätte eesmärk NIS2 artikli 32 lõike 5 punkti b ülevõtmine. Sellise regulatsiooni on Euroopa Liidu seadusandja direktiivis ette näinud ning liikmesriikidel puudub võimalus seda mitte rakendada. Eestil kui Euroopa Liidu liikmesriigil on direktiivi ülevõtmise kohustus. Samuti rõhutavad eelnõu autorid, et tegemist on n-ö viimase võimaluse abinõuga, mida järelevalveasutusel on võimalik rakendada üksnes juhul, kui varem rakendatud järelevalvemeetmed ei ole andnud tulemust ning ülioluline üksus ei ole ka talle antud täiendava tähtaja jooksul puudust kõrvaldanud. See on äärmuslikes olukordades rakendatav meede. Riigi Infosüsteemi Amet peab hindama, kas tegemist on kõige sobivama meetmega konkreetses olukorras tekkinud probleemi lahendamiseks ehk tegemist ei saa olla kergekäeliselt kasutatava meetmega. Seetõttu ei saa ühegi realistliku stsenaariumi kohaselt olema tegemist praktikas tihedat rakendamist leidva meetmega. Samas, nagu eelnõu seletuskirjas ka selgitatud on, ei ole siiski tegemist Eesti õiguses täiesti erakordse lahendusega. Seega ei ole ka õige öelda, et sellist sekkumist erasektori juhtimisse Eesti õiguskord üldse ei toetaks. Nimelt annab krediidiasutuste seaduse § 50 Finantsinspektsioonile õiguse ettekirjutusega nõuda krediidiasutuse juhi või võtmeisiku tagasikutsumist. Sarnast lahendust on kasutatud ka käesolevas eelnõus, kusjuures eelnõu on pärast kooskõlastust muudetud nii, et ettekirjutus tehakse konkreetsele

	Eesti õigusruum ei toeta. Juhtkonna liikme(te) kõrvaldamine ei aita kaasa rikkumise kõrvaldamisse ega kiiremasse tegutsemisse. Pigem motiveerib trahv asjad korras hoidma ning sunniraha rakendamise võimalus võiks olla Eesti õigusruumi sobiv meede. Samas tähendaks see ka järelevalveasutuse poolt vastavale menetlusvormile ettenähtud protseduuriliste normide järgimist. Juhime ka tähelepanu, et säte on üle võetud erinevalt NIS2 direktiivist. NIS2 direktiivi artikkel 35 lõige 5 näeb ette, et pädevatel asutustel on õigus üksnes taotleda (mitte nõuda), et asjaomased organid või kohtud keelaksid kooskõlas liikmesriigi õigusega füüsilisel isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, selles üksuses ajutiselt juhtimisülesannete täitmise. <u>ITL-i ettepanekud</u>: - muuta KüTS § 14 lg 13 p 2 sõnastust selliselt, et RIA-l on õigus taotleda, mitte nõuda; - muuta KüTS § 14 lg 13 p 2 sõnastust selliselt, et taotlus tuleb esitada kohtule, mitte elutähtsa üksuse nõukogule või osanikele; - lisada eelnõu seletuskirja analüüs, kuidas hakkab selle sätte rakendamine praktikas toimuma, näitena kasutada börsiettevõtteid; - lisada eelnõu seletuskirja ka analüüs, mis mõju on KüTS § 14 lg 1 p 1 ehk elutähtsa teenuse osutamise lõpetamisel ning hinnata üle, kes saab olema õigustatud sellist meedet kasutama (sellist otsust tegema).	üliolulisele üksusele, kes peab juhatuse liikme volitused ajutiselt peatama. Eelnõu sõnastuses kasutatav termin „nõuda“ vastab direktiivi sisulisele mõttele (ja direktiivi teistes keeleversioonides kasutatud sõnastustele, inglise keeles *„to request“*, saksa keeles *„verlangen“*). Direktiivi tekst jätab iseenesest liikmesriikidele võimaluse juhatuse liige tagasi kutsuda „kooskõlas liikmesriigi õigusega“. Eelnõu koostamisel ja kooskõlastamisejärgselt kaaluti põhjalikult, kas NIS2 direktiivi artikli 32 lg 5 punkti b ülevõtmiseks on alternatiivseid ja Eesti õigusesse paremini sobivaid meetmeid, ning jõuti järeldusele, et ei ole. Ettekirjutuse tegemise otsustab Riigi Infosüsteemi Amet, kellele antakse KüTS-is sellekohane pädevus. Ameti ettekirjutus allub kohtulikule kontrollile. Üliolulisel üksusel on võimalik esitada selle peale halduskohtusse kaebus ja nõuda ka ettekirjutuse täitmise peatamist esialgse õiguskaitse korras. Üliolulisele üksusele on tagatud kõik halduskohtumenetluses ette nähtud tagatised, sellele eelnevas faasis kohalduvad Ametile kõik HMS-is ette nähtud nõuded haldusmenetluse läbiviimisele. Sarnast lahendust, kus pädev järelevalveasutus nõuab otse järelevalvesubjektilt endal juhatuse liikme tagasikutsumist, on kasutatud ka teiste riikide NIS2 direktiivi ülevõtmiseks koostatud eelnõudes. Näiteks on see selliselt kavandatud Eesti õiguskorra kujundamisel oluliseks eeskujuks olnud Saksa Liitvabariigi vastavas seaduseelnõus. Eelnõuga antakse selle meetme kasutamise pädevus Riigi Infosüsteemi Ametile, kuid eelnõu ei täpsusta, kellel Ameti sees on vastav pädevus selle meetme kasutamiseks. Meetme kasutamisega seotud sisepädevuse paneb paika Amet. Lisaks eeltoodule märgime, et avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17. Avalikule kooskõlastusele edastatud eelnõu KüTS §-s 18^4 sisaldunud väärteokoosseis on eelnõust eemaldatud. NIS2 direktiiv ei nõua karistusõigusliku vastutuse tekitamist (piisab tsiviilõiguslikust vastutusest, mille osas on selgitused antud eelnõu seletuskirjas, KüTS § 6^1 juures). Samuti on juhatuse liikme kohustuste hulgast (KüTS § 6^1) eemaldatud algses eelnõus sisaldunud kohustus „tagada, et teenuse osutaja töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi“.

24.15	Teenuse osutaja süsteemi turvameetmed Eelnõu § 1 punktidega 25-28 muudetakse KüTS §-i 7. Antud muudatusega laiendatakse subjektide kohustusi. Üldise loogika järgi peavad olema turvameetmed kaetud, kui standard on rakendatud. Eelnõud lugedes aga selgub, et peab järgima lisaks standardile ka eelnõus toodud meetmeid. Kusjuures need meetmed on põhjalikult avatud eelnõu seletuskirjas. Oluline probleem on see, et selle sätte lõikega 2 laiendatakse NIS2 direktiivi sõnastust. Käände muutmisega KÜTS-is on muudetud NIS2 direktiivi artikkel 21 lõike 2 punktide a)-j) sisu. Jääb ebaselgeks, kas see on tahtlik või mitte. Oleme seisukohal, et kui NIS2 direktiiv jätab võimaluse subjektil midagi teha, siis ei tohi seda Eesti õiguses kohustuseks muuta. Seetõttu tekib olukord, kus NIS2 direktiivi artikkel 21 lõike 2 punkt e) sätestab muuhulgas: "*meetmed hõlmavad sh. nõrkuste käsitlemist ja avalikustamist*". KüTS § 7 lg 1 punktis 7 näiteks on aga kohustuseks "*tagama sh. nõrkuste käsitlemise ja avalikustamise*". Kui NIS2 direktiiv ütleb, et avalikustamise protseduur/ulatus peab meetmetes kirjas olema, siis eelnõus on sellest saanud kohustus avalikustada. <u>ITL-i ettepanekud</u>: - vaadata KüTS § 7 sõnastused üle eesmärgiga tagada arusaadavus ja kohustuste ühekordne rakendamine. Vt ka ITL-i konkreetseid märkusi ja ettepanekuid käesoleva kirja lisast [(siinse tabeli kommentaarid 24.20-24.71)];	Selgitatud vastavalt esitatud ettepanekute järjekorrale - Eelnõu KüTS § 7 sõnastused on üle vaadatud, sh on NIS2 direktiivi artikli 21 lõike 2 üle võtmise sisu viidud KüTS § 7 lõike 5 alusel antud Vabariigi Valitsuse määruse muutmise kavandisse (vt tolle määruse kavandi sõnastusi). - Eelnõus ei ole planeeritud anda juhise vormis olevat nõuete kogumit rakendusaktina. See siiski ei välista võimalust, et Riigi Infosüsteemi Amet ei võiks enda võrgulehel taolisi selgitusi ning juhiseid avaldada. Siin vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust. - Kommentaaris mainitud kohustusliku koolituse osas vt Rahandusministeeriumi kommentaari 6.1 vastust. Samuti on eelnõust eemaldatud kommentaaris mainitud väärteokoosseis (eelnõu KüTS § 6^1 nõuete rikkumine).

	- meetmete kirjeldus kehtestada eraldi rakendusaktina, mis võiks olla juhise kujul ehk elav dokument. Seaduse seletuskiri ei ole õige koht, kuna antud juhul ei ole tegemist kohustuste selgitamise, vaid sisustamisega. Eraldi rõhutame vajadust määrusega sisustada kohustusliku koolituse skoop ja nõuded koolituse läbimist tõendavale hindamisele. Kuna tegemist on sanktsioneeritava kohustusega, siis peab olema subjektidele selge, mida neilt nõutakse.	
24.16	Eelnõu alusel vastuvõetava määrusega vastuolus oleva rakendusakti kohaldamine Eelnõu § 1 punktiga 28 lisatakse KüTS § 7 lõige 6, mis räägib Euroopa Komisjoni rakendusaktist, mis ei pruugi olla eelnõuga kooskõlas ning kohustab teenuse osutajad sel juhul järgima nimetatud rakendusakti. Vastuseks eelnõu koostajate küsimusele seletuskirjas (lk 87) anname teada, et see säte ega selle eesmärk ei ole arusaadav. Miks peaks üldse tekkima olukord, et Eestis kehtestatakse riigi poolt määrus, mis on vastuolus EL-i rakendusaktiga? Samuti on äärmiselt ebaproportsionaalne panna vastutus kohustatud isikutele ehk teenuse osutajale tuvastamaks vastuolusid määruse ja rakendusakti vahel. ITL-i ettepanek: vaadata selle sätte sõnastus üle ning jätta sellest välja teenuse osutajate kohustus erinevaid õigusakte omavahel võrrelda ja hinnata kumba täita. ITL-i täiendavad kommentaarid, küsimused ja ettepanekud eelnõu konkreetsete sätete ja	Selgitatud Tolle lõike mõte on tekitada selgus küsimuses, mida teeb KüTSi teenuseosutaja, kui ta peab samal ajal järgima lisaks KüTSi nõuetele ka NIS2 direktiivi artikli 23 lõike 5 alusel antud rakendusakti. Selle lõike mõte on vastavast olukorrast tõusetuva võimaliku ebaselguse lahendamine. NIS2 direktiivi tõttu on KüTSi teenuseosutaja kogu oma tegevusega KüTSi nõuete järgimise kohustuse all (vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust; jättes üksikud erandid kõrvale - vt DORA määruse subjektid), siis olukorras, kus teenuseosutaja peab viidatud rakendusakti järgima ühtede teenuste korral, siis teiste teenuste puhul peab ta NIS2 direktiivi ehk KüTSi ja selle alusel antud õigusaktide nõudeid järgima. Siin tuleb lähtuda õiguse üldisest loogikast, et kui mingit küsimust eriseaduses (mainitud rakendusakt) lahendatud ei ole, tuleb lähtuda üldseaduses (NIS2 direktiivis, täpsemalt seda üle võtvas KüTS) sätestatust. See ei ole KüTS-le eriomane lähenemine. Tolle sätte sõnastus on üle vaadatud, et selle mõte paremini välja tuleks – vt uuendatud eelnõu KüTS § 7 lõiget 7.

	seletuskirja osas leiate käesoleva kirja lisast [(siinse tabeli kommentaarid 24.20-24.71)].	
24.17	NIS2 direktiivi ja DORA määruse kattuvuse regulatiivne lahendus Eelnõus ei adresseerita turuosaliste poolt tõstatatud murekohta seoses finantssektori digitaalse tegevuskerksuse ehk DORA määrusega (EL-i määrus 2022/2554). Praegu pole selgelt määratletud, kas NIS2 direktiivi kohuslased, kes osutavad krediidiasutustele teenuseid kriitilise või olulise funktsiooni osas, peavad lisaks NIS2 direktiivile tõendama ka DORA-le vastavust ning kuuluma DORA järelevalve alla. See tekitab dubleerivat halduskoormust. ITL-i ettepanek: Käsitleda KüTS-is kui üldseaduses seda teemat, et vältida dubleerivat halduskoormust ning tagada sujuvam nõuetele vastavuse tagamine. Oluline on keskenduda: - topelt nõuete vähendamisele, võimaldades lihtsustatud tõendamist; - koordineeritud järelevalvele, et vältida ebavajalikku bürokraatiat ja tagada tõhusam regulatiivne järelevalve. Eelnõuga jääb lahtiseks ka küsimus, et kas krediidiasutused peavad tagama vastavuse DORA kui otsekohalduva määruse nõuetele ning ka Eestis kehtiva KüTS-i nõuetele. Ehk kas läbima peab lisaks Finantsinspektsiooni auditeerimisele ka E-ITS auditi või saama ISO27001 sertifikaadi või loetakse ka DORA alusel tehtav audit samaväärseks nii nagu täna E-ITS ja ISO27001 on alternatiivid. Hetkel peab teenuse osutaja justkui	Selgitatud Avalikul kooskõlastusringil olnud eelnõus sooviti kommentaaris mainitud teemat lahendada ära KüTS § 1 lõike 4 muutmisega ning sama paragrahvi täiendamisega lõikega 4^1, mis oleks määrusega täpsustanud lõike 4 sisu. Eelnõu teksti uuendamisel mainitud volitusnorm eemaldati, kuid selle mõte on jätkuvalt olemas KüTS § 1 lõike 4 muudatuses ja seda kirjeldavas osas eelnõu seletuskirjas. Kõige olulisem on põhimõte, et olukorras, kus mõne üksuse jaoks kehtivad teisest õigusaktist tulenevad nõuded (nt DORAst tulenevalt), mis on samaväärsed NIS2 direktiivi riskijuhtimismeetmete või olulistest intsidentidest teavitamise nõuetega, siis sellises olukorras lähtub see üksus samaväärselt reguleeritud ulatuses (turvameetmete rakendamise, küberintsidentidest teavitamise või mõlema eelneva osas) mitte KüTS-s sätestatust, vaid vastavast valdkondlikus õigusaktis sätestatud nõuetest. Finantssektori näitel ei kohaldata DORA määruse kohaldamisalas oleva üksuse DORA määruse kohaldamisalas olevale teenusele eelnõujärgse KüTSi §-e 3^1, 6, 6^1, 7 ja 8 ega ka nende rikkumisega seotud järelevalve- ja karistusnorme. Siin vt ka Finantsinspektsiooni kommentaari 15.2 vastust.

	ise võrdluse tegema (eelnõu § 1 punktiga 4 muudetav KüTS § 1 lg 4), kas otsekohalduva määrusega on kohustused täidetud või mitte. Samal ajal on teada, et nii nagu E-ITS ja ISO ei ole identse sõnastusega, ei ole seda ka DORA (kuigi sarnane), ometi on E-ITS ja ISO õigusakti tasemel loetud võrdsustatuks. Ebaselgeks jääb, kes ja kuidas ikkagi vastavust hindab ja kontrollib, millises osas kattub ja millises osas mitte, milliseid nõudeid tuleb täita otsekohalduvast määrusest ja milliseid KüTS-ist.	
24.18	**Lõpetuseks tõdeme, et meie poolt välja toodud eelnõu probleemid on tingitud sellest, et eelnõu osas ei ole viidud läbi eelkonsultatsioone ega tehtud mõjuanalüüsi**. Eelnõu ei arvestada riigis püsitatud eesmärki vähendada bürokraatiat ja halduskoormust ning iga uue õigusaktiga ka millestki vanast loobuda. **Loodame, et leiate võimaluse tagasisidet arvestada ja võtta NIS2 direktiiv Eesti õigusesse üle selliselt, et tagatud on riskipõhisus ja proportsionaalsus ning küberturvalisuse valdkonna areng.** Soovitame ülevõtmisel arvestada ka seda, mis moodi võetakse NIS2 direktiivi üle teistes liikmesriikides, kus räägitakse palju rohkem ettevõtete konkurentsivõimest ja nende enda rollist küberturvalisuse tagamisel. Riigi roll on seejuures pakkuda ettevõtetele nõustamist ja tõhusaid koostöömehhanisme. Eesti on mõõtnud juba alates 2008. aastast kriitilise infrastruktuuri vastupanu rünnetele. Seetõttu võiks eeldada, et Eesti riigil on olemas hea tervikpilt	Võetud teadmiseks

	olukorrast ning sellest lähtuvalt saab ka sõnastada, mis probleemi eelnõuga lahendatakse. Kooskõlastusele saadetud eelnõu versioon aga jätab mulje nagu seni oleks kõik valesti olnud ja valdkond vajab põhjalikku uuendust, sealjuures teenuste kirjeldusest ja kohustatud üksustest ei ole võimalik üheselt järeldada, kellele või millele need kohalduvad Eesti kontekstis.	
24.19	**Teeme Justiits- ja Digiministeeriumile ettepaneku korraldada ITL-iga kohtumine**, et arutada meie poolt eelnõus tõstatutud murekohti ning välja pakutud lahendusi. Samuti **palume selle eelnõu menetlusega mitte kiirustada.** Eelnõu kokku kirjutamiseks võttis riik kaks aastat aega pärast NIS2 direktiivi vastuvõtmist. Nüüd on vaja aega ka selle huvigruppidega läbi arutamiseks ning eelnõu mõjude ja rakendatavuse analüüsiks. Tegemist on olulise valdkonnaga ja suure mõjuga eelnõuga.	Võetud teadmiseks
24.20	**Eelnõu § 1 p 1 – KüTS § 1 lg 1[1] ja eelnõu § § p 7 – KüTS § 2 p 1[1]** Üksus terminina on antud kontekstis kasutamiseks võõras ja pigem kasutatakse seda militaarvaldkonnas. Eesti keeles oleme harjunud ettevõtete/äriühingute ja (riigi/KOV) asutustega. Teeme ettepaneku kasutada Eestis kasutusel olevaid mõisteid, nii on selgem kõigile, sh kohustatud subjektidele. Variant on kaaluda ka hädaolukorra seaduse analoogiat. Seal nimetatakse elutähtsa teenuse osutajatena juriidilised isikud, kelle pädevuses on	Selgitatud. Vt Regionaal- ja Põllumajandusministeeriumi kommentaari 7.2 vastust. Samuti on parendatud „üksuse“ definitsiooni, et oleks selgus selle mõiste seosest füüsilise isiku korral.

	seaduses nimetatud elutähtsa teenuse osutamine (HOS § 38 lg 1). Segadust tekitab ka see, et KüTS § 1 lg 1^1 kohaselt on üksus ettevõtte, hiljem eelnõus ka avaliku sektori asutus. Samuti jääb lõpuni arusaamatuks füüsilise isiku hõlmamine üksuse definitsiooniga. Kas mõeldud on füüsilisest isikust ettevõtet? Sest füüsilist isiku ju ei asutata. Seonduva teemana kordame veel, et kuigi eelnõu koostajad on suuliselt selgitanud, et teenuse osutaja ongi üksus, siis eelnõust see ei nähtu.	
24.21	**Eelnõu § 1 p 1 – KüTS § 1 lg 1^2** Palusite eelnõu seletuskirjas tagasisidet, kas sõnastused on arusaadavad või vajavad täpsustamist. ITL-i tagasiside on, et sõnastused ei ole arusaadavad ja vajavad kindlasti täpsustamist. Teeme ettepaneku sõnastada subjektide loetelu lühemalt, selgemalt ja üheselt arusaadavalt. EL-i õigusele viitavatesse punktidesse on vaja sisulist eesti keelset mõistet, nt punktides 5 ja 6. **Punkti 34** (interneti vahetuspunkti teenuse osutaja) tõlge on ebaõnnestunud (vrdl. *telephone exchange* - kas see on telefoni vahetus?). Siin aitaks seaduses ingliskeelse termini kasutamine. IXP on üldiselt igale eksperdile mõistetav. **Punkti 35** puhul on raske mõista sõnastust, kus on kaks korda järjest sõna süsteem - domeeninimesüsteemide süsteemi teenuse osutaja. **Punkti 36** (pilvandmetöötlusteenuse osutaja) puhul palume selgitada, kas see kohaldub ka vahendusteenuse osutajale.	Osaliselt arvestatud ja selgitatud Esmalt märgime, et eelnõu koostamisel on eelnõu KüTS §-de 1 ja 3 struktuuri, sisu ning sõnastusi, mh õigusselguse parendamise eesmärgil ja vastavalt kooskõlastusringi käigus saabunud tagasisidele oluliselt muudetud. Punktide 5 ja 6 osas: - Tegemist on viitega EL õigusele ja seal olevale mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). - Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Punkt 34 osas: avalike andmete kohaselt on „interneti vahetuspunkt“ / „interneti vahetuspunkti teenus“ laialt levinud. „IXP teenus“ ei oleks parem alternatiiv, kuivõrd

	Punkt 38 (sisulevivõrguteenuse osutaja) ei ole arusaadav. Kirjelduse järgi oleks tegemist justkui võrguomanikuga, kuid sisulevi viitab sisule või vahendamisele. Teeme ettepaneku seda punkti täpsustada (samuti ka KüTS § 2 punkti 7^2), et see pole side, TV või raadioteenus (seletuskirjas hetkel on täpsustus). Samuti teeme ettepaneku lisada ingliskeelse termini "*Content Delivery Network* - CDN", et oleks arusaadavam. Kindlasti aitaks kaasa ka see, kui nimetada ära, kes need (5) ettevõtet on, kes eelnõu koostajate hinnangul selle sätte alla lähevad. **Punkt 39** (hallatud teenuse osutaja) on kõige arusaamatum üksuse kategooria, millest tõesti ei saa aru, keda mõeldud on. Seletuskirja sõnastuse kohaselt võiks sellesse kategooriasse kuuluda väga paljud erinevad ettevõtted. Seletuskirjas pakutakse, et neid võiks olla 20 tükki. Palun kirjutage eelnõus lahti, milliste teenuste osutajatega tegemist on ning kuidas on vastutus jagunenud, kui vahendatakse kellegi teise toodet/teenust. Vastavalt vaja üle vaadata ka eelnõu § 1 p 14 – KüTS § 2 p 11. **Punkti 40** (hallatud turbeteenuse osutaja) tekib kõigepealt küsimus, miks see eraldi välja toodud on, kui eelmine mõiste – hallatud teenuse osutaja – katab ka selle kategooria. Või need ikkagi ei kattu? Näiteks võib turbeteenus võib olla ka sisse ostetud infoturbejuhi teenus, mis ei sobi KüTS § 2 p 11 definitsiooniga.	see tuleks samuti eestikeelsena lahti selgitada, mille tulemusel jõutaks praegusega analoogse definitsiooni juurde (parema tõlke puudumisel). Eelnõus on selle punkti puhul muudetud sõnastust ning see on nüüd „interneti sõlmpunkti teenuse osutaja". Punkt 35: arvestatud (uus sõnastus on „domeeninimede süsteemi teenuse osutaja"). Punkt 36: kommentaaris ei ole mainitud, mida peetakse „vahendusteenuseks", mistõttu ei ole võimalik täiendavalt selgitada. Juhime tähelepanu, et eelmise küberturvalisuse direktiivi ja NIS2 direktiivi tekstis on vastava termini mõiste ainult väheses osas muutunud. Seega, kui mingi üksus osutab kehtiva KüTSi tähenduses olevat pilvandmetöötlusteenust ning see hõlmab ka „vahendusteenust", siis kohaldub sellele üksusele ka siinse eelnõu järgselt KüTS. Punkt 38: eelnõus on selle üksuse sõnastamisel ning defineerimisel lähtutud NIS2 direktiivi artikli 6 punktis 32 olevast „sisulevivõrgu" sõnastusest. Vt siin ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.1 vastust. Punkt 39: eelnõus on selle üksuse sõnastamisel ning defineerimisel lähtutud NIS2 direktiivi artikli 6 punktis 39 olevast „hallatud teenuse osutaja" sõnastusest. Uuendatud eelnõu tekstis on selle sõnastuseks „haldusteenuse osutaja", Punkt 40: eelnõus on selle üksuse sõnastamisel ning defineerimisel lähtutud NIS2 direktiivi artikli 6 punktis 40 olevast „hallatud turbeteenuse osutaja" sõnastusest. Uuendatud eelnõu tekstis on selle sõnastuseks „infoturbeteenuse osutaja". Mõte on selles, et kõik infoturbeteenuse osutajad on haldusteenuse osutajad, kuid vastupidi see seisukoht ei päde: kõik haldusteenuse osutajad ei pruugi osutada küberturvalisuse riskijuhtimisega seotud teenuseid. Punkt 47: vastav sisu on selgitatud seletuskirjas, mistõttu seda eraldiseisvalt eelnõu sõnastuses ei korrata.

	Termini sisu jääb arusaamatuks. Näiteks kas mõeldud on vahendajaid või kedagi muud? Vahendajate puhul võib olla oluline, et kas vahendaja saab ise midagi teha või üldse sekkuda, kui tegemist on valmistootega. Vahendustegevuse juures on oluline ka küsimus, kas tegemist põhitegevuse või kõrvaltegevusega. Teisel juhul võivad kohustused olla ettevõtte jaoks ebaproportsionaalselt suured. Sarnaselt vaja üle vaadata ka eelnõu § 1 p 14 – KüTS § 2 p 12. **Punkti 47** (Eurostati klassifikaatori NACE Revision 2 C jao jaotistes 26, 27, 28, 29 ja 30 osutatud majandustegevusega tegelev ettevõtja) osas teeme ettepaneku lisada sisu ehk mis majandustegevusele need punktid viitavad.	
24.22	**Eelnõu § 1 p 1 – KüTS § 1 lg 1[3]** **Punkti 1** (üldkasutatava elektroonilise side võrgu pakkuja) puhul juhime tähelepanu, et Elektroonilise side seaduses (ESS § 2 p 66) kasutatakse terminit võrguteenuse pakkuja. See vastab Direktiivi (EL) 2018/1972 artikli 2 punktile 2 mis tõepoolest kasutab terminit „elektroonilise side võrgu pakkumine“. Seega teeme ettepaneku mitte luua uut terminit vaid võtta ESS-ist õige sisuga termin. Neid ettevõtteid on kindlasti rohkem kui 4, kuna siia alla lähevad muuhulgas ka kõik riigiabi eest ehitatud sidetaristu (nt optikakiu) pakkujad. **Punkti 2** (üldkasutatava elektroonilise side teenuse osutaja) kohta on samasugune kommentaar – neid ettevõtteid on kindlasti rohkem kui 4. Õige numbri	Selgitatud vastavalt kommentaaris esitatud punktidele: Punktid 1 ja 2: eelnõus kasutatakse läbivalt sõnastusi „üldkasutatava elektroonilise side võrgu teenuse osutaja“ ja „üldkasutatava elektroonilise side teenuse osutaja“. Eelnõus on KüTS §-i 2 tekitatud mõisted „üldkasutatav elektroonilise side teenus“ ja „üldkasutatav elektroonilise side võrk“, mis viitavad samadele terminitele elektroonilise side seaduses. Avalikul kooskõlastusringil olnud eelnõu versioonis oli kommenteeritud punktis viidatud „elektroonilise side teenusele“, kuid uuendatud eelnõust on see eemaldatud. Punkt 3: tegemist oli Riigi Infosüsteemi Ameti esmase arvamusega. Siin vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.1 vastust. Punkt 5: seletuskirja on vastavalt muudetud ja selgitatud, et Eesti Interneti Sihtasutus teostab järelevalvet kokku 51 akrediteeritud .ee registripidaja teenuse osutamise suhtes.

	saab Tarbijakaitse ja Tehnilise Järelevalve Ametilt. ITL-ile teadaolevalt on neid ettevõtteid üle 200. Teeme ettepaneku lisada antud mõiste definitsioon, mis on elektroonilise side seaduses. Eelnõu § 1 punktiga 16 KüTS-i lisatava § 3 lg 1^2 punkt 9 räägivad "elektroonilise side võrgu ja elektroonilise side teenuse **pakkujast**". Pakkuja mõistet pole aga defineeritud . Samuti kasutatakse vahepeal mõistet "elektroonilise side teenuse **osutaja**". Jääb selgusetuks mis vahe on osutajal ja pakkujal KüTS-i tähenduses. Meile teadaolevalt kasutatakse võlaõigusseaduses ja tarbijakaitseseaduses lähenemist, et pakkuja on see, kel on teenus olemas, kuid kes seda veel ei osuta. Ehk õigem oleks kasutada mõistet teenuse osutaja. **Punkti 3** (usaldusteenuse osutaja) osas tekkis küsimus, kuidas on hinnatatud, et esialgselt usaldusteenuseid osutajaid on 28 tk. Millistel allikatel see informatsioon tugineb? Taaskord oleks abiks avalik nimekiri, keda eelnõu koostajad selle kategooria alla liigitaksid. Siiski peab eelnõu tekst ka olema piisavalt selge selles osas, et kohustatud isik ise ka aru saaks, kas on kohuslane või ei. **Punkti 5** (domeeninimede registreerimise teenuseid osutav üksus) osas märgime, et registripidajaid on www.internet.ee andmetel 51 (seletuskirjas 10).	
24.23	**Eelnõu § 1 p 1 – KüTS § 1 lg 1^4** Kas üksus käesolevas paragrahvis on ainult ettevõte või ka avaliku sektori asutus?	Selgitatud Kommenteeritud lõige on eelnõust eemaldatud. Selle asemel selgitatakse seletuskirjas konkreetse üksuse juures, kas ja kuivõrd kohaldub selle üksuse puhul NIS2 direktiivi artikli 2 lõike 2 punktides b–e sätestatud kriteeriumid.

	Punkt 2 - miks siin kasutatakse sõna "häire"? Pigem see on ikka küberintsident (mille mõiste sees on häire). NIS2 direktiivi artikkel 2 lg 2 punkt c kasutab sõna "distruption" mis on pigem "teenuse häirimine", mitte "häire" (ingl.k "alert"). Häire on küll NIS2 tõlkes, aga pole korrektne. **Punkti 2** osas võiks pigem olla sõnatus „on oluline mõju", mitte „võib olla". **Punkti 3** osas sarnaselt „võib tuua" asendada „toob kaasa". **Punkti 4** osas jääb ebaselgeks, milline on kriitilise tähtsuse tuvastamise metoodika.	
24.24	**Eelnõu § 1 p 1 – KüTS § 1 lg 1^5** Normitehniline märkus, et saatelauses piisab viitest KüTS § 1 lõikele 1^4, ei näe vajadust nimetada kõiki selle alapunkte (1-4).	Mittearvestatud ja selgitatud Uuendatud eelnõus on KüTS §-de 1 ja 3 sõnastust muudetud, sh on ka eemaldatud § 1 lõige 1^4 tervikuna. Selle asemel selgitatakse seletuskirjas konkreetse üksuse juures, kas ja kuivõrd kohalduvad selle üksuse puhul NIS2 direktiivi artikli 2 lõike 2 punktides b–e sätestatud kriteeriumid.
24.25	**Eelnõu § 1 p 2 – KüTS § 1 lg 2^1** Küsimus: Keda on selle sättega mõeldud – millise asutuse kohta see reaalses elus käib?	Selgitatud Kõnealune säte ei käi ühegi spetsiifilise isiku/asutuse kohta. Tegemist on NIS2 direktiivi art 2 lõikest 9 tuleneva kohaldamisala kitsenduse piiranguga (erandiga), mis liikmesriikidel tuleb riigisisesesse õigusesse üle võtta.
24.26	**Eelnõu § 1 p 5 – KüTS § 1 lg 4^1** Õigusselguse mõttes asendaks sõna "võib" sõnaga "peab".	Mittearvestatud ja selgitatud Vastava määruse volitusnorm on eemaldatud, mistõttu esitatud ettepanekut ei ole võimalik täita. Siin vt ka Finantsinspektsiooni kommentaari 15.2 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.17 vastust.
24.27	**Eelnõu § 1 p 6 – KüTS § 1^1** Kuna seadus on ülimuslik, siis kas teenuselepingu sätted, mille kohaselt toimuksid teenuse pakkujaga võimalikud vaidlused Eesti Vabariigi kohtusüsteemis, muutuksid kehtetuks, kui teenuse pakkuja asub nt Leedus?	Selgitatud KüTS (kui avalik-õiguslik kohustus) ei muuda subjekti ja teenusepakkuja vahelist teenuslepingut (tsiviilõiguslik õigussuhe) kehtetuks. Teenuse lepingu sätted peavad arvestama õigusakte, sh ka kohtualluvusega seotud õigusnorme. Lisaks märgime, et eelnõu ei reguleeri kohtuvaidlustega seotud küsimusi.

	Hea oleks selgemaks saada ka, mida tähendab KüTS § 1^1 lg 3 p 1 "peamine tegevuskoht ..., kus turvameetmeid käsitlevad otsused valdavalt tehakse." Tekib küsimus mis laadi otsused – kas strateegilised, operatiivsed? Kelle otsused?	„Peamise tegevuskoha" sisustamisel tuleb lähtuda NIS2 direktiivi pp-s 114 toodud selgitustest: *Käesoleva direktiivi tähenduses eeldatakse tegevuskohakriteeriumi puhul püsivalt korraldatud tegelikult toimuvat tegevust. Sellise korralduse õiguslik vorm (filiaal või juriidilisest isikust tütarettevõtja) ei ole antud juhul määrav tegur. Selle kriteeriumi täitmine ei tohiks sõltuda võrgu- ja infosüsteemide füüsilisest paiknemisest teatavas kohas; selliste süsteemide olemasolu ja kasutamine ei näita iseenesest peamist tegevuskohta ning seega ei ole need peamise tegevuskoha kindlakstegemisel otsustavad kriteeriumid. Peamise tegevuskohana tuleks käsitada liikmesriiki, kus liidus tehakse valdav osa otsustest küberturvalisuse riskijuhtimismeetmete kohta. Tavaliselt on see liidu asukoht, kus asub üksuse peakontor. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata või kui selliseid otsuseid ei tehta liidus, tuleks peamise tegevuskohana käsitada liikmesriiki, kus toimub küberturvalisuse alane tegevus. Kui sellist liikmesriiki ei ole võimalik kindlaks määrata, tuleks peamise tegevuskohana käsitada seda liikmesriiki, mille tegevuskohas on üksusel liidus kõige rohkem töötajaid. Kui teenuseid osutab kontsern, tuleks kontserni peamiseks tegevuskohaks lugeda kontrolliva ettevõtja peamine tegevuskoht*. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.28	**Eelnõu § 1 p 7 – KüTS § 2 p 1^2** Siin on huvitav lähenemine, kus terminis sätestatakse KüTS § 1 lg 1^3 punktis 7 nimetatud asutused. Miks need ei saa olla seal, kus sätestatakse, et regulatsioon laieneb neile? Teeme ettepaneku lisada siia viide, mitte korrata loetelu.	Selgitatud Kuna eelnõus on KüTS § 1 sõnastust muudetud, siis kommentaaris viidatud mõiste sõnastatakse esmakordselt KüTS §-s 2. Vt ka Regionaal- ja Põllumajandusministeeriumi kommentaari 7.2 vastust. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.29	**Eelnõu § 1 p 7 – KüTS § 2 p 1^4** Tegemist on olulise muudatusega, sest esmakordselt defineeritakse Eesti õiguses küberturvalisus. Kahjuks on seda tehtud viitega	Mittearvestatud ja selgitatud Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse

	EL-i õigusele. Teeme ettepaneku see mõiste eelnõus avada, sest viide EL-i määrusele ei taga õigusselgust.	ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.30	**Eelnõu § 1 p 9 – KüTS § 2 p 3[3]** Teeme ettepaneku sõnastada „risk“ järgmiselt: 1) vaatlusaluse ohu potentsiaal ära kasutada mingi vara või vararühma nõrkusi ja tekitada seeläbi kahju; 2) võimalus, et küberintsidendi läbi tekib kahju või tõrge, väljendatakse kahju ulatuse mõju hinnangu ja realiseerumise esinemise võimalikkuse kombineeritud näitajana. Ehk aitaks KüTS-i kontekstis selgusele kaasa ka see, kui sõna risk juures kasutada eristumiseks mingit täiendavat sõna? Kummaline konstruktsioon eelnõus sisalduva selgituse puhul on „häire võimekus“. Kas see on eesti keeles “häire (mis pole ka õige sõna) tekkimise võimalus”. Või siis sündmuse? Pigem on tegu ohuga küberintsidendist tekkivale kahjule, kas teenuse katkemisest või toimimisest tingituna või juurdepääsu piiramisest.	Vt Kaitseministeeriumi kommentaari 2.1 ja Riigi Infosüsteemi Ameti kommentaari 17.23 vastust. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.31	**Eelnõu § 1 p 9 – KüTS § 2 p 3[4]**	Mittearvestatud ja selgitatud

	Siia on vaja mõistet, mitte viidet määrusele.	Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Juhime ka tähelepanu, et §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.32	**Eelnõu § 1 p 9 – KüTS § 2 p 3[5]** Eelnõus peab olema eristatavad ja arusaadav, milline on küberoht ja milline on oluline küberoht. Seletuskirjast ei tule välja selle mõiste täpsustus ehk milline on „tõsine mõju“ ja milline on „märkimisväärne rahaline kahju“. On oluline, et selline osa oleks toodud välja seletuskirjas, nt tõsine mõju on kui süsteem maas oleks on nii pikk või mõjutab sellisel hulgal isikud või kaasneb märkimisväärne kahju, mis on aastakäibes selline protsent. ITL-i ettepanek on seega seda mõistet täpsustada. Äkki läbi mõju (lõppkasutajate arv vmt).	Osaliselt arvestatud ja selgitatud Termini „küberoht“ osas vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.31 vastust. Termin „oluline küberoht“ on esitatud ühetaolisel kujul direktiivis toodud definitsiooniga. Siseriiklikult ei ole võimalik definitsioonis toodud „tehniliste näitajate“ ringi kitsendada. Tegemist on määratlemata õigusmõistega ning valdkonna arengutempot ja volatiilsust arvestades on see põhjendatud. Seletuskirja on kõnealust terminit puudutavas osas täiendatud. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.33	**Eelnõu § 1 p 9 – KüTS § 2 p 3[6]** NIS2 direktiivi artikkel 6 punkt 15 kasutab siinkohas sõna „vulnerability“. Selgitame, et	Vt Riigi Infosüsteemi Ameti kommentaari 17.11 vastust.

	"vulnerability" ja "weakness" mõistetel tehakse infoturbes sageli sisulist vahet ja „vulnerability" tähenduses on kasutusel ikkagi "haavatavus" ja "weakness" on "nõrkus". Teeme ettepaneku sisustada see mõiste järgmiselt: (Võiks kasutada nt ISO27001 sõnastust) vara või meetme nõrk koht, mille saab ära kasutada üks või mitu ohtu.	
24.34	**Eelnõu § 1 p 9 – KüTS § 2 punktid 3^7 - 3^9** Teeme ettepaneku defineerida need terminid Eesti õigusaktide mõistete pinnalt, mitte ainult viidata EL-i määrusele.	Mittearvestatud ja selgitatud Eelnõus on tehtud viiteid EL õigusele ja seal defineeritud mõistetele - neid ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri" § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.35	**Eelnõu § 1 p 11 – KüTS § 2 punktid 4^6 ja 4^7** Toetame nende mõistete puhul viitamist EL-i õigusaktidele ning teeme ettepaneku lisada viide ka eIDAS 2 määrusele (määrus nr 2024/1183).	Mittearvestatud ja selgitatud Viidatakse EL määrusele, mitte seda muutvale määrusele. Vastasel juhul tuleks seadusi muuta iga kord, kui muutub viidatav (otsekohalduv) EL õigusakt. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.36	**Eelnõu § 1 p 12 – KüTS § 2 p 6**	Mittearvestatud ja selgitatud

	Siia on vaja mõistet, mitte viidet EL-i määrusele.	Tegemist on viitega EL õigusele ja seal defineeritud mõistele - seda ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.37	**Eelnõu § 1 p 13 – KüTS § 2 p 7^4** Teeme ettepaneku „on mõeldud“ asendada konkreetsema sõnastusega („on“). Lisaks kaaluda loetelu vormistamist punktidena.	Mittearvestatud ja selgitatud Kommenteeritava punkti sõnastuse puhul oli lähtutud sarnasest sõnastusest nagu avalikule kooskõlastusele edastatud eelnõu sama paragrahvi punktidest 1^2 ja 1^3 (uuendatud eelnõu tekstis KüTS § 2 punktid 14 ja 15). Normitehniliselt ei saa punkti sees alapunkte tekitada - vt Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 25 lõiget 2.
24.38	**Eelnõu § 1 p 14 – KüTS § 2 p 10** Siin jääb arusaamatuks, kas mõeldakse elektroonilise side teenust (elektroonilise side seadus (ESS) § 2 p 6) või üldkasutatavat elektroonilise side teenust (ESS § 2 p 68). Seletuskiri viitab üldkasutatavale teenusele. Tegu on olulise erinevusega, mistõttu palume seda täpsustada. Kui tegu pole üldkasutatava elektroonilise side teenusega, siis läheksid ka näiteks ettevõtete	Selgitatud Avalikul kooskõlastusringil olnud eelnõu versioonis oli kommenteeritud punktis viidatud „elektroonilise side teenusele“, kuid uuendatud eelnõust on see termin eemaldatud. Siin vt ka Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.22 vastust. Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.

	sisesed sidevõrgud (milles ei osutata üldkasutatavat teenust igaühele, kes tahab tüüptingimustel kättesaadavat teenust) KüTS-i regulatsiooni alla.	
24.39	**Eelnõu § 1 p 14 – KüTS § 2 p 13** Mõiste sisu ei vasta Eesti teadus- ja arendustegevuse seaduse § 3 lõikele 1. Tegemist on küll NIS2 direktiivi artikkel 6 punkti 41 otse ülevõtmisega. Samas sisu tundub olevat Eesti teadus-ja arendustegevuse seaduse mõttes eraõiguslik teadusarendusasutus (aga ei ole ka).	Selgitatud Kohustuste EL-ülese võimalikult ühetaolise rakendamise huvides on vajalik KüTSi kontekstis lähtuda NIS2 direktiivi järgsest definitsioonist ja selle põhjenduspunktis 36 esitatud selgitustest: *Teadusuuringutel on uute toodete ja protsesside väljatöötamisel võtmeroll. Paljusid neist tegevustest viivad ellu üksused, mis jagavad, levitavad või kasutavad oma teadusuuringute tulemusi ärilistel eesmärkidel. Need üksused võivad seega olla olulised osalejad väärtusahelates, mis muudab nende võrgu- ja infosüsteemide turvalisuse siseturu üldise küberturvalisuse lahutamatuks osaks. Teadusorganisatsioone tuleks käsitada nii, et need hõlmavad üksusi, mis pühendavad olulise osa oma tegevusest rakendusuuringutele või tootearendusele Majanduskoostöö ja Arengu Organisatsiooni 2015. aasta Frascati käsiraamatu „Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing and marketing of a product, process or the provision of a service“ („Teadus- ja arendustegevuse andmete kogumise ja esitamise suunised, et kasutada nende tulemusi ärilistel eesmärkidel, näiteks toote, protsessi või teenuse tootmiseks või turustamiseks“) tähenduses.* Nimetatud Frascati käsiraamatu järgi loetakse rakendusuuringuteks originaalne uurimistöö, mille eesmärk on omandada uusi teadmisi, ning eksperimentaalseks arendustegevuseks süstemaatiline töö, mis toetub teadustegevusest ja praktilistest kogemustest saadud teadmistele ning toodab lisateadmisi, mille eesmärk on uute toodete või protsesside loomine või olemasolevate toodete või protsesside täiustamine. „Äriline eesmärk“ on määratletud laialt, kui toote/protsessi tootmine või arendamine, teenuse osutamine või selle turustamine.

		Juhime ka tähelepanu, et KüTS §-s 2 esitatud terminite järjestus on muutunud, arvestades avaliku kooskõlastusringi käigus saabunud ettepanekuga viia loetelu parema loetavuse huvides tähestikulisse järjekorda.
24.40	**Eelnõu § 1 p 16 – KüTS § 3 lg [1[2]] p 10** 250+ töötajat ja bilansimaht on üle 43 mln euro või aastakäive üle 50 mln euro tähendab suurettevõtet. Sättes viidatakse keskmise suurusega ettevõtjale ning bilansimahud ja käibed on veel omakorda sassi läinud. Ehk siin on vasturääkivusi rohkem kui üks.	Arvestatud osaliselt ja selgitatud Sätte eesmärk on võtta üle NIS2 direktiivi artikli 3 lõike 1 punkt a) ehk viide on tehtud üksustele, kes ületavad keskmise suurusega ettevõtja ülemmäärasid (suurettevõtted). Kuna ülemmäärad, mille ületamine suurettevõtteks kvalifitseerumise tingib, on seotud keskmise suurusega ettevõtja definitsiooniga, sisaldub sättes ka vastav viide. Juhime tähelepanu, et KüTS §-de 1 ja 3 struktuur ja sisu on olulisel määral võrreldes avalikule kooskõlastusele saadetud eelnõuga muutunud. Bilansimahtude ja käibe osas on näitajaid korrigeeritud, sh muudatus viidud uuendatud eelnõu tekstis KüTS §-i 3.
24.41	**Eelnõu § 1 p 19 – KüTS § 3 lg 3[1]** Sätet lugedes tekkisid järgmised küsimused: - Punkti 3 puhul jääb arusaamatuks, mida tähendab asjakohasel juhul. Seletuskirjas lk 73 öeldakse, et seda ei pea kõik üksused esitama. Kes siis peab? Sama kommentaar eelnõu § 1 p 21 – KüTS § 4 lg 1 p 2 kohta. - Kas vastava teemal teeb teenuse osutajale esmase päringu RIA? Kui jah, siis millal vastav päring tehakse? Kui ei, siis kuidas see protsess ette näeb? Milline on vastamise tähtaja pikkus? - Mida mõistetakse IP aadresside vahemiku all ja mis on selle eesmärk? Juhime veel tähelepanu, et seletuskirjas lk 145 viidatud once only põhimõte ehk ühekordne teavitus IT-lahenduse/digitaalse teenuse kaudu peaks olema prioriteet. Kindlasti on ka oluline, et andmeid, mis ükskõik millisel riigiasutusel olemas on, ei tohi uuesti küsida. Praegu jääb seletuskirjast mulje, et kõik on väga lahtine. Kas see on tõesti nii?	Selgitatud vastavalt esitatud küsimuste järjekorrale - „Asjakohasel juhul“ on riigisisese õiguse sõnastuslik vaste NIS2 direktiivi tekstis kasutatule „kui see on kohaldatav“. Teisisõnu, nagu seletuskirjas viidatud sätte juures selgitatud, hõlmab sättes toodud ülesanne ka domeeninimede registreerimise teenuse osutajate tuvastamist, kuna need pole üliolulised üksused ega olulised üksused. Järelikult ei saa domeeninimede registreerimise teenuseid osutajad ka NIS2 direktiivi I või II lisas osutatud sektorit/allsektorit teavitada. - Riigi Infosüsteemi Ameti poolset esmast teavitust teenuseosutajatele ei tehta. Üksused, kellele KüTS kohaldub, esitavad sättes toodud teabe Riigi Infosüsteemi Ametile, misjärel koostab Amet saadud info põhjal vastava loetelu. Subjektsuse tuvastamise kohustus lasub subjektil. Vastavate andmete esitamise tähtaeg on ette nähtud üleminekusätetes – vt eelnõu KüTS § 28[1] ning asjakohasel juhul ka §-i 4[1]. - Internetiprotokolli aadresside vahemiku andmed on ette nähtud NIS2 direktiivis (vt artikkel 3 lõike 4 punkti b ja artikkel 27 lõike 2 punkti f). Need annavad pädevale asutusele indikatsiooni, kelle omandis on turvahaavatavusega seade või süsteem. Riigi Infosüsteemi Ametil on kohustus KüTS § 12 lg 3 kohaselt edastada isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid. Ehk internetiprotokolli aadresside vahemikud võimaldavad sihistada antud ohuteateid konkreetsetele teenuseosutajatele.

		- Hetkel puudub sellekohane info konsolideeritud ja ühetaolisel kujul. Seletuskirjas on sedastatud, et eelnõu koostamise hetkel ei olnud analüüsitud, kas seda teavitust on võimalik teha ka mõnda IT-lahendust kasutades. Siin vt ka Regionaal- ja Põllumajandusministeeriumi kommentaari 7.6 vastust.
24.42	**Eelnõu § 1 p 19 – KüTS § 3 lg 3[4]** Selle sätte eesmärk jääb arusaamatuks. Sõnastuse kohaselt võivad üksused juhinduda viidatud suunistest, kuid võivad ka mitte. Oluline on selgelt aru saada, millest juhinduda tuleb ja mis on otsekohalduv. Sama kommentaar eelnõu § 1 p 21 – KüTS § 4 lg 1[4] kohta.	Selgitatud Tegemist on vabatahtliku võimalusega järgida viidatud suunistest ja vormidest ehk tegemist ei ole otsekohalduvate suuniste ja vormidega. Siin vt ka Regionaal- ja Põllumajandusministeeriumi kommentaari 7.6 vastust.
24.43	**Eelnõu § 1 p 22 – KüTS § 5 lg 1** Esimese lause teine pool (alates komast) vajab grammatiliselt üle vaatamist. Samas – kas seda lause teist poolt on üldse vaja eelnõus sätestada?	Arvestatud ja selgitatud Lause on üle vaadatud. Esimese lause teine pool on vajalik, et oleks selge, et riikliku küberturvalisuse strateegiat oleks võimalik koostada digiühiskonna arengukava ühe osana.
24.44	**Eelnõu § 1 p 22 – KüTS § 5 lg 3 p 3** Teeme ettepaneku lisada sättesse lühend CSIRT.	Mittearvestatud ja selgitatud CSIRT lühend on inglise keelne lühend sõnadest *„computer security incident response team“*, kuid seaduseelnõu keelekasutus peab vastama eesti kirjakeele normile. Samuti võib kasutada võõrsõna (mitte võõrkeelset lühendit) üksnes juhul, kui selle kasutus on eesti keeles levinud või kui sõnal puudub eesti keeles algupärane vaste. Samuti välditakse seaduseelnõu tekstis lühendeid. Siin vt Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 15 lõiget 1, 17 lõiget 3 ja § 19 lõiget 1.
24.45	**Eelnõu § 1 p 22 – KüTS § 5 lg 5** Mis on „ajaomastele teenustele“ ja „asjakohasel juhul“ tegelik sisu? Punkti 15 osas on vajalik selle kontrollimise dokumenteerimine või logimine. Selline kontroll peab olema kokkulepitud tegevus, mis ei sea ohtu teenust ning viiakse läbi ikkagi teenuse osutaja teadmisel.	Selgitatud Viidatud sätte sisu on viidud Riigi Infosüsteemi Ameti põhimäärusesse. Tegemist on määratlemata õigusmõistetega, mis tuleb sisustada juhtumipõhiselt. NIS2 direktiivi inglise keeleses tekstis käsitletakse seda *„essential and important entities concerned“,* mis tähendab olukorrast puudutatud osapooli. Kirjeldatud ennetaval kontrollil ei tohi olla negatiivset mõju teenuseosutaja osutatava teenuse toimimisele.

24.46	**Eelnõu § 1 p 23 – KüTS § 5^2 lg-d 2 ja 3** Õigusselguse mõttes ei ole selline edasivolitamine mõistlik. Jääb arusaamatuks, miks minister volitab täitevasutuse edasi volitama. Teeme ettepaneku fikseerida koheselt ja ilma edasi volitamiseta asutuse, kes on vastav pädev asutus. Juhul, kui seda ei soovita teha, siis palume selgitada, miks soovitakse see pädev astus osaliselt lahtiseks jätta ja kuidas isikuid teavitataks, kui asutus muutub.	Vt Riigi Infosüsteemi Ameti kommentaari 17.37 vastust.
24.47	**Eelnõu § 1 p 24 – KüTS § 6^1** Esimene küsimus on, kes on juhtorgan antud sätte mõttes. Kas nõukogu, juhatus või ainult juhatuse esimees? Kui lähtuda äriseadustiku definitsioonist, siis juhtorgan osaühingu ja aktsiaseltsi puhul on juhatus. Et kas siis on mõeldud, et kogu juhatus peab tagasi astuma? Palume täpsustada seda eelnõus. Teiseks palume punkt 2 osas täpsustada, et kui spetsiifilisel tasemel peab juhtorgan turvameetmed heaks kiitma. Võib eeldada, et enamik ettevõtete juhatusi ei oma piisavaid pädevusi, et otsustada ega mõista konkreetseid turvameetmeid (nt mis protokolle, krüpteerimismeetodeid vm) kasutada. Lisaks: NIS2 direktiivis räägitakse hoopis "riskijuhtimismeetmetest", mis erinevad turvameetmetest. Eelnõu peab lähtuma direktiivist, mitte laiendama kohustusi. Kolmandaks on vaja selgust, kes hindab, milline koolitus on piisav selle nõude täitmiseks. Tegemist on kohustusega, mille rikkumisel ootab ees vastutus.	Selgitatud kommentaaris esitatud teemade järjekorras - Juhtorgani osas vt Advokatuuri kommentaari 20.9 vastust. Eelnõu on vastavalt muudetud. - NIS2 direktiiv näeb ette, et juhtorgani (eelnõus juhatuse liikme või liikmete ehk juhatuse) tasand on see tasand, kus toimub turvameetmed heaks kiidetakse. Seletuskirjas on selgitatud, et tegemist on juhatuse liikme tasandi ülesandega, mida ei ole võimalik edasi delegeerida. See tõlgendus tuleneb nii eelnõu koostajatele Euroopa Komisjoni poolt antud selgitustest kui ka NIS2 direktiivi artikli 21 lõike 5 alusel antud rakendusmäärusest 2024/2690, mille põhjenduspunkt 9 viitab ka sellele, et taolised aspektid tuleb juhtorgani tasandil (eelnõus juhatuse tasandil) heaks kiita. Sama rakendusmääruse lisa, mis täpsustab selle rakendusmääruse artiklis 2 osutatud tehnilisi ja metoodilisi nõudeid, viitab ka sellele, et seda rakendusmäärust järgivate üksuste puhul on juhtorganil (eelnõus juhatuse tasandil) erinevaid ülesandeid seoses riskijuhtimismeetmetega (eelnõu mõttes turvameetmetega) ning nende rakendamise ja kontrolliga. - NIS2 direktiivi sõnastuses on kasutatud sõnastust „riskijuhtimismeetmed", kuid eelnõusse üle võtmisel on kasutatud sõnastust „turvameetmed". Seda on ka seletuskirjas selgitatud ning see ei tähenda, et seetõttu on direktiivi kohustusi laiendatud. - Koolituse sisu ja välba osas vt Rahandusministeeriumi kommentaari 6.1 vastust.

	Seletuskirjas palutakse tagasisidet, kas peaks määratlema ka nende koolituste tegemise välp ehk mis aja tagant tuleks taolisi koolitusi teha. Leiame, et teatav miinimumnõue selles korrapärasuses peaks olema, sest kord 10 aasta jooksul pole piisav. Teadlikkus küberriskidest on organisatsioonides madal ja neisse riskidesse kiputakse suhtuma üleolekuga. Vt ka käesoleva kirja II osa punkti 5 [(siinse tabeli kommentaaris 24.15)].	
24.48	**Eelnõu § 1 p 26 – KüTS § 7 lg 2** Siin vajab sätte algus korrigeerimist, sest sätestab, et muudetakse selle lõike punkte 1-3, kuid tegelikult tekitatakse 14 punkti. Teeme ettepaneku tõlkida turvameetmete nimekiri täpselt NIS2 direktiivist, praegu on tekitatud meetmeid juurde sõnastuste muudatustega. Isegi kui need on väikesed ning sisuliselt on proovitud osa teemasid lahti lüüa eraldi punktideks. Punkti 9 osas kommenteerime, et küberhügieen ei ole ametikult kasutatav termin. Selle välja toomine eelnõus on täiesti ebamõistlik. Mis asi see on? Selle sõna võiks üldse välja jätta. Organisatsioonid on erineval tasemel. Hakata küberturvalisuse teenust pakkuvates organisatsioonides regulaarseid hügieenikoolitusi tegema ei tundu eriti mõistlik. Punktide 10 ja 13 osas on taas küsimus, mis on „asjakohane juht“. See tuleb siduda riski kaalutlemisega. Punkt 13 valgub üsna laiali – et on justkui turvaline ja siis ebaturvaline(?) lahendus ja siis peaks asjakohasel juhul valima turvalise ja mitteasjakohasel ebaturvalise?	Arvestatud ja selgitatud vastavalt kommenteeritud punkti arvestades - Paragrahvi muutmiskäsu sõnastust on muudetud. Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavaneid). Tolle sätte sõnastamisel on arvestatud ja lähtutud kommentaaris toodud ettepanekust. Järgmised kommentaarid on esitatud tolle määruse muutmise kavandi kontekstis. - p 9: jätame välja sõna „küberhügieen“; - p -d 10 ja 13: sõnad „asjakohasel juhul“ tähendab, et kui see on konkreetse teenuseosutaja puhul kohaldatav. Kui seda otsesõnu siduda riskide kaalutlemisega, siis ei oleks see sõnastus kooskõlas NIS2 direktiivi artikli 21 lõike 2 sõnastusega ehk vastuolus siinse kommentaari ettepanekuga. - Punktis 13 ei ole mainitud ebaturvalist lahendust, mistõttu on see kommentaar segane.
24.49	**Eelnõu § 1 p 27 – KüTS § 7 lg 2[1]**	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.

	Kaitsetarve ei ole üldiselt mõistetav termin. Teeme ettepaneku selle ja teised E-ITS standardis kasutatavad ja ainult E-ITS sõnastikus defineeritud spetsiifilised mõisted eelnõust välja jätta.	
24.50	**Eelnõu § 1 p 29 – KüTS § 8 lg 1** Kui teenuse osutaja on MSSP (Managed Security Service Provider), kes osutab teenust KüTS subjektidele, siis kes sel juhul on kohustatud isik? Kas MSSP või klient, kellega intsident aset leidis?	Selgitatud Üldine loogika on, et KüTSi teenuseosutaja teavitab olulise mõjuga küberintsidendist ja soovi korral ka muudest küberintsidentidest. Kui tegemist on infoturbeteenuse osutaja (MSSP) enda süsteemidega seotud küberintsidendiga, siis esitab vastava teate MSSP - nt olukorras, kus sama juhtum võib mõju avaldada ka teistele KüTSi teenuseosutajatele (MSSP klientidele). Kui MSSP osutab teenuseid mõnele teisele KüTSi teenuseosutajale (tema jaoks kliendile), siis konkreetse teavitaja selgeks tegemiseks tuleb MSSPl ja tema kliendil see detail selgeks teha. Näiteks võib olla siin kokkulepe, et MSSP ise teavitab kliendi nimel vms. Kuid peamine on, et kui tegemist on olulise mõjuga küberintsidendiga, et sellest teavitatakse pädevat asutust.
24.51	**Eelnõu § 1 p 31 – KüTS § 8 lg 2** Siin ja KüTS § 8 lg 3 on oluline küberintsident. Umbes sama on terminites KüTS § 2 p 3^1 ulatuslik küberintsident. Kas need on ühe tähendusega või erinevad mõisted?	Selgitatud Tegemist on erinevate mõistetega ning need on eelnõus ka erinevalt sisustatud-defineeritud. Olulise mõjuga küberintsident võib olla ka „ulatuslik küberintsident“, kuid ei pruugi seda olla. Ulatuslik küberintsident on alati ka olulise mõjuga küberintsident.
24.52	**Eelnõu § 1 p 33 – KüTS § 8 lg 4^1** Punkti 1 kohaselt tuleb anda teavet “turvarikkemärgi” kohta. Kas see on üldtuntud termin ega vaja seletust või võiks selle ikkagi lahti seletada? Mujal eelnõus seda ei esine. NIS2 direktiivi eesti keelses versioonis on see artikkel 23 lg 4 punkti b viimane sõna „turvarikke indikaator“ (ingl. k: the indicators of compromise). Sama NIS2 direktiivi põhjenduspunkt 102. Mis on selle tegelik sisu?	Vt Välisministeeriumi kommentaari 10.2 vastust.
24.53	**Eelnõu § 1 p 33 – KüTS § 8 lg 4^2** Vahearuande küsimine on RIA võimalus ehk puudub selgus, millal RIA võib vahearuannet	Selgitatud Teavituskohustuse, sh selle erinevate etappide sisu on eelnõus korrigeeritud ning seletuskirjas täpsustatud, kuid viitame NIS2 artikli 23 lõike 4 punktidele c–e, millest

	küsida. Mingil liiga varasel hetkel (näiteks poliitilise surve tõttu) võib vahearuande nõudmine võtta ära aja küberintsidendi lahendajalt. Seletuskiri lk 89 tähtaega ei määratle, kas see on siis organisatsiooni enda otsustada? Ebaselgus on veel suurem kui küsitakse "täiendavat teavet". Mis on see "asjakohane juht", kui seda küsitakse? Arusaamatuks jääb ka mis on vahearuande eesmärk. Kas RIA soov olla lihtsalt kursis või aidata lahendada? On vist olnud juhtumeid kus RIA ei vaja vahearuannet aga seda küsib ootamatult Vabariigi Valitsus. Teeme ettepaneku kaaluda, kas vahearuanne on põhjendatud pigem ulatusliku mõjuga, mitte olulise mõjuga intsidendi korral. Kui need on erinevad, vt ka p 32 [(siinse tabeli kommentaaris 24.51)].	johtuvalt võib aru saada, et Riigi Infosüsteemi Amet võib küsida vahearuannet siis, kui lõpparuannet (eelnõus raportit) ei ole esitatud. Viimase esitamine sõltub omakorda ennekõike sellest, kui kiiresti mingi küberintsident lahendatakse. Kui üks kuu pärast (olulise mõjuga) küberintsidendi teate (eelnõus intsidenditeate) esitamist jätkuvalt toimub küberintsidendi lahendamine, siis on lõpparuanne (eelnõus raport) käsitatav vahearuandena ehk teenuse osutaja peab selle igal juhul esitama ühe kuu jooksul. Täiendava teabe küsimisega soovitakse lisateavet võrreldes juba esitatud teatega. „Asjakohasel juhul" on sisuliselt olukorras, kus seda lisateavet on vaja juurde küsida. Direktiiv otsesõnu ei võimalda määratleda, et vahearuannet on võimalik küsida ühe või teise küberintsidendi korral, mistõttu seda vahetegu ei ole ka eelnõus tekitatud. Vt siin ka Siseministeeriumi kommentaari 8.7 vastust.
24.54	**Eelnõu § 1 p 35 – KüTS § 8 lg 7** Kui teenuse osutaja on MSSP (hallatud turbeteenuse osutaja), kes osutab teenust KüTS subjektidele, siis kes sel juhul on kohustatud isik? Kui teenuse osutaja on MSSP siis toob see kaasa dubleerivad tegevused ning lisapersonali palkamise aruannete koostamiseks, mis omakorda tõstab teenuse hinda klientidele. Lisaks moonutab dubleeriv andmete edastamine tegelikku statistikat. Ehk see säte illustreerib, et kohustused ja vastused hallatud teenuse osutaja vaatest vajavad selgitamist. Lisaks tekib küsimus, kui vahendajaid on mitu.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.50 vastust.
24.55	**Eelnõu § 1 p 39 – KüTS § 8[1]**	Selgitatud

	Säte reguleerib vabatahtlikku teavitamist. Leiame, et seaduse tasemel kehtestada, et võib teavitada, tundub kummaline. RIA võib seda soovi korral oma kodulehel reklaamida ja luua vastava kanali. Lg 1 osas palume täpsustada, kas tegemist on intsidentidega, mis ei ole KüTS § 8 all toodud. Lg 2 sätestab, et anonüümsus on tagatud üksnes avalikult. Lause esimene pool on eksitav jättes mulje, et ka RIA-le saab esitada anonüümselt ilma, et nemadki isikut teaksid.	Vabatahtliku teavitusmehhanismi seaduse tasandil reguleerimine võib esmapilgul tunduda ebavajalik, kuid arvestades, et (i) märkimisväärne osa teenuseosutajatest on riigiasutused, vajavad nad igasuguseks tegevuseks õiguslikku alust; ning (ii) NIS2 direktiivi artikli 30 lõike 2 (menetluskord) ülevõtmine on igal juhul kohustuslik, mistõttu ei ole head lahendust jätta ka lõiget 1 üle võtmata. Lõike 1 puhul on tegemist muude küberintsidentidega, mis ei ole olulise mõjuga küberintsidendid KüTS § 8 tähenduses. Lõike 2 puhul näeb NIS2 artikkel 12 lõike 1 teise tekstilõigu esimene lause, et nõrkusest (eelnõus turvahaavatavusest) võidakse teavitaja „taotlusel“ esitada ka anonüümselt. Direktiivi tekst ei täpsusta, kas see tähendab ka täielikku anonüümsust ehk ka Riigi Infosüsteemi Amet ei tea teavitaja isikut või on siin mõeldud seda, et Amet tagab teavitava isiku anonüümsuse. Samas näeb direktiiv ette, et kui tegemist on turvahaavatavusest teavitamisega, siis on siin Riigi Infosüsteemi Amet nö vahemees, kes suhtleb nii teavituse tegija kui ka potentsiaalse nõrkusega IKT-toodete tootja või IKT-teenuste osutaja vahel, tegutsedes ükskõik kumma poole taotlusel (vt NIS2 direktiivi artikli 12 lõiget 1). Seetõttu ongi lisatud vastavasse lõikesse teine lause, mis kohustab omakorda Riigi Infosüsteemi Ametit tagama teavitaja isiku anonüümsust, kuid see ei tähenda, et teavituse enda tegemine peab olema anonüümne.
24.56	**Eelnõu § 1 p 41 – KüTS § 12 lg 3[1]** Sättest jääb mulje nagu RIA ise ei võiks abi pakkuda. Kas see on nii? Siit sättest on puudu NIS2 direktiivi artikkel 23 lõikes 5 veel sätestatud pädeva asutuse (st. RIA) kohustus “anda nõu, kuidas toimida” ja “ka juhiseid olulisest intsidendist õiguskaitseasutuste teavitamiseks“.	Selgitatud Kommentaaris mainitud lõige reguleerib selgituste ja suuniste andmist. Seetõttu jääb kommentaari puhul ebaselgeks, et mis laadi abi on siin veel mõeldud. Seletuskirjas on selgitatud, et tagasiside all ongi mõeldud kommentaaris mainitud nõu ja juhiseid.
24.57	**Eelnõu § 1 p 41 – KüTS § 12 lg 3[2]** Millisel juhul eelistatakse ametlikku teavitamist vabatahtlikule? Selle sätte mõte jääb arusaamatuks, viites on midagi valesti.	Selgitatud NIS2 direktiivi artikkel 30 lõike 2 esimese tekstilõigu teine lause sedastab: „Liikmesriigid võivad seada kohustuslike teadete menetlemise vabatahtlike teadete menetlemisest tähtsamale kohale.“ Ehk siin võib CSIRT eelistada, et ta tegeleb ennekõike kohustuslikus korras esitatud intsidentidega (eelnõus olulise mõjuga küberintsidentidega). Millal seda tehakse, on CSIRTi diskretsiooniotsus.

24.58	**Eelnõu § 1 p 44 – KüTS § 12 lg 5** Antud juhul võetakse NIS2 säte üle kitsamalt ja subjektide jaoks piiravamalt. NIS2 direktiivi artikkel 2 lg 13 kohaselt võib vahetada ainult teavet, mis on teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne. Teabevahetuse puhul tuleb säilitada asjaomase teabe konfidentsiaalsus ning kaitsta asjaomaste üksuste turvalisust ja ärihuve. Palume need samad põhimõtted viia eelnõuga sisse ka KüTS-i.	Arvestatud – lõike teksti on muudetud.
24.59	**Eelnõu § 1 p 49 – KüTS § 13[3]** See säte on ebamäärane ja jääb ebaselgeks. Küsimus on kas valitsus kehtestab nõuded protsessidele v.a. siis kui on olemas õigusakt, protsessid töötab välja teenuse osutaja või protsessid sertifitseeritakse. Tundub, et viga on eestikeelses tõlkes ja NIS2 direktiivi mõte on selles, et võib nõuda teenuses kasutatavate teenuseosutaja enda või kolmanda isiku loodud IKT toote, teenuse jms sertifitseerimist EL küberturvalisuse skeemide kohaselt. Üldisem küsimus on, et kas lisaks nendele KüTS-i skeemidele on lubatud ka muudel alustel sarnased sertifitseerimisskeemid? Näiteks siseriiklikult meil lubatud EITS-i ja ISO järgi auditeerimine, ISO-t sertifitseeritakse. Kas nõutakse neile lisaks? Siin tuleb lisada ka täpsustus, et kui on teenuseosutaja valdkonna spetsiifiline sertifitseerimisskeem, siis aktsepteeritakse seda ja ei tohi nõuda midagi sinna otsa. Näiteks eIDAS alusel või rahvusvaheliste standardite alusel	Arvestatud ja selgitatud Tolle paragrahvi eesmärk oli tekitada võimalus Vabariigi Valitsusel anda määrus, millega pannakse teenuseosutaja(te)le kohustus järgida EL küberturvalisuse sertifitseerimise skeemi, et tagada KüTS § 7 nõuete täitmine. Kvalifitseeritud usaldusteenuse osutajate jaoks on ette nähtud eraldi nõuded KüTS § 7 täitmise tõendamiseks - need tulenevad NIS2 direktiivi artikli 23 lõike 5 alusel antud rakendusaktist (vt eelnõus ka KüTS § 7 lõiget 7). Eelnõust on vastav paragrahv välja jäetud, et võtta üle NIS2 direktiiv minimaalses mahus.

	sertifitseeritakse kvalifitseeritud usaldusteenuse osutajaid. Praegu nähakse vaeva, et viia nõudeid NIS2 direktiiviga kooskõlla.	
24.60	**Eelnõu § 1 p 52 – KüTS § 14 lg 6** Tegemist on ebaselge sättega, mis ütleb, et üldreeglina kasutakse seda või teist. Mõistlik oleks selgelt väljendada, millistel juhtudel (subjektide osas) on järelevalve ennetav ja millistel juhtudel järelkontrollina. Punkt 1 ja 4 annavad justkui täitsa vaba tõlgenduse, kelle juurde kontrollima minna, küll põhjenduse leiab.	Selgitatud Eelnõu KüTS § 14 lg 6 p 1 on mõeldud NIS2 direktiivi artikli 32 lõikes 2 sätestatud vabatahtliku põhimõtte ülevõtmiseks - seda ülevõtmata oleks järelevalve kõigi subjektide osas intensiivsem ja paindumatum, kuivõrd Riigi Infosüsteemi Ametil puuduks prioriseerimise võimalus. Prioriseerimist ei saa direktiivi järgi ega mõistlikkuse põhimõttest tulenevalt aga kohustuseks määrata - vastasel juhul võib järelevalve end prioriseerimisega omadesse reeglitesse „kinni kirjutada“ ja mitte reageerida olulistele muutustele küberruumis. Vastavalt eelnõu järgse KüTS § 14 lg 6 p-dele 2 ja 3 on üliolulise üksuse suhtes kontroll nii ennetava kui järelkontrolli formaadis, olulise üksuse suhtes aga järelkontrolli formaadis.
24.61	**Eelnõu § 1 p 52 – KüTS § 14 lg 7** Eelnõus ega NIS2 direktiivis ei ole defineeritud ega loetletud, mis on olulised nõuded (ja mis on siis mitte olulised nõuded). Kust seda teada saaks? Kes neid hindab?	Selgitatud „Oluline“ on määratlemata õigusmõiste, mis vajab tõlgendamist ja hinnangu andmist. NIS2 direktiivi artikli 32 lg 7 punkt a ei näe ette täpsemaid kriteeriume selle kohta, mis nõudeid pidada oluliseks, seega ei ole ka riigisiseselt direktiivi ülevõtmisel täpsemaid lahendusi ette nähtud. Samas on NIS2 direktiivi artikli 32 lg 7 punkti a alapunktide i)-v) alusel KüTS-i § 14 lõikes 8 ette nähtud täpsemad kriteeriumid, mille abil rikkumise raskust hinnata. Kuivõrd tegemist on sättega, mis reguleerib järelevalve teostamist pädeva asutuse poolt, annab esmase hinnangu pädev asutus, kelleks Eestis on Riigi Infosüsteemi Amet. Sama hinnang on omakorda ka kohtulikult kontrollitav.
24.62	**Eelnõu § 1 p 52 – KüTS § 14 lg 8** Siduvate juhiste andmist ei ole reguleeritud. Siin on “siduv juhis” üks ja ainus kord eelnõus ja selle andmist ei ole reguleeritud. KüTS § 12 lg 3^1 on “suunised”. Seletuskirja kohaselt võetakse üle NIS2 direktiivi artikkel 32 lg 7 punti a alapunktid i-v, kus on tõesti kirjas juhised. Samas KüTS § 14 lg 9 kohta on seletuskirjas (lk. 94): Kui mingis NIS2 direktiivi sättes on kasutatud	Arvestatud ja selgitatud Eesti õiguses tõesti ei ole kasutusel instituuti „siduv juhis“. KüTS § 14 lg 8 punkti 4 sõnastust on parandatud, et see vastaks samale loogikale, mis on sama paragrahvi lõikes 9 (eelnõu uues versioonis KüTS § 16 lõikega 1^1) – tegemist on olukorraga, kui järelevalveasutuse tehtud ettekirjutuses toodud puudused on jäetud kõrvaldamata.

	sõnastust „korraldus“ või „siduvad juhised“, siis eelnõus on selle all mõeldud ettekirjutust. Ehk see säte vajab selgitust ja igal juhul tuleb saada selgeks mis (siduv juhis, suunis, …) on õigusakt või ühekordne haldusakt. Siduv juhis ei ole vist Eesti õiguses kasutusel?	
24.63	**Eelnõu § 1 p 52 – KüTS § 14 lg 9** Punkt 2 sihipäraste turvaauditite puhul võiks olla ka eelnõus toodud ära, et kui palju RIA peab teenuse osutajat sellest soovist audit läbi viia ette teavitama. Samuti tuleb teenuse osutajat teavitada, et kes viib auditi läbi ja teenuse osutajale peab jääma võimalus esitada auditi läbiviijale põhjendatud vastuväiteid. Punkti 2 osas tekib ka küsimus, mis on muu riskialane teave. Punktis 3 tekitab küsimusi „vajaduse korral” - millise või kelle vajaduse? Milles seisnevad punktis 3 nimetatud “turvalisuse kontrollid”? Punktis 10 on kasutuses vastavushaldur, mille mõiste on E-ITS-I rollisõnastikus, kuid seaduses defineerimata. ITL-i ettepanek on E-ITS spetsiifilisi mõisteid eelnõus mitte kasutada.	Selgitatud vastavalt kommentaaris esitatud punkti kohta järgmist: - Punkt 2: kuna NIS2 direktiiv seda aspekti ei reguleeri, siis kohalduvad siin haldusmenetluse üldised põhimõtted. "Muu riskialase teave" ei ole NIS2 direktiivis täpsemalt selgitatud, kuid eelduslikult on siin mõeldud nt avastatud nõrkused või muu ohuhinnang konkreetsel teemal. - Punkt 3: turvalisuse kontrolli olemust on seletuskirjas selgitatud. Sõnad „vajaduse korral“ indikeerivad, et seda tehakse sõltuvalt olukorrast koostöös konkreetse teenuseosutajaga. - Punkt 10: juhime tähelepanu, et NIS2 direktiiv näeb ette, et sellist rolli kandvat isikut võidakse teatud KüTSi üliloluliste üksuste suhtes kindlaks määrata. NIS2 direktiivi artikli 32 lg 4 punkti g Eesti keelses tekstis on siin kasutatud sõnastust „seireametnik“ (inglise keeles *„montoring officer“*), mille olemus ei oleks ka niivõrd selge (sh pole sellist vastet ka AKITis). Seetõttu on siin kasutatud sõna „vastavushaldur“, mis on kasutusel Eesti infoturbestandardis ning mis on kõige lähedasem ja selgem mõiste iseloomustamaks *„monitoring officer“* ülesannet. Lisaks eeltoodule märgime, et avalikul kooskõlastusel olnud eelnõu KüTS § 14 lõiked 9–14 on viidud uuendatud eelnõus KüTS §-desse 16 ja 17.
24.64	**Eelnõu § 1 p 52 – KüTS § 14 lg 10** Teeme ettepaneku punkt 4 eelnõust eemaldada. Juhime tähelepanu, et NIS2 direktiivi ülevõtmisega ei ole kohustust kehtestada kulude katmise osa, eriti tehes seda täiesti põhjendamatult. Lisaks ei nähtu seletuskirjast, mis väljamineku see võib põhjustada ja kokkuvõtlikult jääb üldine mulje, et sellega soovitaks luua olukord, kus ISO 27001 teed läinud isikute/asutuste osas tekiks	Mittearvestatud ja selgitatud NIS2 direktiivi artikli 32 lõike 2 kolmanda tekstilõike teine lause ja 33 lõike 2 kolmanda tekstilõike teine lause on mõlemad sõnastuses: „Sõltumatu organi poolt läbi viidava sihipärase turvaauditi kulud tasub auditeeritud üksus, välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti.“ Seega ei ole võimalik kommentaaris esitatud ettepanekut arvestada – vastasel juhul toimub NIS2 direktiivi valesti üle võtmine. Pärast kooskõlastamist on aga eelnõu täiendatud KüTS § 16 lõikega 1^2 ja § 17 lõikega 1^2 mis näevad ette volitusnormi sihipärase turvaauditi korraldamise täpsemate tingimuste ja korra kehtestamiseks. Sealhulgas saab määrusega kehtestada

	olukord, kus on võimalik auditeerida KüTS eelnõu 7 lõikes 2 ja 2^1 toodud E-ITS meetmeid ja selle eest peaks tasuma isik/asutus ise. Palume selgitada selle punkti eesmärki ja muuta see selliselt, et RIA-l on enne auditi tellimist selgituskohustus, miks seda tehakse ning see selgituskohustus täpselt lahti kirjutada ka seletuskirjas, et oleks kohuslastele arusaadav. Lisaks tuua välja ka aeg, mille jooksul on võimalik esitada vastulauseid.	loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale turvaauditi kulu ja kulu hüvitamise korra. Mõistame, et uute reeglitega rakendamisega kaasnevad kulud, kuid õigusakti eelnõu koostamisel ei ole alati võimalik ette näha, kelle suhtes tuleks või peaks sihipärast turvaauditit tegema. Seda enam, et võimaliku kulu suurus võib varieeruda konkreetsest auditi skoobist kui ka konkreetse üksuse enda võrgu- ja infosüsteemidest. Nimetatud lõikega ei soovita tekitada olukorda, kus „ISO 27001 teed läinud isikute/asutuste osas tekiks olukord, kus on võimalik auditeerida eelnõu KüTS § 7 alusel kehtestud Eesti infoturbestandardi meetmeid“. Eelnõu mõte ei ole ka siin eristada neid üksusi, kes rakendavad Eesti infoturbestandardit ning neid, kes rakendavad rahvusvahelist standardit ISO/IEC 27001. Tegemist on EL õiguse ülevõtmisega. Eesti infoturbestandardi ja selle alternatiiviks oleva rahvusvahelise standardi ISO/IEC 27001 rakendamine on nõude mõttes olnud riigisisene valik. Tegemist on seega kahe eraldiseisva küsimusega. Esitatud ettepaneku viimase tekstilõike osas selgitame, et sihipärase turvaauditi sisu osas ei ole NIS2 direktiivis ette nähtud kommentaaris mainitud sätteid. Siiski saab ja tuleb Riigi Infosüsteemi Ametil konkreetses olukorras teha diskretsiooniotsus selle meetme kasutamiseks (vt haldusmenetluse seaduse § 4), sh selgitada teenuseosutajale, kas ning mis põhjusel soovitakse auditit tellida.
24.65	**Eelnõu § 1 p 55 – KüTS § 17^3** Lg 6 osas palutakse seletuskirjas tagasisidet, kas kommenteeritava lõike puhul on vaja ka sätestada, et teise riigi pädeva asutuse töötaja võib kasutada KüTSis sätestatud meetmeid, mida saab eelnõu tulemusena kasutada ainult Riigi Infosüsteemi Amet või piisab sellest, et vastavad volitused on ja jäävad ainult Riigi Infosüsteemi Ametile? Kui ootus on, et teise riigi pädev asutus võiks kasutada ka KüTS-is sätestatud meetmeid, siis kas ta võiks kasutada kõiki meetmeid või osasid neist – viimase variandi korral, milliseid meetmeid?	Võetud teadmiseks - vastavaid volitusi siinse eelnõuga ei tekitata.

	ITL-i liikmed ei kujuta hästi ette seda halduskoormuse kasvu, kui neid ametkondi (ja seda rahvusvaheliselt) lisandub, kellel on õigus auditeerida ja küsida aruandeid ning trahvida ka veel. Samuti puudub Eesti ettevõttel teadmine sellest, kas välismaine asutus on tegelikult ikka ka riigiasutus ja mis pädevused tal oma riigiski on.	
24.66	**Eelnõu § 1 p 56 – KüTS § 17[4]** See pealkiri on vale. Tegu on volitustega teha koostööd erinevate osapoolte ja ametkondadega. Omaette küsimus on, kas see paragrahv on üldse seaduses kajastatav teema või peaks see olema Vabariigi Valitsuse määruse tase. Või ei vaja see üldse reguleerimist õigusaktiga? Lõike 2 osas tekitab küsimusi see, et teabevahetus on ette nähtud ainult ETO-dega. Aga teised üksused, kellel on intsident vms?	Selgitatud Pealkiri on üle vaadatud ja see jääb samaks – tegemist on ennekõike NIS2 direktiivi artikli 8 kohaste pädevate asutuste ehk Riigi Infosüsteemi Ameti ning julgeolekuasutuste tehtava koostöö reguleerimisega teiste asutustega. Lõike 2 kommentaari osas juhime tähelepanu asjaolule, et selle puhul on tegemist NIS2 direktiivi artikli 13 lõike 5 üle võtmisega. Kuna direktiiv võetakse üle kitsas sõnastuses, siis ei ole teiste üksuste kontekstis sarnaseid sätteid tekitatud. Siiski juhime tähelepanu ka KüTS § 13 alusel asutatud küberintsidentide registri põhimäärusele, milles sätestatakse tingimused ja asutused, kellega Riigi Infosüsteemi Amet (olulise mõjuga) küberintsidentidega seotud teavet vahetab. Eelnõuga muudetakse ka KüTS §-si 13 ning registri põhimäärust, et samade asutustega toimuks teabevahetus ka küberohtude ja turvahaavatavuste puhul (vt määruste kavandeid).
24.67	**Eelnõu § 1 p 56 – KüTS § 17[5]** Jääb arusaamatuks, miks eraettevõtete omavahelisi kokkuleppeid peab seaduses reguleerima - miks kirjutada seadusesse, et teenuse osutajad ja muud isikud võivad infot vahetada. Meil on lepinguvabadus. Riigi/KOV asutustel võib küll mingi akti tasemel olla antud õigus teavet vahetada, kuid kas seda reguleerida käesoleva eelnõuga? Infovahetamine sõltub ettevõttest ja tema riskide hindamisest, millist infot saab ja peab vahetama, millist mitte (konfidentsiaalne, ärisaladus, toimepidevuse vaatest kõrge riskitasemega info)	Selgitatud Tegemist ei ole ainult eraettevõtete vahelise teabevahetusega, vaid ka era- ja/või avaliku sektori vahel teabe vahetamisega, kes võivad olla samal ajal ka KüTSi kohaldamisalas. Kuna ka märkimisväärne osa teenuseosutajatest on avalikust sektorist, on nende puhul vajalik ka õiguslikku alust vastavate toimingute tegemiseks. Punkt 5: too säte on üle võetud NIS2 artikli 29 lõike 4 tõttu: *Liikmesriigid tagavad, et [üliolulised] ja olulised üksused teavitavad pädevaid asutusi oma osalemisest lõikes 2 osutatud küberturvalisuse alase teabevahetuse kokkulepetes, kui nad on selliste kokkulepetega ühinenud, või, kui see on asjakohane, kokkulepetest taganemisest pärast taganemise jõustumist.*

	Punkti 5 alusel tuleb lausa RIA-t teavitada teabevahetuse kokkuleppega ühinemisest või sellest taganemisest. Kui see oleks konkreetsete ettevõtete vahel, siis miks peaks sellest RIA-t teavitama?	
24.68	**Eelnõu § 1 p 56 – KüTS § 17[6]** Kas vastastikuse hindamise niivõrd detailne reguleerimine seaduse tasemel on vajalik? Lõike 4 osas - kas edasivolitamine on lubatav ja vajalik? Kui volitada siis saab seda teha minister. Seletuskirja lk 146 öeldakse, et pole otsustatud, kas Eesti soovib selles osaleda. Leiame, et võiks aru saada, kas on seda vaja või mitte. Variant oleks ka eelnõus sätestada, kes seda otsustab või kirjutada hetkel lühidalt, et vajadusel määratakse need siseriiklikult vastavalt NIS2 direktiivi artiklile 19 ja praegu jätta välja.	Osaliselt arvestatud ja selgitatud Algselt oli soov vastastikuse hindamise temaatika KüTSis ära reguleerida, kuid tagasiside analüüsimise käigus leiti, et kasulikum on tekitada põhilised sätted seaduse tasandile ning tekitada volitusnorm, mis täpsustaks vastastikuse hindamise detaile. Samas ei olnud võimalik seda teemat reguleerida nii, et KüTSis on ainult viide NIS2 direktiivi artiklile 19, kuna tegemist ei oleks direktiivi kohase üle võtmisega. Lõike 4 osas oli volitus mõeldud olukorraks, kus on vajadus delegeerida vastavas lõikes olevaid ülesandeid, näiteks Riigi Infosüsteemi Ametile. See on ka seletuskirjas kirjas. Uuendatud eelnõus on see temaatika viidud määruse kavandisse.
24.69	**Eelnõu § 1 p 60 – KüTS § 19 lg 4** Kui KüTS §-des 18^2 – 18^6 sätestatud väärtegude kohtuväline menetleja on RIA, siis kas § 19 lõikest 2 võib järeldada, et 18^2 ja 18^3 sätestatud väärtegu menetletakse ainult isikuandmete kaitse seaduse alusel (3 aastat aegumistähtaeg seal juba kirjas) või mõlema alusel ja kas trahvid ja aegumine käivad ühe või mõlema seaduse järgi?	Selgitatud Kui tegemist on isikuandmete töötlemisega seotud rikkumisega ning Andmekaitse Inspektsioon alustab tolles olukorras väärteomenetlust ja määrab ka väärteotrahvi, siis Riigi Infosüsteemi Amet sama teo eest väärteotrahvi ei saa määrata. Tegemist on topelt karistamise keelu põhimõttega (*ne bis in idem*). Kui mingil põhjusel otsustab Andmekaitse Inspektsioon, et ei alusta väärteomenetlust, siis on Riigi Infosüsteemi Ametil võimalus alustada väärteomenetlus KüTSis olevate väärteokoosseisude alusel. Siin topelt menetlemist ei toimu. Kui eelnõu KüTS §-des 18^2–18^5 sätestatud väärtegu on seotud isikuandmete töötlemise nõuete rikkumisega, toimub menetlemine Andmekaitse Inspektsiooni poolt nii, nagu tegemist oleks algusest peale olnud isikuandmete kaitse seaduse 6. peatükis oleva(te) väärteokoosseisu(de) (sõltuvalt konkreetsetest asjaoludest) menetlemisega. Kuna kehtivas isikuandmete kaitse seaduses on juba ette nähtud, et tolles seaduses ette nähtud väärtegude aegumistähtaeg on kolm aastat (vt tolle seaduse § 73 lg 1), siis on eelnõu puhul soov tekitada sama aegumistähtaeg ka KüTSi väärtegude korral (vt KüTS

		§ 19 lg 4 muutmist). Süüteo aegumine toimub mõlema seaduse väärteokoosseisude puhul ühtsetest alustest ehk karistusseadustikust.
24.70	**Eelnõu § 1 p 61 – KüTS § 20** Seletuskirjas palutakse tagasisidet, kas eelnõuga ette nähtud tähtajad on arusaadavad ning selged või tuleks nende sisu ja tingimusi muuta ehk et mis tähtajaks või millistest tingimustest lähtuvalt tuleks vastavad tähtajad kindlaks määrata. Jääb arusaamatuks, miks seotakse jõustumised erinevate sätete jõustumisega olukorras, kus kõik need sätted jõustuvad ühel kuupäeval ehk seaduse jõustumisel, vt eelnõu § 11.	SelgitatudEelnõu § 11 näeb ette seaduse üldise jõustumise reegli. KüTS §-ga 20 määratletakse ära esimene tähtaeg, mis ajaks seal viidatud KüTSi sättes olev ülesanne tuleb ära täita. Jah, need sätted jõustuvad praktikas ühel kuupäeval, kuid normitehniliselt ei ole võimalik KüTS § 20 lõigete sisu kehtestada stiilis „kui seadus jõustub, siis tuleb need toimingud ära teha“, kuna sel juhul oleks tähtaeg juba minevikus ehk tähtaja kulgemine hakkaks pihta KüTSi esmasest kehtestamisest ehk maist 2018. a.
24.71	Seletuskirja lk 3 kohaselt nähakse ette KÜTS-i jõustamiseks toetus uutele subjektidele EL taasterahastust (uusi subjekte on umbes 2000). Samas jääb ebaselgeks, kuna seletuskirjas ei ole välja toodud, kas rahastust võib laiendada ka alltöövõtjatele. Näiteks on palju ettevõtteid, mis peavad KüTS-i nõudeid järgima läbi KüTS-i kohuslasele teenuse osutamise. Selleks, et KüTS kohuslane ei peaks loobuma oma koostööpartnerist, kes peab vastama samadele tingimustele, siis teeme ettepaneku vastavat toetust ka neile laieneda läbi KüTS-i kohuslase taotluse. See kergendaks oluliselt ka KüTS-i kohuslaste olukorda ning ei tekiks üksustes olukorda, et üksused ei saa kasutada teatud teenuseid, kuna need ei ole seadusega vastavuses. Läbi selle toetaks riik erinevaid teenuse osutajaid ja ettevõtteid ning tagaks pakutavate teenuse turvalisuse.	Selgitatud Eesmärk on anda toetust ka teistele üksustele kui teenuseosutaja – vt eelnõu KüTS § 28^2.
25. Eesti Jõujaamade ja Kaugkütte Ühingu arvamus 31.01.2025 kiri nr 3		

25.1	Eelnõu § 1 punktis 1 tuuakse välja, et seadust kohaldatakse keskmistele ja suurtele ettevõtetele Euroopa Komisjoni soovituse 2003/361/EÜ järgi, kes tegutsevad eelnõus loetletud tegevusvaldkondades. Samas on eraldi välja toodud, et juhul kui tegemist on elutähtsa teenuse osutajaga, siis kohaldatakse üksuse suhtes kõiki nõudeid olenemata tema suurusest. Leevendusena on elutähtsate teenuste osutajatele ettenähtud 5 aastane üleminekuaeg. Teeme ettepaneku täpsustada seaduse sihtrühma ning eemaldada sealt näiteks kaugjahutuse pakkujad, sest meie hinnangul ei ole tegemist kaugkütteseadusega reguleeritud tegevusega ning samuti pole kaugjahutuse pakkumine täna elutähtsate teenuste loetelus. Pakutud sihtrühma laienemise osas tuleb muidugi üldiselt välja tuua, et küberturvalisuse seaduse subjektide nimekiri läheb liiga laiaks ning raskelt hallatavaks. Esiteks puudub lõplik kindlus, et millised ettevõtted ja asutused üldse seaduse regulatsiooni alla lähevad (juhul kui ei avaldata suletud nimekirja) või siis pole sellise hulga subjektide mahu juures realistlik nõuetekohase järelevalve teostamine. Sellest tulenevalt võib süveneda risk, kus selle asemel, et keskenduda kõige kriitilisematele ettevõtetele ja riskidele hakatakse hoopis plaani täitma. Tuleks leida võimalused nimekirja kokku tõmbamiseks ning samuti kaaluda erisusi ja lihtsustusi väiksematele ettevõtetele.	Selgitatud. Eelnõu autorid on subjektide ringi ja kohustuste osas viinud sisse või ette valmistanud mõningad riigisisesest õigusest tulenevad korrektuurid (eelkõige selleks et säilitada senise KüTS-i kohaldamisealasse juba hõlmatud subjektid), kuid valdavas osas tuleb lähtuda NIS2 direktiivis ettenähtud piiridest. Direktiivijärgsest (kohustuslikust) subjektide ringist ei ole võimalik erisusi luua. Kaugjahutuse pakkujad peavad NIS2 direktiivi I lisa punkti 1 (b) kohaselt kohaldamisalasse kuuluma ning meile teadaolevalt on selline teenus juba täna Eesti turul olemas, olgugi et seda ei ole eriseadusega reguleeritud. KüTSi teenuseosutajate ammendavat nimekirja ei avalikustata – vt siin eelnõus KüTS § 3^1 selgitusi.

25.2	Eelnõu näeb ette teenuse osutaja juhtorgani kohustuse läbida korrapäraselt erikoolitusi, mille õpiväljunditeks on piisavate teadmiste ja oskuste omandamine, et mõista küberturvalisuse riske jne. Samuti peab teenuse osutaja juhtorgan tagama, et töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi. Seletuskirjas on lk 82 välja toodud võimalikud õpiväljundid ning samuti on lk 83 viidatud, et võimaliku koolitusvälba osas oodatakse tagasisidet. Eelnevaga seoses palume kindlasti kriitiliselt üle vaadata ja täpsustada vajaliku küberkoolituse sisu ning õpiväljundid. Eelnõu seletuskirjas väljatoodud oskused tunduvat olevat juba sellisel tasemel erioskused, milleks üldjuhul värvatakse organisatsiooni vajaliku pädevusega valdkondlikud spetsialistid (teatud juhul isegi vajaliku kutsetunnistusega). Pole võimalik eeldada ja puudub ka vajadus, et asutuse juhtorgan omandaks lühikese koolituse järgselt näiteks järgmised erioskused: a) oskus töötada välja asjakohased meetmed küberriskide leevendamiseks, b) oskus juhtida küberkriiside lahendamist, c) oskus koostada ja testida küberintsidentide haldamisplaani jne. Samas on mõistetav, et asutuse juhil on vajalik omada kübervaldkonna riskidest piisavat ülevaadet. Võib eeldada, et vajalikest riskidest saadakse ülevaade esimesel võimalusel, mistõttu puudub vajadus teatud regulaarsuse kehtestamiseks. Samas kui võtta paralleel kutsesüsteemiga, siis seal toimub	Arvestatud Seletuskirjas on üle vaadatud võimalike õpiväljundite sisu. Vt ka Rahandusministeeriumi kommentaari 6.1 vastust.

	pädevuste taastõendamine üldjuhul iga 5 aasta järgselt. Lisaks teeme ettepaneku, et sellise ülevaatliku küberkoolituse võiks juhtorganile teha ka ettevõtte IT-juht või vastutav turbespetsialist. Vastava täpsustuse võiks seletuskirjas välja tuua, et vältida hilisemaid vaidlusi ning tõlgendusi.	
25.3	Juba varasemalt viitasime, et sellisele suurele hulgale subjektidele (ca 5500 organisatsiooni) riikliku järelevalve korraldamine pole usutavalt realistlik ning võib eeldada, et see muutub juhuse vms asjaolu põhiseks. Samas on eelnõus on märgitud, et riikliku ja haldusjärelevalvemenetluse käigus ettekirjutuse täitmata jätmise korral on asendustäitmise ja sunniraha seaduses sätestatud korras rakendatava sunniraha kohaldamise igakordne ülemmäär 7 000 000 eurot või kuni 1,4 protsenti teenuse osutaja omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. Eelnõu punktis 58 on välja toodud, et juriidilisest isikust olulist üksust karistatakse rahatrahviga kuni 7 000 000 eurot või kuni 1,4 protsenti olulise üksuse omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. Elutähtsa üksuse korral on rahatrahvi suurus kuni 10 000 000 eurot või kuni 2 protsenti elutähtsa üksuse omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem.	Mittearvestatud ja selgitarud Eesti õigus ei võimalda rikkumiste korral karistuste määramist haldustrahvi vormis, nii nagu näeb ette NIS2 direktiiv ja mitmed teisedki EL õigusaktid. Väärteomenetluses alusel määratavate rahatrahvide osas on vastavate ülemmäärade ülevõtmine riigile NIS2 direktiivi artikli 34 lõigete 4 ja 5 kohaselt kohustuslik. Seetõttu ei ole võimalik selle maksimaalmäärasid muuta nii nagu kommentaaris on soovitud. Sunniraha- ja trahvimäärade ühtlustamisel on lähtutud isikuandmete kaitse üldmäärusest ja isikuandmete kaitse seaduses sätestatud põhimõtetest, millega on Eesti õiguses kohaldamatu haldustrahvi kontseptsioon samuti väärteokoosseisude ja sunniraha määramise võimalusega üle võetud (seejuures kattuvate summadega). Siseriiklikult erisuste loomine analoogses olukorras ei oleks õiguslikult põhjendatud ega läbipaistev. Seejuures juhime tähelepanu, et sunniraha ülemmäär on madalam kui NIS2 direktiivi artikli 34 lõike 4 järgne trahvi ülemmäär. Eelnõus sätestatud sunniraha ülemmäära suurust on selgitatud seletuskirjas, sh on ka selgitatud, et sunniraha määramisel tuleb arvestada ka proportsionaalsuse põhimõtet. Tegemist on sunniraha maksimaalse ülemmääraga, mitte igal juhtumil määratava sunniraha suurusega.

	Juhime tähelepanu, et paljude Eesti elutähtsa teenuse osutajate jaoks on selliste summade tasumine võimatu. Sisuliselt tähendaks see ettevõtte ja teenuse osutaja pankrotti. Reguleeritud sektorites on tulukus reguleeritud ning mitmete ettevõtete aastakäive võib olla väiksem kui eelnõus väljatoodud 10 mln eurot. Sellest tulenevalt teeme ettepaneku muuta sunniraha ja trahvisummad realistlikumaks arvestades Eesti ettevõtete ja teenuseosutajate suurusi ning reguleeritud sektorite eripärasid. Samuti tuleb arvesse võtta esinenud riski ja rikkumise proportsionaalsuse põhimõtet.	
26. Eesti Kaubandus-Tööstuskoja arvamus 31.01.2025 kiri nr 4/15		
26.1	Üheks suurimaks muudatuseks, mis eelnõu endaga kaasa toob, on küberturvalisuse seaduse (edaspidi KüTS) subjektide nimekirja täiendamine (eelnõu § 1 p 1). Eelnõuga säilitatakse kehtiva KüTSi subjektid ning lisanduvad ennekõike need uued üksused, kes on ette nähtud NIS2 direktiivi kohaselt. Kaubanduskoda tunneb muret KüTS-i kohaldamisala on laiendatud oluliselt rohkem kui NIS2 direktiivi artikkel 2 nõuab. Eelnõu koostajad on hetkel valinud lähenemisviisi, mille tulemusel peavad ettevõtted, kelle üks teenus kuulub NIS2 direktiivis nimetatud sektoritesse, eelnõus sätestatud meetmed kohaldama kogu oma tegevusele, mitte üksnes NIS2 direktiivis nimetatud teenuste osutamisele. Selle tulemusel võib KüTS-i subjektideks langeda ettevõtted, kelle tegevusest väga väike osa moodustab selline tegevus, mis	Selgitatud Eelnõu tekst on üle vaadatud, et see ei hõlmaks rohkem üksusi KüTSi kohaldamisalasse kui NIS2 direktiiv ette näeb. Siin vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust. Samuti on eelnõud täiendatud sättega, mis sätestab, et KüTSis üksuse töötajate arvu, aastakäibe ja aastabilansi mahu kindlaksmääramisel ei arvestata partner- või sidusettevõtja andmeid Euroopa Komisjoni soovituse 2003/361/EÜ tähenduses, kui üksus on oma partner- või sidusettevõtjast teenuste osutamisel kasutatavate süsteemide osas sõltumatu. See asub eelnõu KüTS § 3 lg 7. Eelnõu kohaldamisala täiendav kitsendamine ei oleks NIS2 direktiiviga kooskõlas.

	muudaks ta KüTS-i subjektiks. Leiame, et selline laiendamine ei ole põhjendatud ning võib osadele ettevõtetele tuua kaasa ebavajalikult mahukad KüTS-i nõuded. Lisaks leiame, et sellise subjektide nimekirja laiendamise tulemusel võib ettevõtetel endal olla väga keeruline mõista ja hinnata, kas nad hakkavad olema KüTS-i subjektid ehk keeruline on tuvastada, millised ettevõtted on KüTS-i subjektid ja millised mitte. Eelnõu näeb KüTS-i subjektiks langemise suhtes ette teatud välistavad tingimused. Näiteks kohaldamisalast on välja jäetud mikro- ja väikeettevõtjad teatavate erisustega. Lisaks sätestab eelnõu, et eelnõu § 1 p 1 loetletud tegevusaladel tegutsevad ettevõtted on KüTS-i subjektid siis, kui ettevõttel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või aastakäive ületab 10 miljonit eurot. Arvestades neid nüansse, mis välistab teatud ettevõtete langemise KüTS-i subjektiks ning asjaolu, et eelnõuga on otsustatud KüTS-i kohaldamisala oluliselt rohkem laiendada kui NIS2 direktiiv ette näeb, siis on oluline ka vaadata praktilist poolt ja sõnastada eelnõu selliselt, et oleks välistatud see, et KüTS-i subjektideks langeksid ettevõtted, kelle tegevusest väga väike osa moodustab sellest tegevusest, mis muudaks ta KüTS-i subjektiks. Näiteks on eelnõu kohaselt KüTS-i subjektiks toidukäitlemisettevõtjad, kui ettevõttel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või	

	aastakäive ületab 10 miljonit eurot. Samas võib sellele tingimusele vastata ka ettevõte, kelle põhitegevusala ei ole toidukäitlemine ehk näiteks toidukäitlemine moodustab väga väikese osa ettevõtte tegevusest, aga sõltumata sellest muutuks ta KüTS-i subjektiks. Selle olukorra lahendamiseks oleks võimalik näiteks sätestada, et toidukäitlemisettevõtetest lähevad KüTS-I subjektide alla need ettevõtted, kelle töötajate arv on üle 50 ning aastakäive üle 10 miljoni euro ja kui nende põhitegevusalaks on toidu tööstuslik tootmine, toidu tööstuslik töötlemine või toidu hulgikaubandus ja nimetatud **tegevuste osutamisest saadav aastakäive ületab 50% ettevõte aastakäibest**. Selline lisatingimus aitaks KüTS-i skoobi alt välistada need ettevõtted, kelle tegevusest tegelikult suurem osa ei puuduta toiduainekäitlemist. Lisaks on oluline, et oleks tagatud see, et mikro- ja väikeettevõtted ei satuks KüTS-i subjektide hulka ka näiteks läbi kontserni kuulumise. Oluline on vältida seda, et mahukad ja suured KüTS-i nõuded hakkaksid kehtima nendele ettevõtetele, kellele need tegelikult kehtima ei peaks ja kes neid nõudeid ka võibolla täita ei suuda. **Eeltoodut arvestades on Kaubanduskoda seisukohal, et on väga oluline, et eelnõust tuleks lihtsalt ja selgelt välja see, kellele KüTS-i nõuded hakkavad kohalduma ehk kes on KüTS-i subjektid. Lisaks leiab Kaubanduskoda, et eelnõuga ei tohi laiendada NIS2 direktiivi kohaldamisala, sest selle tulemusel võivad väga**	

	paljud ettevõtted muutuda KüTS-i subjektiks isegi siis, kui nende tegevusest ainult väike osa on seotud sellise tegevusega, mis langeb KüTS-i kohaldamisalasse.	
26.2	Eelnõu § 1 p 1 all olev KüTS § 1^6 lubab Vabariigi Valitsuse määrusega lisada uusi KüTS-i subjekte. Kaubanduskoda ei toeta sellise sätte olemasolu eelnõus, kuna see ei taga võrdsust subjektide vahel. Kui enamus KüTS-i subjekte on määratud seaduse alusel ja samas on Vabariigi Valitsuse määrusega võimalik määrata ka uusi subjekte, siis ei ole see meie hinnangul asjakohane. Selliste ulatuslike kohustuste panemine peab toimuma ühtsetel alustel ehk seaduse alusel. **Kaubanduskoda palub eelnõust välja jätta § 1 p 1 all olev KüTS § 1^6, mille alusel on Vabariigi Valitsusel õigus määrusega lisada uusi sektoreid või valdkondi, kellele hakkaksid KüTS-i nõuded kohalduma.**	Arvestatud – vastav volitusnorm on välja jäetud.
26.3	Kaubanduskoda tunneb muret eelnõu mõjuanalüüsi suhtes, kuna see on puudulik. Eelnõu seletuskirja lk-l 11 on välja toodud, et "Üldistatult saab kokku võtta, et olemasolevaid subjekte on 3537 ning uusi subjekte on u 2000 ehk kokku on u 5500 subjekti, kellele küberturvalisuse seaduse nõuded hakkavad kohalduma. Nende arvude puhul tuleb arvestada ka asjaoluga, et ilmselt osad subjektid vastavad mitmele tunnusele: näiteks tegemist on elutähtsa teenuse osutajaga ning samal ajal ka üldkasutatava elektroonilise side võrgu pakkujaga; või tegemist on vee-ettevõtjaga, kes samal ajal tegutseb ka	Selgitatud Mõjude analüüs on üle vaadatud ja võimaluse korral täiendatud.

	reovee valdkonnas.” Lisaks on seletuskirja lk-l 129 täpsustatud, et “Samuti tuleb ka arvestada võimalusega, et esialgne analüüs subjektide arvu osas toetub poolikutele algandmetele või eeldustele, mistõttu on ka eespool märgitud, et eelnõu koostajatena ootame tagasisidet, kas esialgsed arvud on õiged või õiges suurusjärgus”. Nagu eelnõu seletuskirja tekstist nähtub, siis ei ole eelnõu koostajatele hetkel täielikult ikkagi selge, kui palju uusi subjekte hakkab olema ning kes tegelikult täpselt nende nõuete alla lähevad. Sama toodi välja ka 23.01.2025 toimunud Küberturvalisuse seminaril. Soovime rõhutada, et kui eelnõu väljatöötamisel on jäädud hätta sellega, et tuvastada subjektide ringi, kellele nõuded kohalduma hakkavad, siis on ilmselt ka ettevõtetel endil väga keeruline mõista, kas nad on KüTS-i subjektid või mitte. Muuhulgas on sellest tulenevalt ka keeruline ning pea võimatu hinnata eelnõu mõjusid, kui ei ole üheselt selge ja teada, kellele ning kui paljudele ettevõtetele hakkavad kohalduma KüTS-I nõuded. Lisaks ei ole näiteks eelnõu mõjuanalüüsis käsitletud seda, kui suured kulud kaasnevad nendele ettevõtetele, kes varasemalt ei olnud KüTS-i subjektid, kuid uute nõuete kohaselt on. Oluline on hinnata, kui suured kulutused uute nõuetega kaasnevad ning kas ettevõtted suudavad neid täita üleminekuperioodi jooksul. Kuigi eelnõu seletuskirja lk-l 3 on öeldud, et “Majanduslik mõju igale subjektile on väga erinev ning seda ei ole eelnõuga võimalik mõistlikult hinnata”, siis	

	Kaubanduskoda leiab, et nii suure mõjuga eelnõu osas on hädavajalik toestada majandusliku mõju analüüs, et näha kuidas ja kas ettevõtted suudavad KüTS-i nõuetega toime tulla ning kuidas nende nõuete täitmine hakkab ettevõtete tegevust üleüldiselt mõjutama. Seega, kuna mõjutatud isikute ring ja mõjud ise on suured, siis on hädavajalik, et eelnõu sisaldaks korralikku ja põhjendattud mõjuanalüüsi. **Kaubanduskoja hinnangul on oluline seletuskirjas olevat mõjuanalüüsi täiendada, et oleks võimalik praegusest paremini hinnata kaasnevaid mõjusid ettevõtetele ning näha, kui suutlikud on ettevõtted oma kohustusi täitma ning millised on uute kohustustega kaasnevad tagajärjed.**	
26.4	Eelnõu tutvustusüritusel tõi Justiits- ja Digiministeerium välja, et üleminekuaja KüTS-i nõuete rakendamisele uutele KüTS-i subjektidele on 3 aastat, kuid erisus on neile üksustele, kes said elutähtsa teenuste osutajateks pärast 18.10.2024. Sellisel juhul on üleminekuaeg 5 aastast. Samas toodi ka välja, et üleminekuaega ei ole nendele ettevõtetele, kes on juba praegu KüTS-i subjektid. Samas eelnõus endas rakendusaegasid täpselt sätestatud ei ole ning eelnõu § 11 ütleb, et kogu seadus jõustub 1. juulil 2025. **Kaubanduskoja hinnangul on oluline, et üleminekuajad nõuete rakendamise osas oleksid selgelt eelnõus sätestatud.**	Arvestatud – vt eelnõu KüTS §-e 4^1 ja 28^1 ning nende kohta eelnõu seletuskirjas antud selgitusi. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
26.5	Arvestades eelkirjutatud soovib Kaubanduskoda rõhutada, et oluline on tagada kõigile ettevõtetele	Arvestatud – vt eelnõu KüTS § 28^1. Vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.

	üleminekuaeg ehk ka neile, kes on juba praegu KüTS-i subjektid. Leiame, et üleminekuaeg peab olema tagatud ka olemasolevatele subjektidele, sest ka neile tuleb eelnõuga uusi kohustusi, mida nad varem täitma ei pidanud. **Kuna KüTS-i eelnõu toob kaasa muudatusi kõikidele subjektidele, siis on oluline tagada vähemalt 3 aastane rakendamisaeg kõikide subjektide suhtes.**	
27. Eesti Kaupmeeste Liidu arvamus 31.01.2025 e-kiri		
27.1	Teeme ettepanekud õigusselguse suurendamiseks, et oleks üheselt arusaadav, millised toidukäitlejad kuuluvad [NIS2] direktiivi skoopi ja millised mitte. Kuna Läti ja Leedu on [NIS2] direktiivi juba üle võtnud ning skoobi defineerinud, teeme ettepaneku, et Eesti kasutaks sarnast lähenemist, mis meie Baltikumi naabrid. [NIS2 direktiiv] piiritleb enda skoopi kuuluvad toidukäitlemisettevõtted järgnevalt: - Toidukäitlemisettevõtja (üldine mõiste) - avalik või eraõiguslik kasumit taotlev või kasumitaotluseta juriidiline isik, kes on seotud toidu ükskõik millisel tootmis-, töötlemis- või turustusetapil toimuva mis tahes tegevusega - [NIS2 direktiiv] laieneb toidukäitlemisettevõtjatele: a) kes tegelevad hulgimüügi, tööstusliku tootmise ja töötlemisega ning b) kelle puhul on täidetud järgmised tingimused:	Selgitatud. Eelnõu tekst on üle vaadatud, et see ei hõlmaks rohkem üksusi KüTSi kohaldamisalasse kui NIS2 direktiiv ette näeb. Siin vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 ning Eesti Kaubandus-Tööstuskoja kommentaari 26.1 vastust.

	• ta osutab teenuseid või tegutseb Euroopa Liidus; • tal on majandusaasta jooksul keskmisel 50 või rohkem töötajat; ja • tema aasta bilansimaht või aastakäive ületab 10 miljonit eurot. Leedu küberturvalisuse seaduses, millega on NIS2 üle võetud, loetletakse lisades 1 ja 2 sektorid, millele küberturbe nõuded laienevad. (sarnaselt direktiivile) Kaubandus on lisas 2 „teiste oluliste sektorite“ seas defineeritud selliselt: *Sektor: 4. Toidu tootmine, töötlemine ja kaubandus Skoobis olevad ettevõtted: 4.1.1. Toidukäitlemisettevõtted Artikli 3(2) tähenduses Euroopa Parlamendi ja Nõukogu regulatsioonis (EC) No 178/2002 28. jaanuarist 2002, mis sätestab toiduseaduse üldmõisted ja nõuded, loob Euroopa Toiduohutuse Ameti ning toidukäitlemise ohutusnõuded, kes tegelevad toidu hulgimüügiga, tööstusliku tootmise ja tööstusliku tootmisega.* Leedu küberturvalisuse seaduse artikkel 11 paragrahv 4, jagu 1 sätestab üldised nõuded muudele olulistele sektoritele, mis piirab seaduse kehtivuse vaid nendele toidukäitlemisettevõtetele, kes vastavad suuruse, põhitegevusala ja üle poole käibest toidu hulgimüügist tulemise kriteeriumitele. Teeme ettepaneku, et Eesti kasutaks analoogset piirangut, et: “**Nõuded kohalduvad üksnes ettevõtetele, kelle töötajate arv on üle 50 ning aastakäive üle 10 miljoni euro**	

	ja kui nende põhitegevusalaks on toidu tööstuslik tootmine, toidu tööstuslik töötlemine või toidu hulgikaubandus ja nimetatud tegevuste osutamisest saadav aastakäive ületab 90% ettevõte aastakäibest.[3]“ Selline definitsioon võimaldab piiritleda [NIS2 direktiivi] skoobi ettevõtetega, kelle põhitegevusala on toidu hulgikaubandus või selle tööstuslikes kogustes tootmine või töötlemine. Direktiivi alt jäävad välja sellisel juhul keskmise suurusega ja suuremad ettevõtted, kes muu tegevuse kõrvalt toovad ka maale mõningaid toiduaineid (näiteks ehituspoed, kelle sortimendis on ka toitu, alkoholi maaletoojad, kes toovad maale ka mõningaid maiustusi) või töötlevad väikestes kogustes toitu (näiteks kauplused, kus küpsetatakse grillkana või saiakesi). Samuti on direktiivi skoobist väljas toidu jaekaubandus, ühetaoliselt teiste EL liikmesriikidega. **Soovitame eelnõu seletuskirjas need asjaolud välja tuua ning välistatud tegevused kasvõi näidetena välja tuua, et vähendada hilisemaid vaidlusi ja kulusid nii riigile kui turuosalistele.** Skoopi jäävad keskmise suurusega ja suuremad toidu maaletoojad, kes tegutsevad sageli ka Läti ja Leedu turul ja on ka nendes riikides [NIS2 direktiivi] skoobis (näiteks puu-ja juurviljade maaletoojad, horeca sektori varustajad, kuivainete ja muu kauasäiliva kauba maaletoojad). Samuti	

[3] Leedu definitsioon: Article 11 Paragraph 4 section 1 of the Law: “the entity provides services and (or) carries out activities in the sectors specified in Annex 2 to this Law, exceeds the number of employees of small enterprises and the limits defining financial data set out in the Law on small and medium-sized business development, and the amount of annual income from the services and /or activities carried out by this entity specified in this paragraph exceeds 50 percent of the total annual income of the entity”.

	jäävad skoopi kõik peamised toidutööstused, kes Eestis toitu valmistavad.	
28. Eesti Perearstide Seltsi ja Eesti Esmatasandi Tervisekeskuste Liidu ühisarvamus 31.01.2025 kiri		
28.1	**Ebapiisav meetmete proportsionaalsuse ja subjektide ringi analüüs** Nõustume, et infoturve on perearstide töös oluline ning et perearstiabi teenuse osutajate (edaspidi **perearst**) suhtes peavad kehtima infoturbe nõuded. Sellised meetmed peavad aga olema proportsionaalsed ning põhinema valdkonna terviklikul analüüsil. Praegusel kujul eelnõus sisalduv lahendus ei vasta meie hinnangul kummalegi tingimusele ning võib kaasa tuua olukorra, kus osades piirkondades ei ole enam võimalik kodule lähedal perearsti poole pöörduda. Küberturvalisuse 2. direktiivi (edaspidi ka **NIS2**) läbimõtlematu ülevõtmine seab ohtu tervishoiuteenuse osutamise toimepidevuse, seades ühtlasi kahtluse alla ka riigi võime jätkuvalt täita talle põhiseaduse § 28 lg-st 1 tulenevaid kohustusi.	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.
28.2	**Diskretsiooniruum nõuete kehtestamisel ning sektori tervikliku analüüsi puudumine** Meie arusaamise kohaselt on KüTS-is sätestatud nõuete kõikide perearstide suhtes kohaldamine olnud siseriiklik valik ning ei NIS ega NIS2 direktiivist ei tulene kohustust kohaldada nõudeid selliste perearstikeskuste suhtes, mis ei ole elutähtsa teenuse osutajad (edaspidi **ETO**) ega keskmise suurusega (või suuremad) ettevõtjad. Eelnõu seletuskirjas on tervishoiu valdkonna osas märgitud, et NIS2 direktiivi soovitakse üle võtta	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

	võimalikult kitsalt. Seetõttu ei ole põhjenduste järgi arusaadav, mil põhjusel laiendatakse direktiivi ülevõtmisel siseriikliku valikuna regulatsiooni kohaldamisala isikutele, kes NIS ega NIS2 direktiivi reguleerimisalasse ei lange. Olenemata praegu ametis oleva justiits- ja digiministri Liisa-Ly Pakosta teravast kriitikast sellise õigusloome aadressil, kus direktiivide ülevõtmisel rakendatakse neid oluliselt laiemalt kui direktiiv ise nõuab, on püsib Eestis selline õigusloome halb praktika. Seletuskirja perearste puudutavas osas on viidatud kehtiva KüTS regulatsiooni säilitamisele ning teatud NIS2 artiklitele, kuid ei nähtu, et seejuures oleks (i) tervishoiusektorit tervikuna analüüsitud, (ii) hinnatud meetmete proportsionaalsust, (iii) arvestatud asjaoluga, et perearstid lisati algselt KüTS-i alles Riigikogu menetluses ilma piisava siseriikliku aruteluta (ja Sotsiaalministeeriumi valdkonnapõhistest ekspertteadmistel rajanevatest seisukohtadest hoolimata), ega (iv) arvestatud muutunud olukorraga (eelkõige perearstidest ETO-de võrgustiku loomine ning baasturbemeetmete kehtestamine). Seega on eelnõu vastuolus HÕNTE § 42 lg 1 punktidega 1-3 ning § 43 lg 1 punktidega 3 ja 5. Seletuskirjas ei ole selgitatud ning meile jääb arusaamatuks: 1. miks peetakse vajalikuks kohaldada nõudeid kõikide perearstide suhtes, kuigi NIS2 nõuaks kohaldamist üksnes kas vähemalt keskmise	

	suurusega ettevõtjate või ETO-deks olevate perearstide suhtes; 2. kas ja millistest kaalutlustest lähtuvalt vastab iga väike perearstikeskus NIS2 direktiivi artikli 2 lg 2 punktides b, c ja e (ehk KüTS § 1 lg 1^4 punktides 1, 2 ja 4) olevatele kriteeriumidele olukorras, kus üle riigi luuakse ETO-de võrgustik. Samuti, kuidas saadi sellele kriteeriumile vastavate üksuste arvuks 163 (Eestis tegutsevaid perearstikeskuseid on umbes 400, ETO-deks on kavas muuta neist ca 26-60); 3. mille poolest eristuvad perearstid kõigist teistest tervishoiuteenuste pakkujatest, kes samuti töötlevad eriliigilisi isikuandmeid ning on kohustatud edastama andmeid Tervise Infosüsteemi (v.a. haiglad, kes on ETO-d), ning miks ei kohaldata nende suhtes nõudeid isegi juhul, kui nad on sedavõrd suured, et kvalifitseeruvad vähemalt keskmise suurusega ettevõtjateks ja peaksid seega NIS2 üldreegli kohaselt olema regulatsiooni subjektiks (nt erakliinikud, eriarstiabi osutajad, hambaarstid, laborid jt diagnostikaasutused jne); 4. kas on hinnatud tervishoiu infosüsteeme tootvate ja haldavate ettevõtjate rolli sektoris ja nendega seotud riske, arvestades nende poolt töödeldavate eriliigiliste isikuandmete mahtusid, süsteemide toimimise olulisust ning asjaolu, et väikestel tervishoiuteenuste pakkujatel puuduvad sisulised võimalused nende tegevuse kontrollimiseks.	

	Ka Sotsiaalministeerium on eelnevate KüTS-iga seotud eelnõude menetlustes viidanud, et tervisoiusektorit tuleks analüüsida tervikuna, mida meie teada ei ole praeguseni tehtud. Süsteemse käsitluse ning riskide hindamise vajadust ilmestavad ka ülaltoodud küsimused. Rahvusvahelise koostöö gruppides avaldatakse teiste Euroopa Liidu liikmesriikide esindajate poolt suurt imestust, et Eestis kohaldatakse kõikide perearstide suhtes niivõrd ulatuslikke nõudeid ning ei ole teada teisi liikmesriike, kus sama tehtaks. Leiame, et infoturbe meetmed peaksid olema kehtestatud selliselt, et suur saab olla üks kahest – kas kohustuste ulatus või subjektide ring – mitte aga mõlemad korraga, nagu praeguses regulatsioonis. Meie arvates oleks mõistlik jätta ulatuslikud nõuded (nagu seda on E-ITS või ISO/IEC 27001 rakendamise kohustus) kohalduma üksnes kitsale subjektide ringile ning kehtestada näiteks määrusandluse teel (või muul moel) baastaseme nõuded sektoris mõnevõrra laiemalt, et vältida „kõik või mitte midagi“ olukorda. Seejuures peaksid nõuded olema riigi poolt tervishoiu jaoks võimaldatavaid ressursse arvestades proportsionaalsed ja realistlikud. Eeltoodust lähtuvalt teeme ettepaneku analüüsida tervishoiusektori subjektide ringi ja nende suhtes kohaldatavate nõuete ulatust tervikuna.	
28.3	**Nõuete proportsionaalsus ja mõju perearstiabi kättesaadavusele** Nagu öeldud, peavad ka perearstid infoturbe nõuete olemasolu vajalikuks, kuid need nõuded peaksid	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

	olema proportsionaalsed, arvestama valdkonna kui terviku vajadusi, tegevuse eripärasid ning subjektide väiksust. Need peavad toetama, mitte seadma ohtu ravi kättesaadavuse tasakaalustatud arengut käsikäes küberturvalisuse eesmärkide poole pürgimisega. Küberturvalisuse meetmete rakendamise legitiimseks eesmärgiks saab pidada küberintsidentide, vähendamist ja nende häiriva mõju vähendamist. Põhiseaduse § 11 kohaselt peavad sellist eesmärki taotlevad meetmed olema sobivad, vajalikud ja mõõdukad. Proportsionaalsuse põhimõtte rakendamisel on elementaarne, et mida suuremat ohtu või häiringut on vaadeldavast nähtusest võimalik tajuda, seda intensiivsemad meetmed on selle ärahoidmiseks sobilikud. Seisukoht ei saa olla erinev ka küberturvalisuse taotlemisel – mida suurem on andmeid töötlevast isikust lähtuv risk, seda intensiivsem on lubatav sekkumise määr. Paratamatult tähendab see vajadust hinnata riskiallikaid ning nende gruppe ja kohandada meetmeid lähtuvalt riskide realiseerumise tõenäosusest. Meie hinnangul aitaks lihtsamate, kitsamate ning tegevuse spetsiifikat arvestavate nõuete kehtestamine kaasa perearstide infoturbe taseme tõstmise eesmärgi saavutamisele, kuivõrd perearstid tuleksid arusaadavamate ja hoomatavamate nõuete rakendamisega paremini toime – seda iseäranis olukorras, kus enamik perearste peab nõuete rakendamisega ise hakkama	

	saama, kuna neil ei ole võimalik teenust väljastpoolt tellida. Sobivamate nõuete väljatöötamisse saab kaasata Riigi Infosüsteemi Ameti, kellega koostöös on varasemalt välja töötatud baasturbemeetmeid perearstidele, mis on Tervisekassa lepingute kaudu kohustuslikud kõigile perearstidele. Proportsionaalsemate nõuete kehtestamine ei avalda perearstide toimepidevusele ega infoturbe tasemele olulist negatiivset mõju, pigem on mõju hoopis positiivne. Lisaks ei ole meie hinnangul üksiku perearsti teenuse katkestusel olulist mõju perearstiabi toimepidevusele. Arvestades, et üle Eesti luuakse ETO-de võrgustik, ei ole üksiku perearstikeskuse teenuse ajutise katkestuse mõju suur. Lisaks säilib enamasti ka intsidentide korral esmase abi osutamise võimekus. Võimalike intsidentide mõju hindamisel tuleks arvestada ka seda, et perearstidel on kohustus edastada andmed Tervise Infosüsteemi, mis tähendab, et patsiendi terviseandmete ajaloo säilimine ei põhine üksnes perearsti infosüsteemil. Ebaproportsionaalsed nõuded seevastu on toonud kaasa olukorra, kus perearstide halduskoormus on hüppeliselt suurenenud ning lisandunud on kohustused, mille katmiseks ei ole ressursse ette nähtud. Perearstide tegevus põhineb peaaegu täielikult riiklikul rahastusel ning kehtestatud on ulatuslikud tegevuspiirangud, mis ei võimalda perearstidel muul moel oma sissetulekut suurendada. Samas ei ole aga kahe aasta jooksul leitud nõuete täitmiseks rahastust - kulumudelis on	

	küberturvalisuse jaoks ette nähtud ainult 49 eurot kuus ühe nimistu kohta. Ka tuleviku osas on perearstidele antud selge sõnum, et perearstide küberturvalisuse rahastuse suurendamine ei ole lähiajal võimalik, mis loob olukorra, kus KüTS-ist tulenevate ulatuslike nõuete rakendamine tuleb kliinilise raviressursi ning inimestele abiandmise võimekuse arvelt. Kehtiv standard on mõeldud eelkõige oluliselt suuremate ettevõtete jaoks ning selle rakendamiseks puudub perearstidel ühelt poolt kompetents ja teiselt poolt ressurss teenuse väljastpoolt tellimiseks. Ebaproportsionaalselt suur halduskoormus ning puudulik rahastus ohustavad perearstiabi kättesaadavust. Eestis valitseb juba praegu perearstide puudus ning tulemuseks võib olla, et paljudes piirkondades ei ole lõpuks võimalik kodule lähedal perearsti juurde pääseda, kuna perearstid loobuvad tööst. Meie hinnang ei ole paljasõnaline. Nagu ülal juba kord viitasime, märkis Sotsiaalministeerium küberturvalisuse seaduse eelnõud kooskõlastamata jättes oma 02.11.2017 kirjas nr 1.2-3/3754-3, et eelnõu toob kaasa täiendava kulu tervishoiuteenuste osutajatele, kelle valikukriteeriumid on jäetud selgitamata ja mis avaldab täiendavat survet Tervisekassa (2017.a Eesti Haigekassa) tervishoiuteenuste loetelule ning sellega seoses negatiivset mõju ravikindlustuse eelarvele. Kritiseeriti ka kergemeelset hinnangut, et küberturvalisuse meetmete rakendamisega kaasnev kulu on vähene ning et eelnõu ei näe ette täiendavaid rahalisi vahendeid tervishoiuteenuste	

	osutamisele. Sotsiaalministeeriumi hoiatused osutusid õigeks, need probleemid ei ole tänaseks muutunud ega leidnud lahendust. Halduskoormuse ja -kulu suurendamine ilma sellega toimetulekuks vajalike rahastusallikateta on seega kujunenud süsteemseks probleemiks, mis saab valimatu küberturvalisuse nõuete karmistamisega muutuda vaid halvemaks. Julgeme väita, et mõeldavate küberriskide realiseerumisest tingitud üksikute perearstide töö ajutised katkestused või häiringud on laiapindsele tervishoiuteenuste kättesaadavusele väiksem oht kui perearstide vabatahtlik või sunnitud loobumine tööst suurenenud halduskoormuse tõttu, sest viimasel juhul ei ole enam võimalik tagada ka esmase abi kättesaadavust. Eeltoodust tulenevalt teeme ettepaneku, et perearstid, kes pole ETO-d ega vähemalt keskmise suurusega ettevõtjad, tuleks KüTS kohaldamisalast välja jätta või kehtestada nende suhtes näiteks määrusandluse teel või muul moel proportsionaalsed nõuded. Arvestades, et perearstid on kohustatud järgima ka baasturbe meetmeid, ei tähendaks perearstide eelnõust väljajätmine nende jäämist ilma infoturbe nõueteta, ent võimaldaks sihitult, paindlikult ja proportsionaalselt rakendada küberturbe nõudeid vastavalt riskiastmele.	
28.4	**Auditikohutuse lävendi muutmine ja kohustuse täitmise tähtaeg** Tänane 10 töötaja kriteerium E-ITS auditi tellimiseks on ebaproportsionaalne nii finantskoormuse kui halduskoormuse osas ning	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

	selline kohustus ei ole jõukohane ei rahastusmudeli jätkusuutlikkuse ega perearsti teenuse pakkumise seisukohalt (auditi maksumus jääb eeldatavasti suurusjärku 10 000 – 30 000 eurot, audiitorite vähesuse tingimustes võivad aga hinnad olla veelgi suurenenud). 10 töötajat võib olla juba ka väga väikeses perearstikeskuses, kus osutatakse teenust 2-3 nimistule. Selliseid keskuseid on Eestis hinnanguliselt üle 200, st enamik Eesti perearstikeskustest. Lisaks, arvestades auditikohustuslaste hulka, ei ole Eestis tegutsevate audiitorite hulk kaugeltki piisav auditikohustuse tähtaegseks täitmiseks. Praegusel kujul kehtestatud auditeerimiskohustus on nõue, mille täitmine ei ole suure osa kohuslaste jaoks realistlik ega võimalik. Küberturvalisuse seaduse, avaliku teabe seaduse ja Eesti Rahvusringhäälingu seaduse muutmise seaduse eelnõu seletuskirjas on tõdetud, et auditeerimiskulud võivad majanduslikult koormavamad olla väikestele ettevõtetele ja majandusliku mõju tasakaalustamiseks võiks olla erand mikroettevõtetele, sealhulgas suurele osale tegutsevatele perearstidele (viidatud eelnõu esimese lugemise seletuskirja lk 35 "*Seega on majandusliku mõju tasakaalustamiseks auditikohustust kehtestava rakendusakti kavandis ettenähtud ka erand mikroettevõtjatele (nt suurele osa tegutsevatele perearstidele))"*. Praeguste reeglite alusel kohaldub auditi nõue aga siiski suurele hulgale perearstidest. Seega ei ole praegune auditikohustuse regulatsioon meie hinnangul kooskõlas seadusandja tahtega.	

	Teeme käesolevaga ettepaneku muuta E-ITS auditeerimise kohuslase lävendit selliselt, et see vastaks NIS2 direktiivi üldreeglile, st auditeerimiskohustust kohaldatakse üksnes ettevõtjate suhtes, kes on vähemalt keskmise suurusega ettevõtjad. Juhul, kui eeltoodud ettepanek ei ole vastuvõetav, palume kaaluda alternatiivina auditeerimise kohuslase lävendi viimist samale tasemele, mis on kehtestatud majandusaasta aruande auditeerimiskohustuseks audiitortegevuse seaduse § 91 lõikes 1 (kaks kriteeriumi vastavalt: tulu/müügitulu 4M€, varad 2M€, 50 töötajat). Märgime seejuures, et finantsaudititega kaasnev rahaline ja halduskoormus on oluliselt madalam spetsiifilisest E-ITS auditiga kaasnevast kulust. Juhul, kui auditikohustusega seotud siseriiklikeks aruteludeks kulub aega ning lävendi muutmise otsust ei tehta lähiajal, või kui lävendit otsustatakse mitte muuta, siis palume pikendada auditeerimiskohustuse täitmise tähtaega. Perearstide jaoks saabub tähtaeg käesoleva aasta lõpus.	
28.5	**Nõuded tervishoiu infosüsteeme tootvatele ja haldavatele ettevõtete** Viimaste aastate praktika kinnitab, et tervishoiu infosüsteeme tootvate ja haldavate ettevõtete intsidentide mõju on oluliselt suurem kui üksiku perearstikeskuse intsidendi mõju, seda nii perearstiabi toimepidevuse kui andmete tervikluse, kättesaadavuse kui konfidentsiaalsuse aspektist – peaaegu kogu Eesti perearstiabisüsteemi toimivus	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust. Lisaks selgitame, et kommentaaris mainitud ettevõtjatest osad võivad saada KüTSi teenuseosutajaks, kui nad on eelnõu kohaselt „haldusteenuse osutajad“ või „infoturbeteenuse osutajad“ ning nn suuruse kriteeriumid on täidetud.

	sõltub paari üksiku teenusepakkuja süsteemide tööst. Kohati kasutavad samade arendajate teenuseid ka haiglad vm tervishoiuasutused, mistõttu võib nendega seotud intsidentide mõju tervishoiusektorile olla iseäranis laialdane. Enamikus perearstikeskustes ei hoita enam andmeid kohapeal, vaid need on majutatud infosüsteemide tootjate/haldajate serveristesse. Kirjeldatud teenuspakkujad käitlevad ning säilitavad suures koguses patsientide terviseandmeid ning kuid nende tegevust kontrollivad üksnes klientideks olevad tervishoiuasutused, sealhulgas väikesed perearstikeskused, kellel puudub sisuline kompetents ja võimekus teenusepakkujate tegevuse piisavaks kontrollimiseks. Terviseinfosüsteemide arendajatele koostalitluse ning turvanõuete kehtestamist käsitletakse ka e-Tervise strateegias. Seetõttu peame oluliseks, et perearstide põhitegevuse seisukohast kõige olulisemate tervishoiu infosüsteemide tootjad ja haldajad oleksid iseseisvad KüTS subjektid ning et nende tegevust reguleeritaks tsentraalselt. Vähem kriitiliste teenuste (nt perearstide tarbeks loodud suhtlusplatvormide) puhul tuleks taaskord analüüsida valdkonna nõudeid ja vajadusi tervikuna. Kaaluda võiks selliste nõuete kehtestamist, mis on võrreldavad süsteemi kasutava tervishoiuteenuse osutaja enda suhtes kehtivate nõuetega. Kui seejuures piirab tervishoiu infosüsteemide tootjate või haldajate suhtes nõuete kehtestamist	

	oht, et teenused võivad nõuete tulemusel turult kaduda, siis see on selge märk sektorisse kavandatavate nõuete ebaproportsionaalsusest. Perearste ega teisi ettevõtjaid ei tohiks panna olukorda, kus nad peaksid lepingute kaudu nõudma teenusepakkujatelt selliste nõuete täitmist, mille osas on tekkinud kahtlus, kas teenus oleks nõuete õigusaktide tasandil kehtestamise korral kättesaadav. Teeme ettepaneku, et tervishoiu infosüsteeme tootvate ja haldavate ettevõtete suhtes kehtivad infoturbenõuded tuleks kehtestada tsentraalselt, tuginedes valdkonna terviklikule hindamisele. Sellisteks ettevõteteks on näiteks: • tervishoiuteenuse osutamiseks kasutatavad infosüsteemid - s.h. perearstide, haiglate, erakliinikute ning laborite infosüsteemid, Tervise Infosüsteemiga liidestatud andmebaasid jm; • digiregistratuurid tarkvarade juures (näiteks perearstide veebiregistratuur); • tervishoiuteenuse osutamisel kasutatavad suhtlusplatvormid, mille kaudu edastatakse konfidentsiaalset infot; • eeltoodud süsteemide majutusteenuse pakkujad.	
29. Eesti Proviisor Apteekide Liidu arvamus 31.01.2025 kiri		
29.1	Põhiliseks probleemiks on meie jaoks asjaolu, et kahjuks ei ole ammendaval määral arusaadavad ei eelnõust ega seletuskirjast tulenevad kohustused, rakendamise subjektid jne. Seetõttu vajaksid need dokumendid märksa rohkem lahti kirjutamist.	Võetud teadmiseks. Arvestatud osaliselt ja selgitatud. Eelnõu on pärast kooskõlastuselt saadud tagasiside analüüsi muudetud, sh on oluliselt muudetud ja lihtsustatud eelnõu KüTS §-e 1 ja 3. Eelnõu kohaldamisala reeglid on koondatud nüüd tervikuna KüTS §-i 3. Loodame, et selline lahendus on seaduse rakendajatele selgem ja paremini hoomatav.

	Teine probleemide ring seisneb selles, et me ei ole veendunud, et eelnõu on koostatud põhimõttel, et direktiivi ülevõtmine toimub minimaalselt vajalikul määral ning kohustatud subjekte kõige vähem koormaval viisil. Toome välja fakti, et eelnõu sisu ja selle tõlgendamise kohta on isegi eelnõu dokumentides enestes mitmeid küsimusi, mis alles vajavad vastuseid. Samasugune tõdemus kõlas eelnõu koostajateks olnud lektorite poolt ka 23.01.2025 toimunud eelnõu tutvustamise seminaril. Kindlasti oleks oluline saada vastused ka seminaril Slido süsteemi kaudu veebipõhiselt esitatud küsimustele. Eeldame seetõttu, et käesolevad eelnõu ja seletuskirja versioonid on alles esialgses valmidusastmes ja vajavad täiendamist. Kindlasti vajab täiendatud eelnõu versioon samuti kommenteerimise võimaluse andmist mõistliku etteteatamisega. Palume seetõttu käsitelda meie tagasisidet esialgsena.	Ministeerium kinnitab, et NIS2 direktiiv on üle võetud lähtudes nn minimaalsuse põhimõttest. See on küsimus, mida analüüsiti ja hinnati pärast kooskõlastamist veel täiendavalt ning pakuti, seal kus see vähegi direktiivi piirides võimalik oli, eelnõu subjektidele täiendavaid leevendusi. Näiteks võib välja tuua eelnõukohases KüTS § 3 lg 7 ette nähtud reegli, mille kohaselt ei arvestata üksuse töötajate arvu, aastakäibe ja aastabilansi mahu kindlaksmääramisel partner- või sidusettevõtja andmeid Euroopa Komisjoni soovituse 2003/361/EÜ tähenduses, kui üksus on oma partner- või sidusettevõtjast teenuste osutamisel kasutatavate süsteemide osas sõltumatu. Teise näitena võib välja tuua üksuse juhatuse liikme vastutuse, mis on eelnõu uue versiooni kohaselt üksnes tsiviilõiguslik (vt eelnõukohane KüTS 6^1; esialgses eelnõu versioonis KüTS §-s 18^4 ette nähtud karistusõigusliku vastutuse reegel on eelnõust välja jäetud) Eelnõu autorid selgitavad, et seletuskirja kooskõlastusele saadetud versioonis olid teadlikult tõstatud küsimused, millele eelnõu koostajad ootasid vastuseid. Eelnõule tagasiside saamine ongi selle kooskõlastamise üks peamistest eesmärkidest. Saadud vastused on läbi analüüsitud ja kasutatud sisendina eelnõu muutmisel.
29.2	Soovime selgitust eelnõusse/seletuskirja, kas liikmesriikidel on õigus (ja kui lai) seada täpsustavaid tingimusi NIS2 lisades I ja II nimetatud valdkondades tegutsevate üksuste määratlemisel KüTS kohaldamisalasse kuuluvaks või sellest välja jätmisel olukorras, kus üksus (juriidiline isik) tervikuna täidab küll numbriliste lävendite kriteeriumid, kuid üksuse tegevus NIS2 lisades nimetatud sektorites moodustab vaid osa (eriti juhul, kui väiksema osa) üksuse majandustegevusest ning üksnes selline tegevus eraldivõetuna mastaabi lävenditele ei vastaks.	Selgitatud Eelnõu tekst on üle vaadatud, et see ei hõlmaks rohkem üksusi KüTSi kohaldamisalasse kui NIS2 direktiiv ette näeb. Siin vt ka Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 ning Eesti Kaubandus-Tööstuskoja kommentaari 26.1 vastust.

	Eelnõu tutvustusel 23.1.2025 selgitasid eelnõu autorid, et riikide käsitlused on selle aspekti lahendamisel varieeruvad. Näiteks Läti puhul peab subjektiks saamiseks üle 50% üksuse tegevusest olema kriteeriumite kohaselt eelnõu skoobis. Kahtlemata pooldame sel juhul minimaalsuse printsiibi rakendamist ka Eestis ehk võimalikult vähe koormavaid regulatsioone. Samuti võimaldab direktiiv liikmesriikidele mingil määral diskretsiooni selle üle, kas kaasata mõni tegevusvaldkond KüTS kohaldamisalasse olenemata selles tegutseva üksuse numbrilistest mastaapidest. Seda lähenemist on eelnõus ka kasutatud näiteks perearstide puhul. Perearstide esindajatelt on kõlanud jõulist kriitikat, et kohustused on nende suhtes ebaproportsionaalsed ja ülejõukäivad – neil puuduvad majanduslikud võimalused kaasnevate, märkimisväärselt suurte kulude kandmiseks, kasvõi auditeerimiskohustuse näitel. 23.01.2025 seminaril kõlas lektorite poolt ka tõdemus, et tõepoolest tuleks üle mõelda proportsionaalsuse küsimused: väikeettevõtteid ei saa ülejõukäivate nõuetega pankrotti ajada. Apteegid väikeettevõtetena on samuti mures ülejõukäiva uue kohustuse suhtes.	
29.3	Pole arusaadav, kelle initsiatiivil ja millises menetluses toimub üksuste määratlemine KüTS kohaldamisalasse kuuluvaks. Eelnõu kohaselt määratleb teenuse osutajad RIA. Eelnõu näeb selleks ette tähtajad, kuid mitte menetluskorda. Mõnevõrra vastuoluliselt on samas teenuse osutajatel endil kohustus esitada RIA-le teave enda	Selgitatud Subjektsus sõltub kohaldamisala ja seaduses toodud teenuseosutaja tingimustele vastamisest, subjekte ei määrata ja vastavat menetluskorda ei looda. Riigi Infosüsteemi Amet koostab teenuseosutajate (üliohuliste üksuste ja olulise üksuste) ning domeeninime registreerimise teenuse osutajate loetelu, kuid ei tee seda paralleelselt teenuseosutajate endi teavitustega, vaid viimane on esimesele sisendiks.

	kui teenuse osutaja kohta. Kahtlemata tuleb sellised vastuolud ja mitmeti mõistetavused kõrvaldada.	Seda näeb ette ka NIS2 direktiivi art 3 lõige 4 *(„lõikes 3 osutatud loetelu koostamiseks nõuavad liikmesriigid...“*). Eeltoodust on lähtutud ka eelnõu KüTS § 3^1 koostamisel. Riigi Infosüsteemi Ametil on võimalik teha ka nõustamis- ja selgitustööd nende üksuste puhul, kes ei ole enda andmeid esitanud või kes kahtlevad, kas nad KüTSi subjektid.
29.4	Nagu selgitati seminaril: kaotatakse eristus oluliste teenuste operaatorite ja digitaalse teenuse osutajate vahel ning luuakse uute kategooriatena elutähtsad üksused ja olulised üksused. Eelnõus KüTS § 3: *(1^2) Elutähtis üksus on:* *10) üksus, kellel on majandusaasta jooksul keskmiselt 250 või rohkem töötajat ja kelle **aasta bilansimaht ületab 50 miljonit eurot** või **aastakäive ületab 43 miljonit eurot**, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ning kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1^2 punktides 1–51.* *(1^3) Oluline üksus on:* *10) üksus, kellel on majandusaasta jooksul keskmiselt rohkem kui 50 töötajat ja kelle **aasta bilansimaht on vahemikus 10–43 miljonit eurot** ning **aastakäive on vahemikus 10–50 miljonit eurot**, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ja kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1^2 punktides 1–51.* Meie küsimused: • Kas elutähtis üksus on elutähtsa teenuse osutaja (ETO) KüTSi tähenduses ka siis, kui ta on	Selgitatud esitatud küsimusi nende esitamise järjekorras: - Elutähtsate üksuste hulgas on mh ka hädaolukorra seaduse tähenduses olevad elutähtsa teenuse osutajad ning nende puhul ei ole ette nähtud, et nad peavad mainitud numbrilistele künnistele vastama - nad on KüTSi kohaldamisalas olenemata nende suurusest. See tuleneb NIS2 direktiivi art 2 lg-st 3 ja art 3 lg 1 punktist f. - Üldapteekide ja haruapteekide küsimuste osas: kui tegemist ei ole elutähtsa teenuse osutajaga, siis ta ei ole KüTSi kohaldamisalas, eeldusel, et tema muud tegevused ei ole ka KüTSi kohaldamisalas. - Tervisele infosüsteemile juurdepääsu teemal - eeldame, et küsimuse taust on seotud sellega, et kas tegemist on riikliku andmekogu volitatud töötlemisega. Tol teemal palume vaadata andmekogu volitatud töötleja selgitust, milles selgitatakse, et tegemist on volitatud töötlejaga avaliku teabe seaduse tähenduses, mitte isikuandmete kaitse valdkonnas oleva volitatud töötlejaga (sh ka mitte andmeandjana).

	seda Hädaolukorra seaduse tähenduses, aga ei vasta KütSi numbrilistele künnistele? • Kas KüTSi numbrilistele künnistele mittevastav üldapteek (või ka haruapteek) on eelnõu tähenduses subjektiks: juhul kui ta ei ole Hädaolukorra seaduse alusel määratud ETOks? - juhul kui ta on Hädaolukorra seaduse alusel määratud ETOks? - juhul kui tulevikus hakatakse apteegis osutama lisaks apteegiteenusele näiteks ka mõningaid tervishoiuteenuseid või ennetusteenuseid vmt ja nende teenuste tarvis saab apteek juurdepääsu Tervise infosüsteemile, sh patsientide tervise andemetele? - Juhul kui apteekritele antakse apteegiteenuse osutamiseks kas osaliselt või täielikult juurdepääs Tervise infosüsteemile, sh patsientide tervise andemetele?	
29.5	23.01.2025 seminaril selgitati, et • Justiits- ja digiministeeriumis on ettevalmistamisel toetusmeede (küberturvalisuse taseme kaardistamine ja arendamine) – voorud ca 2,3 mEUR aastas, lisainfo kevad 2025. • Ettevõtluse ja Innovatsiooni Sihtasutuse muud toetused: nt Digipöörde toetus ettevõtetele https://eis.ee/toetused/digipoorde-toetus/ • EL rahastamisprogrammid https://ria.ee/kuberturvalisus/riiklik-koordinatsioonikeskus-ncc-ee/rahastusvoimalused	Selgitatud. Eesmärk on anda toetust ka teistele üksustele kui teenuseosutaja – vt eelnõu KüTS § 28^2.

	Kahtlemata vajavad ettevõtjad (eriti väiksemad) kindlust, et avalik sektor tuleb neile appi vajalike investeeringute tegemiseks ja ülejõukäivate kulude katmiseks. Selles osas palume jagada konkreetset ja sisukat informatsiooni nii kiiresti kui võimalik. Soovime ka kindlust, et need meetmed on rakendatavad eraettevõtetele.	
29.6	HOS § 38 lõike 1^3 punkt 3 kohaselt on elutähtsa teenuse osutajale KüTS kohustuste täitmiseks **kuni 5-aastane** maksimaalne tähtaeg, mille üle otsustab isiku elutähtsa teenuse osutajaks määrav haldusorgan. Seega võib kohustuste algus osutuda lühemaks, kui seletuskirjas lubatud 5 aastat. Kahjuks pole aga arusaadav, mis alustel ja kaalutlustel täpne tähtaeg määratakse. Ettevõtjad vajavad ranget selgust, et üleminekuajad ja neid selgitavad sätted oleks eelnõus üheselt välja toodud ega sõltuks ametkondade suvast.	Selgitatud Esitatud kommentaar ei ole seotud siinse eelnõuga, vaid see on reguleeritud hädaolukorra seaduses. Täpsemalt on seda aspekti selgitatud Riigikogus arutlusel olnud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse 426 SE seletuskirjas, konkreetsemalt tolle eelnõu § 1 punktis 14.
29.7	Kuna eelnõuga seoses on palju ebaselget ja vastuolulist, teeme ettepaneku korraldada enne uue eelnõu versiooni koostamist veel üks ümarlaud huvirühmade ärakuulamiseks ja selgituste andmiseks.	Võetud teadmiseks
30. Eesti Põllumajandus-Kaubanduskoja arvamus 31.01.2025 kiri nr 10/1-4		
30.1	NIS2 direktiivi ülevõtmise peamine eesmärk on tugevdada ettevõtjate küberturvalisuse süsteeme, hinnata turvariske ja tagada, et nende tegevus ei ohusta mitte ainult ettevõtte enda, vaid ka tarbijate ja teiste ettevõtete ja tarneahela osaliste turvalisust. See on kindlasti oluline, arvestades, et küberintsidendid on toimunud viimastel aastatel ka	Selgitatud Eesti infoturbestandardi auditeerimise teemal vt Sotsiaalministeeriumi kommentaari 9.1 vastust. Riik on tegutsenud aastaid Eesti infoturbestandardi teemaliste koolituste, nõustamiste ja õppuste korraldamisega, mistõttu kommentaaris esitatud väide ei vasta tõele. Eelduslikult on teadmatus olnud seotud sellega, et seni ei ole põllumajandus ja toidutoomisega seotud ettevõtjad olnud KüTSi nõuete järgijad või näiteks ettevõtjad ei

	põllumajanduse ja toidutootmisega tegelevates ettevõtetes. Toidutootjad, kes sõltuvad suurtesti IT-süsteemidest, automatiseeritud tootmisprotsessidest või laiaulatuslikest andmevahetustest, peavad uutele nõuetele vastavalt pöörama senisest rohkem tähelepanu küberturvalisusele ja selle tagamisele, mis toob kaasa ka senisest märkimisväärselt suuremaid kulusid. **Meie peamine mure on KüTS-i E-ITS infoturbestandardi rakendamise kohustus, mis sisaldab nõuet auditeerida riske audiitorkontrolliga ja vajadusel teha suuremahulisi ja kulukaid muudatusi protsessides.** Meile on jätkuvalt arusaamatu, milline on riski ulatus või reaalne oht riigile, kui toidusektori ettevõtjad igaüks eraldiseisvana ei rakenda küberturvalisuse seadust nõutud mahus? Tuleb märkida, et toidutootmine on enamasti mehhaniseeritud ja suures osas digitaliseeritud, kuid seadmeid saab vajadusel manuaalselt käivitada ja protsesside etappe teostada käsitsi. Seetõttu jääb arusaamatuks, miks toiduvaldkonnas tegutsev ettevõte peab kasutama just ettenähtud E-ITS-i ja ei saa ise valida sobivaid meetodeid küberturvalisuse riskidega tegelemiseks. KüTS-i määratud riskide maandamine peab olema osa ettevõtte riskianalüüsist, kus küberturvalisuse riske ja ohte hindab elutähtsa teenuse osutajast ettevõtte juht kaalutletult, võttes vastu vastavad meetmed nende maandamiseks. Eelnõu väljatöötamisel ei ole analüüsitud, kui suures ulatuses tootjad peavad oma	ole huvi tundnud küberturvalisuse vastu, mistõttu ei ole nendeni jõudnud vastav teave. Eesti infoturbestandardi rakendamise kohta on vastav info leitav vastavast portaalist (vt nt koolitusi: https://eits.ria.ee/et/avalehe-menueue/suendmused) ning Digiriigi Akadeemias on ka olemas teatavad tasuta e-kursused (https://digiriigiakadeemia.ee/, kui valida märksõna „küberturvalisus“). Eesti infoturbestandardi auditeerimistsükli osas vt Rahandusministeeriumi 6.5 kommentaari vastust.

	protsesse täiendama ega ole arvestatud E-ITS-i rakendamisega kaasnevat lisainvesteeringute vajadust. Me ei saanud 23. jaanuaril toimunud küberturvalisuse seaduse (NIS2) seminaril kinnitust, et riigil on olemas vajalik oskustugi ettevõtjatele, et aidata küberturvalisuse nõudeid täita nende tootmisspetsiifikast lähtuvalt. Küberturvalisuse seadusest tulenevad kohustused ei saa aga olla ainult ettevõtjate ülesanne. Ettevõtete küberturvalisusega seotud probleemide lahendamiseks tuleb ette näha üleriigilisi õppusi ja ettevõtjapõhiseid koolitusi. Just õppused aitavad tõhusamalt tuvastada probleemkohad nii ettevõtetes, sektoriüleselt kui ka riigi tasandil, olles tõhusam lahendus kui iga seaduse subjekti eraldi auditeerida. Meie arvates ei ole audiitorkontrollide vajadust ja sellega kaasnevat kulu ettevõtjatele piisavalt hinnatud. NIS2 direktiivi rakendamisest tulenev audiitorkontrolli hind sõltub mitmest tegurist nagu ettevõtte suurusest ja tehnoloogiliste protsesside keerukusest. Suuremad ettevõtted, millel on keerukamad IT-süsteemid ja rohkem töötajaid, vajavad tõenäoliselt põhjalikku ja aeganõudvat auditeerimist. Kuna enamik ettevõtteid peab auditi tegema esmakordselt, võib protsess võtta rohkem aega. Kui ettevõtte küberturvalisuse süsteemid vajavad täiendamist, võib see muuta audiitorkontrolli kallimaks. Väiksemate ettevõtete puhul võib audiitorkontrolli hind ulatuda 3000–5000 euroni, kuid suuremate ettevõtete puhul, kus	

	süsteeme rohkem, võib hind ulatuda 15 000–50 000 euroni või enamgi. Lisaks käesoleva eelnõu rakendamisele tahame muuhulgas pöörata tähelepanu, et viimastel aastatel on erinevate eelnõudega lisandunud teisigi audiitorkontrolli nõudeid, nt ESG aruandlus, kuid nende kumulatiivset mõju ja kulu ettevõtjatele ei ole hinnatud. Meie hinnangul võib auditeerimist kui ühte meedet kaaluda juhul, kui teisi võimalusi turvalisuse tagamiseks ei ole ning kui see siiski vajalikuks osutub, on mõistlik teha auditeerimist aeg-ajalt, näiteks iga 3 või 5 aasta järel, mitte pidevalt.	
30.2	EPKK on alati seisnud selle eest, et Eesti põllumajandus- ja toidusektoril oleks strateegiline roll toidujulgeoleku tagamisel. Toidusektor kui üks elutähtsate teenuste osutaja, lisati hädaolukorra seadusesse viimase redaktsiooniga, andes sektorile üleminekuaja seadusest tulenevate kohustuste täitmiseks. 23. jaanuaril toimunud küberturvalisuse seaduse (NIS2) muutmise tutvustusseminaril kinnitati, et ka sellele seadusele kehtib toidusektorile üleminekuperiood. Me loodame, et lubatud ülemineku aeg kehtestatakse seaduse tasandil.	Arvestatud ja selgitatud Elutähtsa teenuse osutaja puhul on vastav tähtaeg ette nähtud juba hädaolukorra seaduses (vt tolle seaduse § 38 lg 1^3 punkti 3), kuid ka siinse eelnõuga täpsustatakse KüTSiga seotud üleminekuaegasid. Vastavad sätted on eelnõu KüTS §-des 4^1 ja 28^1. Vt ka nende sätete kohta seletuskirjas antud selgitusi. Loodame, et selline ülemineku regulatsioon võimaldab ka põllumajandussektoris KüTS-i uued nõuded sujuvalt rakendada.
31. Eesti Ravimihulgimüüjate Liidu arvamus 31.01.2025 kiri		
31.1	Meie hinnangul vajavad eelnõu ja seletuskiri mitmetes küsimustes oluliselt suuremat selgust ning vajadusel ka asjakohaselt täiendamist. Ka eelnõu autorid ise esitavad eelnõu teksti ja selle tõlgendamise kohta seletuskirjas alles küsimusi.	Võetud teadmiseks. Eelnõu ja seletuskirja on pärast kooskõlastamist saadud tagasiside alusel muudetud ja täiendatud. Näiteks on oluliselt muutunud KüTS §-des 1 ja 3 sätestatu, mis muudab loodetavasti eelnõu kohaldamisala seaduse rakendajale selgemaks ja paremini hoomatavaks. Loodame, et muudetud eelnõu toob ka teile soovitud selgust.

	Nõustume autoritega, et seda tüüpi aspektid vajavad selgeid vastuseid, milleta on keeruline või võimatu eelnõud lõpuni mõista. Tunnustame ministeeriumit sisulise kaasamise ja avatud arutelu algatamise üle. Samas tähendab see, et faktiliselt on eelnõu veel koostamise faasis ning arvamuse avaldamiseks saadetud tekst alles esimene versioon tulevastest, mitte juba valitsuse ja Riigikogu järgmistesse menetlusetappidesse saatmiseks valmis lõpptekst. Loodetavasti saadab ministeerium eelnõu viimase variandi huvirühmadele tutvumiseks ja vajadusel arvamust avaldamiseks uuesti ka selle lõplikul valmiskujul.	
31.2	**Selget vastust vajab küsimus sellest, kas ja kui, siis mil määral, on riikidel õigus seada täpsustavaid lävendeid NIS2 lisades I ja II nimetatud sektorites-allsektorites tegutsevate üksuste määratlemisel KüTS kohaldamisalasse kuuluvaks või sellest välja jätmiseks? Nende määratlemine ning maksimaalselt ära kasutamine peaks olema eelnõu koostamise üheks aluseks.** Näiteks muuhulgas, kuid mitte ainult, olukorras, kus - üksus (juriidiline isik) tervikuna täidab küll KüTS kohaldamisala suuruse kriteeriumid, - kuid tema tegevus NIS2 lisades nimetatud sektorites moodustab vaid osa üksuse kogu majandustegevusest - ning üksnes selline tegevus eraldivõetuna kohaldamisala suuruse kriteeriumit ära ei täidaks.	Vt Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.

	Eelnõu tutvustusel 23.1.2025 selgitasid eelnõu autorid, et riikide käsitlused selle aspekti lahendamisel varieeruvad (Läti näide). Ka meile teadaolevalt on Lätis sätestatud erinormid keskmise suurusega teenuse osutajatele, kes kuuluvad küberturvalisuse seaduse kohaldamisalasse vaid juhul, kui küberturvalisuse kontekstis tähendust omav tegevusala kuulub ettevõtte peamiste tegevusalade hulka. Peame seesugust täiendavat piiritlust mõistlikuks ning paluma ka KüTS eelnõus kaaluda tegevusalade osas erisuse sätestamist, mis hõlmaks KüTS kohaldamisalasse ainult need ettevõtted, kelle peamiseks tegevusalaks on KüTS mõistes elutähtsate või oluliste teenuste osutamine. Kindlasti tuleks seesuguseid erisusi arvestada tervishoiu- ja kemikaalivaldkonna tootmis- ja levitamistegevuste puhul. Lisaks võimaldab ka NIS2 direktiiv ise liikmesriikidele teatud ulatuses kaalutlust selle üle, kas näiteks hõlmata mõni sektor KüTS kohaldamisalasse olenemata selles tegutseva üksuse suurusest. Seda diskretsiooni on eelnõus ka kasutatud tervishoiuteenuse osutajate puhul – hõlmates kohaldamisalasse perearstid, kuid jättes sellest välja teised tervishoiuteenuse osutajad (N. hambaarstid, kliinilised psühholoogid, teised eriarstiabi osutajad jm). Eelnõu mõistmiseks ja edasiseks menetluseks on kriitiline jõuda selge arusaamani nende lävendite täpsest piirist ja siseriiklikust kaalutlusvabadusest	

	nende piiride seadmisel. Arvestades eelnõu ulatuslikku mõju ettevõtetele tuleks NIS2 ülevõtmisel piirduda direktiivis minimaalselt nõutuga ning maksimaalselt kasutada siseriiklikusse pädevusse jäetud võimalusi KüTS kohaldamisala piiramisel.	
31.3	**Selget vastust vajab ka küsimus sellest, kuidas, kelle initsiatiivil ja mis menetluses toimub üksuste määratlemine KüTS kohaldamisalasse kuuluvaks. Eelnõu kohaselt „tuvastab" teenuse osutajad RIA. Eelnõu näeb selleks ette tähtajad, kuid mitte menetluskorda.** Teisalt on teenuse osutajatel kohustus esitada RIA-le teave enda kui teenuse osutaja kohta, ennast teenuse osutajana RIA juures „registreerida". Samuti tuleb teavitada asjakohastest muutustest. Selgitamist vajab nende tegevuste ja kohustuste omavaheline koosmõju, tegevuste järjekord ja õiguslik tähendus. Vajadusel tuleks kaaluda RIA poolt teenuse osutajate „tuvastamise" menetluse täpsemat regulatsiooni.	Vt Eesti Proviisor Apteekide Liidu kommentaari 29.3 vastust.
31.4	**Täiendav küsimus meditsiiniseadmete tootjate näitel tekib eelnõu KüTS § 1 lg 1^2 p-de 31 ja 46 koosmõjust, mis tõstatab taaskord eelkirjeldatud laiema küsimuse KüTS kohaldamisalast ning siseriiklikust kaalutlusest sektorite-allsektorite võimalikul täiendaval piiritlemisel.** Esimene viidatud punktidest käsitleb rahvatervise hädaolukorras esmatähtsate meditsiiniseadmete loetellu kuuluvate seadmete tootjaid – teine seevastu kõigi meditsiiniseadmete kõiki tootjaid.	Selgitatud NIS2 direktiiv on neid üksusi sel moel neid eristanud, mistõttu on ka eelnõus soovitud neid eristada, kuna tegemist on üksustega, mis on NIS2 direktiivi erinevates lisades. Seeläbi on olnud direktiivi puhul soov eristada, kas ja milliseid nõudeid konkreetne üksus peab järgima, st kas tegemist võib olla üliolulise üksusega või olulise üksusega. NIS2 direktiivi enda loogika on selline, et kommentaaris viidatud p-s 31 toodu kvalifitseerub ülioluliseks üksuseks (spetsiifilised meditsiiniseadmed) ja p-s 46 toodu oluliseks üksuseks.

	Sätteid kõrvutades saaks väita, et teine kategooria hõlmab alati täies ulatuses ka esimese. Ometi on need direktiivis ja eelnõus sätestatud eraldi sektorite-allsektoritena, st õiguslikus mõttes tehakse neil vahet. Vastavate kohustuste suurt ulatust arvestades on ilmselge, et üleöö ükski üksus enda nõuetelevastavust tekitada ei saa. Arvestades eelnõus teenuse osutajate kohustuste rikkumise puhuks sätestatud haldussunni ja karistusmeetmete rangust, tuleb neile küsimustele anda eelnõu dokumentides ka selge vastus.	
31.5	**Eelnõu selgitustes oleks kasu ka KüTS kohaldamisala reeglite põhjalikumast avamisest ühte kontserni kuuluvate ettevõtete näitel.** Näiteks olukorras, kus kontserni moodustavad emaettevõte A ja kolm tütarettevõtet B, C ja D, kellest: - emaettevõte A ühtegi KüTS-is nimetatud teenust ei osuta ning oleks eraldiseisva juriidilise isikuna EK juhises toodud kriteeriumite kohaselt väikeettevõte ning seega kõigi kriteeriumite lõikes KüTS kohaldamisalast väljas; - tütarettevõte B on elutähtsa teenuse osutaja HOS ja KüTS tähenduses ja seega sõltumata oma suurusest elutähtis üksus KüTS tähenduses; - tütarettevõte C osutab üht või mitut KüTS § 1 lg-s 1^2 nimetatud teenust ning lisaks ka KüTS kohaldamisalast välja jäävaid teenuseid, millest ükski eraldivõetuna ei täidaks KüTS suuruse kriteeriumit, kuid C kui jur.isiku majandustegevus tervikuna ületab nii töötajate arvu kui käibe alusel	Selgitatud - Ettevõte A: ei ole KüTSi subjekt - Ettevõte B: on KüTSi subjekt, sh tegemist on eelnõu uue sõnastuse kohaselt üliolulise üksusega (varasemalt elutähtis üksus). - Ettevõte C: on KüTSi subjekt ja sõltuvalt konkreetsest tegevusvaldkonnast kas üliolulise üksus või oluline üksus. Lisaks C kui juriidilise isiku enda finants- ja tööjõunäitajatele (mille kohaselt toodud näites mahuks ta niikuinii keskmise suurusega ettevõtja määratluse alla) tuleb arvestada ka tema partner- ja sidusettevõtjate ehk mh teiste kontserni liikmete finants- ja tööjõunäitajatega (partnerettevõtete puhul proportsionaalselt, sidusettevõtete puhul täielikult), v.a juhul kui C võrgu- ja infosüsteemid KüTS-s nimetatud teenuse osutamisel on partner- ja sidusettevõtjatest sõltumatud (eraldiseisev IT). - Ettevõte D: selle puhul tuleb arvestada ka tema partner- ja sidusettevõtjate ehk mh teiste kontserni liikmete finants- ja tööjõunäitajatega, v.a juhul kui D võrgu- ja infosüsteemid KüTS-s nimetatud teenuse osutamisel on partner- ja sidusettevõtjatest sõltumatud (eraldiseisev IT). See tähendab, et sõltuvalt D tegevusest ja sõltuvusest partner- ja sidusettevõtjate IT-st võib ta olla nii elutähtis kui ka oluline üksus. Ettevõtete C ja D vastustega seonduvalt selgitame, et eelnõud on täiendatud sättega, mis sätestab, et KüTSis üksuse töötajate arvu, aastakäibe ja aastabilansi mahu

	KüTS lävendid ning võib nende alusel mahtuda olulise üksuse kategooriasse; - tütarettevõte D osutab samuti üht KüTS § 1 lg-s 1^2 nimetatud teenustest, kuid tema kui jur.isiku majandustegevus ei täida KüTS töötajate arvu ega käibe lävendit ja tegemist on mikroettevõttega; siis missugused eelnimetatud juriidilistest isikutest A, B, C ja D oleks „teenuse osutajaks“ KüTS tähenduses ning kas nad liigituks elutähtsaks või oluliseks üksuseks?	kindlaksmääramisel ei arvestata partner- või sidusettevõtja andmeid Euroopa Komisjoni soovituse 2003/361/EÜ tähenduses, kui üksus on oma partner- või sidusettevõtjast teenuste osutamisel kasutatavate süsteemide osas sõltumatu. See asub eelnõu KüTS § 3 lõikes 7. Vt selle kohta vastavaid selgitusi eelnõu seletuskirjas.
31.6	**Eelnõus tuleks täpsemalt ja direktiivile vastavalt ka kitsamalt piiritleda teenuse osutaja kohustus „tagada süsteemi tarneahela turvalisus“.** Erinevalt eelnõus pakutud KüTS § 7 lg [2] p 6 sõnastusega rõhutab ja toob NIS2 direktiiv tarneahela turvalisuse osas ennekõike esile üksuse ja tema otseste tarnijate või teenuseosutajate vahelised suhted. Seega on direktiivi põhirõhk suunatud just eelnimetatud kitsamalt piiritletud suhetele, mitte sama sügavus- ja rõhuasetusega kogu tarneahelale. Sama põhimõte peaks selgelt väljenduma ka eelnõus.	Selgitatud Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid).
31.7	**Vastusena eelnõu autorite küsimusele toidu „hulgimüügi“ mõiste kohta leiame, et selle taandamine/piiritlemine üksnes lähtuvalt „tarbija“ kui tarbijakaitseseaduse tähenduses füüsilise isiku mõiste kaudu võib jääda liiga kitsaks.** Ka NIS2 direktiivi lisas II viidatud toidumääruse 178/2002 „jaemüügi“ definitsioon ei paista jaemüüki piiritlevat kitsalt ja ainult müügina füüsilistele isikutele, vaid kui müüki	Vt Regionaal- ja Põllumajandusministeeriumi kommentaari 7.4 vastust.

	„lõpptarbijale“ *(„final consumer“)* ehk isikutele „kes ei kasuta toitu toidukäitlemistoimingus või sellega seotud tegevuses“ *(„the ultimate consumer of a foodstuff who will not use the food as part of any food business operation or activity“)*.	
31.8	**Soovitame täpsustada kas KüTS § 3 lg 1^2 p-s 10 ja § 3 lg 1^3 p-s 10 sätestatud bilansimahu ja aastakäibe kriteeriumid on omavahel vastavuses või tekib sätete vahel kattuvusi-lünki – seda nii bilansimahu ja käibe summaliste väärtuste võrdluses kui sidesõnade „või“/“ning“ kasutamisel.** Eelnõus KüTS § 3: *(1^2) Elutähtis üksus on:* *10) üksus, kellel on majandusaasta jooksul keskmiselt 250 või rohkem töötajat ja kelle **aasta bilansimaht ületab 50 miljonit eurot** või **aastakäive ületab 43 miljonit eurot**, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ning kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1^2 punktides 1–51.* *(1^3) Oluline üksus on:* *10) üksus, kellel on majandusaasta jooksul keskmiselt rohkem kui 50 töötajat ja kelle **aasta bilansimaht on vahemikus 10–43 miljonit eurot** ning **aastakäive on vahemikus 10–50 miljonit eurot**, arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ, ja kes on osutatud vähemalt ühes käesoleva seaduse § 1 lõike 1^2 punktides 1–51.*	Arvestatud ja selgitatud. Viidatud sätted üle vaadatud ja eelnõu muudatuste tõttu viidud KüTS §-i 3. Eelnõu teksti uuendamisel on soovitud välistada olukorda, kus töötajate arvu ja finantsnäitajate suuruste erisuste tõttu satuks üks üksus sama tegevusvaldkonna puhul erineva üksuse liigi all (varasemas eelnõus kas elutähtis üksus või oluline üksus; muudetud eelnõus vastavalt kas ülioluline üksus või oluline üksus).

31.9	**Täpsemalt ja selgemalt (sh täpsete normiviidetega eelnõu seletuskirjas) tuleks selgitada ka seda, mis hetkest hakkavad kulgema KüTS kohaldamisalasse kuuluva teenuse osutaja kohustuste täitmise tähtajad** – kas isiku „tuvastamisest“ teenuse osutajana RIA poolt või mõnest muust hetkest, sündmusest, asjaolust alates? **Samuti küsimus sellest, mis sättes ja kui pikk üleminekuaeg nähakse käesoleva eelnõuga KüTS nõuetega vastavusse viimiseks ette neile uutele teenuse osutajatele, kes varasemalt seaduse kohaldamisalasse ei kuulunud?** Seletuskirja kohaselt: *„Peamiseks muudatuseks on küberturvalisuse seaduse subjektide nimekirja täiendamine. Küberturvalisuse seaduse nõudeid peavad järgima juba praegu u 3500 organisatsiooni ning eelnõuga lisandub neile (esialgse hinnangu kohaselt) veel juurde u 2000 organisatsiooni.* *Eelmainitud nimekirja täiendamine tähendab ka uusi subjekte, kes peavad hakkama tegelema küberturvalisuse tagamisega ehk rakendama turvameetmeid ja olulise mõjuga küberintsidendi korral teavitama sellest ka järelevalveasutust.* ***Lisanduvatele organisatsioonidele nähakse ette ka üleminekuaeg kolm aastat, mille jooksul tuleb viia oma tegevus küberturvalisuse seaduse põhilisemate nõuetega kooskõlla.*** ***Elutähtsa teenuse osutajatel on erand – nemad lähtuvad** kehtiva õiguse ehk hädaolukorra seaduse tõttu **viieaastasest tähtajast**.”*.	Arvestatud ja selgitatud. Elutähtsa teenuse osutaja puhul on vastav tähtaeg ette nähtud juba hädaolukorra seaduses (vt tolle seaduse § 38 lg 1^3 punkti 3), kuid ka siinse eelnõuga täpsustatakse KüTSiga seotud üleminekuaegasid. Vastavad sätted on eelnõu KüTS §-des 4^1 ja 28^1. Elutähtsa teenuse osutajad, kellel tekkis esmakordselt KüTS-i järgimise kohustus pärast 2024. a 18. oktoobrit, saavad lähtuda hädaolukorra seaduse § 38 lg 1^3 punkti 3 kohaselt määratud tähtaegadest. Need üksused, kes saavad KüTSi teenuseosutajaks, kuid kellele ei kohaldu eelmainitud hädaolukorra seaduse § 38 lg 1^3 punkt 3, neile kohaldub 3 aastane üleminekutähtaeg, sh see tähtaeg ei ole sõltuvuses mõne haldusorgani otsusest. Vt selle kohta eelnõukohase KüTS § 28^1 seletuskirja. Elutähtsa teenuse osutajate puhul on küberturvalisuse nõuete temaatikat selgitatud põhjalikumalt Riigikogus arutlusel olnud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse 426 SE seletuskirjas, konkreetsemalt tolle eelnõu § 1 punktis 14. Seetõttu seda siinses eelnõus täpsemalt ei selgitata.

	Erinevalt seletuskirjas selgitatust nähakse eelnõuga muudetava HOS § 38 lõike 1^3 punkt 3 kohaselt elutähtsa teenuse osutajale KüTS kohustuste täitmiseks aga ette mitte **5-aastane**, vaid **kuni 5-aastane** maksimaalne tähtaeg, mille üle otsustab isikut elutähtsa teenuse osutajaks määrav ETKA haldusaktis. Seega võib ETO-kohustuste algus osutuda oluliselt lühemaks, kui seletuskirjas lubatud 5 aastat. Samas ei selgu eelnõust, mis kriteeriumite ja kaalutluste alusel lõplik tähtaeg selgitatakse ja määratakse. Näeme kindlasti vajadust tagada ettevõtetele piisavalt pikk ja selge üleminekuaeg. Samuti on eelnõust keerukas leida "uutele" KüTS teenuse osutajatele, kes ei ole ETO-ks HOS tähenduses, seletuskirjas lubatud 3-aastast üleminekutähtaega ning selgitusi selle kohta, miks eristatakse seda tähtaega ETO-de üleminekust ning kas KüTS alusel on 3-aastane üleminek igal juhul tagatud või sõltub see samuti mõne haldusorgani täiendavast otsusest. Peame oluliseks, et üleminekuajad ja neid selgitavad sätted oleks eelnõus selgelt välja toodud.	
31.10	**Lisaküsimus tähtaegadest tekib ka selles, kuidas arvestatakse ja millal ning mis alusel tekib teenuse osutajana tuvastatud isikutel kohustus asuda KüTS nõudeid täitma näiteks olukordades, kus:** **- isik võib nö liikuda seaduse kohaldamisala piiridel kord kohaldamise lävendeid täites ja seejärel nende alt välja langedes;**	Selgitatud Esitatud kommentaari esimese olukorraga kirjeldatud lahendus on olemas metoodikas, kuidas arvestatakse ning arvutatakse väikese- ja keskmise suurusega ettevõtjate töötajate ning finantsnäitajaid Euroopa Komisjoni soovituse 2003/361/EÜ kohaselt. Seletuskirjas on eelnõu KüTS § 3 juures selgitatud vastavat metoodikat. Eemaldasime volitusnormi Vabariigi Valitsuse määruse jaoks, millega saanuks lisada uusi teenuse osutajaid KüTSi kohaldamisalasse - uute teenuse osutajate lisamine toimub läbi KüTSi muutmise.

	- valitsus otsustab täiendavate sektorite või teenuseosutajate lisamise KüTS kohaldamisalasse. Küsimus on aktuaalne näiteks KüTS § 1 lg 1^2 p 31 nimetatud rahvatervise hädaolukorras esmatähtsate meditsiiniseadmete loetellu kuuluvate med-seadmete tootjate puhul. Meile teadaolevalt täna seesugust loetelu ei eksisteeri ning asjakohase valdkondliku EL määruse kohaselt tundub, et loetelud luuaksegi alles hädaolukorra tekkides. Kui see on nii, siis ei saa ükski meditsiiniseadmeid tootev teenuse osutaja selguda varem, kui Euroopas on hädaolukord välja kuulutatud. Samas on selge ka see, et alles hädaolukorra alguses teenuse osutajana tuvastatud üksus ei suuda asuda uusi kohustusi üleöö täitma ega nende rikkumise eest üleöö vastutust kanda.	Meditsiiniseadmete (kõigi) tootjatel on niikuinii kohustus NIS2 direktiivist tulenevaid kohustusi järgida (olulise üksusena), seega kui nad muutuvad teatud spetsiifilisi meditsiiniseadmeid tootes üliololuliseks üksuseks (varasema nimetusega elutähtsaks üksuseks), ei ole täiendava rakendusaja andmine põhjendatud. Vahetegu üliolulise üksuse ja olulise üksuse ning neile kohalduvate nõuete osas on ennekõike seotud järelevalve teostamisega (st kas tehakse järel- või eelkontrolli, kas on võimalik teatud täiendavaid meetmeid kohaldada üliolulise üksuse puhul ning millised on maksimaalsed trahvid väärteomenetluses), kuid muud põhilised nõuded on mõlema üksuse grupi puhul samad: nii turvameetmete nõuded, nõuded juhatuse liikme(te)le kui ka olulise mõjuga küberintsidendist teavitamise nõue.
31.11	**Eelnõu tutvustusel 23.1.2025 arutelus tõusetus küsimus sellest, kas seadusemuudatuste rakendamisel jätkub selle kohaldamisteenuse kuuluvate tuhandete teenuse osutajate kohustuste täitmiseks piisavalt kvalifitseeritud audiitoreid, sh kas võimaliku puuduse olukorras eeldatavasti tõusvad hinnad on uute kohustuste täitmiseks isikutele jõukohased.** Arvestades eelnõus teenuse osutajate kohustuste rikkumise puhuks sätestatud sanktsioonide rangust peab kindlasti olema tagatud eelnõu rakendatavus praktikas. Selles aspektis tuleks vastavalt täiendada eelnõu mõjuanalüüsi ning vajadusel kavandada asjakohased ülemineku- või erisätted.	Vt Rahandusministeeriumi kommentaari 6.5 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust. Samuti on eelnõus ette nähtud üleminekusätted – vt eelnõu KüTS § 28^1. Mõistame, et eelnõust tulenevate nõuete rakendamiseks on vaja aega. Üleminekusätete mõjul on seaduse rakendajatele ka selline üleminekuaeg antud. Loodame, et see võimaldab uute nõuete sujuvat rakendamist.

31.12	**Eelnõu tutvustusel 23.1.2025 arutelus tõusetus küsimus ka sellest, kas eelnõuga kavandatud sisulised küberturvalisuse nõuded vastavad NIS2 direktiivis ettenähtud miinimumstandardile või on Eesti vabatahtlikult kehtestamas EL õiguses ettenähtuga võrreldes rangemaid standardeid. Kui see peaks olema nii, siis vajaks iga siseriiklik tugevam standard eraldi põhjendamist ning hindamist selle täidetavuse ja proportsionaalsuse seisukohalt.** Kuna eelnõuga lisandub KüTS kohaldamisalasse väga palju uusi teenuse osutajaid, siis meie hinnangul ei piisa võimalike kõrgemate nõuete põhjendamiseks üksnes asjaolust, et sellised kõrgemad nõuded võivad osalt kehtida ka täna. Meile teadaolevalt on täna kehtiva KüTS rakendamisel mõnedel teenuseosutajatel juba tekkinud tõsiseid probleeme. See on nii näiteks perearstide puhul, kelle praeguste kohustuste ulatust ongi eelnõus kavandatud muudatuste abil juba leevendama asutud. Selles valguses ning vältimaks olukorda, kus range sanktsiooni ähvardusega kehtestataks faktiliselt täidetamatuid nõudeid, tuleks eelnõu sisulisi nõudeid kindlasti hinnata ja vajadusel-võimalusel diferentseerida ka kõigi teiste uute teenuse osutajate võimekuste kontekstis. Selles võtmes võivad väärida ülevaatamist ja täpsemalt piiritlemist või diferentseerimist ka tänased KüTS volitusnormid täitevvõimule küberturbe standardite kehtestamiseks.	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

31.13	**Sunniraha määrast** Peame põhimõtteliselt ebaõigeks tuletada ja võrdsustada KüTS-is sunniraha määr seaduse nõuete rikkumise eest määratava väärteotrahvi määraga. Tegemist on olemuslikult ja õiguslikult erinevate instrumentidega. Samuti ei näe sunniraha suurust ega ka sunniraha kohustust ette NIS2 direktiiv. Kui siiski siseriiklikult sunniraha kui haldussunni meede luua, siis tuleb see kui kohustuse täitmisele suunav meede nii sisus kui rahasummade osas selgelt eristada puhtalt karistusliku iseloomuga väärteotrahvist.	Mittearvestatud ja selgitatud Sunniraha on NIS2 direktiivis ette nähtud - vt artikli 34 lõiget 6: *Liikmesriigid võivad näha ette õiguse määrata sunniraha, mille eesmärk on sundida [üliolulist] või olulist üksust käesoleva direktiivi rikkumist lõpetama, kooskõlas pädeva asutuse eelneva otsusega.* Vt ka Eesti Jõujaamade ja Kaugkütte Ühingu kommentaari 25.3 vastust.
32. Eesti Vee-ettevõtete Liidu arvamus 31.01.2025 kiri nr 2-2/170		
32.1	Edastame küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõule Eesti Vee-ettevõtete Liidu seisukohad. Ühtlasi märgime, et Eesti Vee-ettevõtete Liit ei saanud arvamuse avaldamiseks kõnealust eelnõud, kuigi eelnõu puudutab otseselt suuremaid Eesti vee-ettevõtteid. Seega palume tulevikus lisada partnerite hulka ka Eesti Vee-ettevõtete Liit kui vee-ettevõtete (eelnõu kohaselt elutähtsad üksused) katusorganisatsioon.	Selgitatud Eesti Vee-ettevõtete Liidule edastati siinne eelnõu 09.12.2024. a. ning eelnõu koostajate info kohaselt jõudis eelnõule ka Liiduni ja meil on hea meel, et Liit on eelnõu läbi töötanud ja eelnõule enda tagasiside saatnud.
32.2	Palume selgitada küberturvalisuse seaduse (KüTS) kohaldamise ala. Eelnõu kohaselt täiendatakse küberturvalisuse seaduse § 1 lõigetega 1^1 – 1^6, kusjuures lõike 1^1 kohaselt käesolevat seadust kohaldatakse Euroopa Liidus teenuseid osutavatele või tegutsevatele üksustele, kellel on majandusaasta jooksul keskmiselt 50 või rohkem töötajat ja kelle aasta bilansimaht või aastakäive	Selgitatud Kui vee-ettevõtjad on hädaolukorra seaduse alusel elutähtsa teenuse osutajateks määratud, siis kohalduvad neile KüTSi nõuded hoolimata töötajate arvust ja käibe suurusest (vt NIS2 direktiivi art 2 lõiget 4). Seega ei ole liikmesriikidel võimalust välistada direktiivis toodud nõuete kohaldamisalast elutähtsa teenuse osutajaid. Nn suuruse kriteeriumiga hõlmatakse KüTSi kohaldamisalasse need vee-ettevõtted, kes ei ole määratud elutähtsa teenuse osutajateks (kui neid peaks olema). Eelnõu koostajatel

	ületab 10 miljonit eurot, arvestades mikro- ja väikese ettevõtja määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikese ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41). Üksuste määratlemisele ei kohaldata Euroopa Komisjoni soovituse 2003/361/EÜ lisa artikli 3 lõiget 4. Palume täpsustada, kas oleme õigesti aru saanud, et vee-ettevõtted, kellele küberturvalisuse seadus kohaldub on AS Tallinna Vesi, AS Tartu Veevärk, OÜ Järve Biopuhastus, AS Narva Vesi ja AS Pärnu Vesi. Ühtlasi juhime tähelepanu, et Eestis on kokku ca 130 vee-ettevõtet, kes kõik on hädaolukorra seaduse tähenduses elutähtsa teenuse osutajad. Väiksemate vee-ettevõtete jaoks ei ole seaduseelnõuga ettenähtud kulude kandmine võimalik ega ka vajalik. Näiteks tuleb arvestada, et Eestis on vee-ettevõtteid, kus töötab vaid 2-3 töötajat ning nad pakuvad veeteenust ca 50 inimesele, mistõttu seaduseelnõuga ettenähtud nõuded ei ole nende vee-ettevõtete jaoks proportsionaalsed.	ei ole selles küsimuses võimalik eelnõu muuta. Vastasel juhul ei oleks NIS2 direktiiv kohaselt üle võetud. Siin vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.
32.3	Eelnõu punktis 26, millega muudetakse küberturvalisuse seaduse §-i 7 lg 2 p-i 6 kohustub teenuse osutaja tagama süsteemi tarneahela turvalisuse, sh teenuse osutaja ja tema koostööpartnerite vahelistes lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise. Palume täpsustada eelnõus või vähemalt selgitada seletuskirjas, millised on need turvameetmed, mida teenuse osutaja peaks koostööpartneri lepingus	Selgitatud. Avalikul kooskõlastusringil olnud eelnõu KüTS § 7 lõike 2 sisu on viidud sama paragrahvi lõike 5 alusel antud Vabariigi Valitsuse määruse muudatusse (vt seletuskirja lisaks olevaid määruse kavandeid). NIS2 direktiiv ei näe ette konkreetsemaid meetmeid, mida teenuseosutaja peaks enda koostööpartneriga sõlmitavas lepingus sätestama. Seetõttu määruse kavandis seda ei täpsustata. Samas on näiteks Eesti infoturbestandardi puhul esitatud kommentaariga seotud väljast tellimise moodul OPS.2.3. ja temaatikaga on seotud ka moodul OPS.3.2. Sarnaseid nõudeid peab ka rakendama teenuseosutaja, kes rakendab rahvusvahelist standardit ISO/IEC 27001.

	sätestama? Kas piisab üldisest viitest, et tellija on teenuse osutajaks KüTS-i tähenduses ning seega kohustub koostööpartner arvestama KüTS-st tulenevaga, järgima vähemalt keskmist küberturbe taset ning teavitama tellijat puudutavatest intsidentidest KüTS-is toodud tähtaja jooksul? Kui sellest ei piisa, siis palume täpsustada, mida konkreetselt oodatakse? Lisaks palume täpsustada, mida tähendab regulaarne ülevaatus ja ajakohastamine? Milline on regulaarsus või kas teenuse osutaja määrab selle ise? Kuidas toimub turvameetmete ajakohastamine olukorras, kus koostöölepingu muutmine toimub vaid poolte kokkuleppel (ja sageli teenuse osutajate puhul veel ka riigihanke tulemusel ehk muutmisele kehtivad veel eraldiseisvad reeglid)?	Regulaarsuse määrab teenuseosutaja ise. Kui mõnest õigusaktist tulenevalt on tekkinud uued kohustused, siis saabki selle alusel osapoolte kokkuleppel lepingut muuta. Kui toimub muutus üldises ohupildis, siis tuleb samuti leping ajakohastada. Kui välise partneri turvatase pole piisav, tuleb teenuseosutajal endal rakendada piisavaid lisameetmeid võimalike riskide vähendamiseks. Nõue tagada lepingute muutmise võimalus on tingitud just sellest, et ka pikaajaliste partneritega saaks aeg-ajalt küberturvalisuse teemal omavahel uuesti kokku leppida.
32.4	Palume täpsustada, kas ja millisel juhul võib E-ITS/ISO27001 vastav teenuse osutaja osutuda Euroopa sertifitseerimise kava subjektiks (eelnõu punkt 49, millega muudetakse küberturvalisuse seaduse §-i 13[3]). Kas täiendav auditeerimine võib olla asjakohane ka vee-ettevõtjate puhul, kes on elutähtsaks üksuseks eelnõu kohaselt? Kui jah, siis palume, et vastavasisuline Vabariigi Valitsuse määruse eelnõu saadetakse meile piisava ajavaruga kooskõlastamiseks.	Selgitatud Eelnõud koostades ei olnud soovi koheselt seda volitusnormi kasutada ehk määrust anda, vaid tekitada võimalus vastava Vabariigi Valitsuse määruse andmiseks. Sellele eelneb konkreetsem analüüs, millega selgitatakse välja, kas ja kellele võiks kehtestada nõude järgida ELi küberturvalisuse skeemi. Seega oleks kaasatud varakult ka asjassepuutuvad osapooled, kes saanuks anda ka tagasiside vastava nõude (määruse) koostamiseks. Juhime tähelepanu ka Kaitseministeeriumi kommentaarile 2.3, milles esitati üks võimalik näide, kuidas seda volitusnormi oleks saanud kasutada. Hetkel võeti see sisend teadmiseks. Eelnõust on vastav paragrahv välja jäetud, et võtta üle NIS2 direktiiv minimaalses mahus.
32.5	Kehtiva KüTS § 7 lg 3 kohaselt kui teenuse osutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuse osutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise. Kehtiva	Mittearvestatud ja selgitatud. Kõnealuse eelnõu eesmärk on NIS2 direktiivi ülevõtmine. Esitatud ettepanek on teema kohta, mis pole sätestatud NIS2 direktiivis, mistõttu seda siinse eelnõuga ei lahendata, kuna eeldab laiemat analüüsi ettepanekus toodud teemadel: nt et kuidas üldse on võimalik võtta riigi tasandil vastutusele (eelduslikult on kommentaaris mõeldud

	KüTS § 8 lg 1^1 kohaselt kui teenuse osutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuse osutaja selle eest, et teine isik teavitab teenuse osutajat hiljemalt 24 tundi pärast käesoleva paragrahvi lõikes 1 nimetatud küberintsidendist teada saamist. Antud küsimust arutati ka 23.01.2025. a toimunud infopäeval, kus tõstatati küsimus, et kuidas saab teenuse osutaja vastutada teise isiku tegevuse/tegevusetuse eest, kui ta on omalt poolt teinud kõik endast oleneva (nt sätestanud koostöölepingus vastavad tingimused jne). Sellest lähtuvalt oleks ettepanek täiendada KüTSi selliselt, et teenuse osutaja vabaneb vastutusest, kui selgub, et ta on täitnud seadusest tulenevaid kohustusi ja teinud omalt poolt kõik endast oleneva, et kahjulikku tagajärge ära hoida. Sarnaselt isikuandmete kaitse seadusele (vastutav töötleja vs volitatud töötleja) võiksid ka KüTS-is olla sätestatud eraldi kohustused ja vastutus teenuse osutaja koostööpartneritele, mis võimaldaksid: a) teenuse osutajatel paremini selgitada teenuse osutaja koostööpartneritele nende kohustusi ja vastutust küberturbe tagamisel ja b) riigi tasandil vastutusele võtta teenuse osutaja koostööpartneri, kui teenuse osutaja on enda kohustused nõuetekohaselt täitnud.	väärteomenetluse raames) üksust, kes ei ole KüTSi teenuseosutaja. Eelnõu täiendamine lisaküsimustega viiks kahjuks fookust eemale NIS2 direktiivi ülevõtmisega seotud teemadelt. Küll aga on ministeerium valmis seda küsimust analüüsima tulevikus.
32.6	NIS2 direktiivi ja seaduseelnõu üheks oluliseks märksõnaks on küberturbealased koolitused. Eelnõu väljatöötajad on eelnõu seletuskirjas esitanud ka ettepanekud juhtorgani liikme koolituse võimalike õpiväljundite osas. Nagu ministeerium	Vt ka Rahandusministeeriumi kommentaari 6.1 vastust. Eelnõus ega selle seletuskirjas ei ole planeeritud õpiväljundeid ka üksuse ametnike ja töötajate koolitusnõude rakendamise ühtlustamiseks. Samas, kui arvestada NIS2 direktiivi artikli 20 lõike 2 teksti, siis tolle lõike mõte on, et ka üksuse ametnikud kui teenistujad saavad sarnaseid koolitusi nagu juhatuse tasand. Siiski tuleb ka siin pigem

	23.01.2025.a toimunud tutvustusel mainis, on valmimas sellekohane Digiriigi e-akadeemia koolitus, mis ei piira võimalust korraldada koolitust ka ettevõtte siseselt või osta koolitus sisse mõnelt erasektori ettevõttelt. Meie hinnangul vajab see temaatika täpsustamist, et kõik teenuse osutaja töötajad (sh juhtorgani liikmed) saaksid võrdsetel alustel koolitatud. Seega palume vähemalt eelnõu seletuskirja tasandil täpsustada, kas tänane RIA küberturbe koolitus (millest oli ka 23.01.2025 arutelul juttu) on piisav teenuse osutaja töötajate (v.a juhtorgani liige) koolitusnõude täitmiseks KüTS tähenduses? Lisaks, kas saime õigesti aru, et juhtorgani liikme koolituse võib korraldada ka ettevõtte siseselt (nt infoturbejuhi poolt), kui täidetud on seletuskirjas sätestatud õpiväljundid? Kui mitte, siis kes selleks koolitajaks võib olla või milline pädevus tal peab olema? Kas ministeerium plaanib õpiväljundeid ka töötajate koolitusnõude rakendamise ühtlustamiseks?	arvestada ka konkreetse ametniku või töötaja rolliga ehk on ka võimalus, et konkreetne roll võib tekitada vajaduse mõne spetsiifilisema või täpsema koolituse saamist. See kõik peaks selguma üksuse turvameetmete määratlemisel ning selle osaks oleva küberturvalisus valdkonnaga seotud koolituste (vt NIS2 direktiivi artikli 21 lõike 2 punkti g, mis võetakse üle KüTS § 7 lõike 5 alusel antava Vabariigi Valitsuse määrusega – vt siinse eelnõusse seletuskirja lisaks olevate määruste kavandeid) sisu kokku panemisel.
32.7	Palume selgitada lahendusi 23.01.2025 tutvustusel kõlanud audiitorite hinnangule, et teenuse osutajatel ei pruugi olla võimalik täita KüTS-i nõudeid tähtaegselt, kuivõrd auditite nõudlus ületab pakkumust. Kas see tähendab, et järelevalve teostaja võtab eeltoodut arvesse, kui selgub, et KüTS-i kohustusi ei täidetud eelnimetatud põhjustest tulenevalt?	Vt Rahandusministeeriumi kommentaari 6.5 vastust ja Sotsiaalministeeriumi kommentaari 9.1 vastust.
33. Advokaadibüroo RASK arvamus 06.01.2025 e-kiri		
33.1	Eelnõu seletuskirja sisukokkuvõttes on märgitud: *„Lisanduvatele organisatsioonidele nähakse ette*	Arvestatud ja selgitatud

	ka üleminekuaeg kolm aastat, mille jooksul tuleb viia oma tegevus küberturvalisuse seaduse põhilisemate nõuetega kooskõlla. Elutähtsa teenuse osutajatel on erand – nemad lähtuvad kehtiva õiguse ehk hädaolukorra seaduse tõttu viieaastasest tähtajast." Teisalt ei ole eelnõus endas aga üleminekuaja kohaldumisele viidatud. Seletuskirja sisulises osas ja teistes eelnõu juurde kuuluvates dokumentides on üleminekuaega mainitud, kuid seda üksnes seoses hädaolukorra seaduse muutmisega. Viimase tähenduses on mõiste „elutähtsa teenuse osutaja" aga oluliselt kitsam, kui see on KüTS-i tähenduses. Eeltoodust tulenevalt jääb kõnealuse seletuskirja tausta selgusetuks, kas seal mainitud üleminekuaeg kohaldub üksnes elutähtsa teenuse osutajatele hädaolukorra seaduse tähenduses või kõigile elutähtsa teenuse osutajatele, sh KüTS-i muutmisega elutähtsa teenuse osutajate nimekirja lisanduvatele üksustele. Palun täpsustage seletuskirjas märgitud üleminekuajaga seonduvat.	Elutähtsa teenuse osutaja puhul on vastav tähtaeg ette nähtud juba hädaolukorra seaduses (vt tolle seaduse § 38 lg 1^3 punkti 3), kuid ka siinse eelnõuga täpsustatakse KüTSiga seotud üleminekuaegasid. Vastavad sätted on eelnõu KüTS §-des 4^1 ja 28^1. Vt ka seletuskirja lisatud selgitusi nende sätete kohta.
	34. AS Elenger Grupp arvamus 31.01.2025 kiri	
34.1	Eelnõu kohaselt laiendatakse küberturvalisuse seaduse (KüTS) kohaldamisala tegevusalapõhiselt, hõlmates muuhulgas elektritootjad ja LNG müügiga tegelevad isikud. Lisaks tegevusalale peavad KüTS-i subjektide töötajate arv ja finantsnäitajad ületama teatud künnised – vastavalt 50 töötajat ja lisaks aastakäive või bilansimaht üle 10 miljoni euro. Seotud ettevõtjate puhul (ettevõtja	Osaliselt arvestatud ja selgitatud Üksuste hõlmamise osas KüTSi alla: siin vt Majandus- ja Kommunikatsiooniministeeriumi kommentaari 5.3, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 ning Eesti Kaubandus-Tööstuskoja kommentaari 26.1 vastust. Siinse eelnõuga paralleelselt on Justiits- ja Digiministeeriumil ettevalmistamisel ka KüTS § 7 lõike 5 alusel kehtestatud „Võrgu- ja infosüsteemide küberturvalisuse nõuded" määruse muudatus, mis muudab ka kriteeriume, millal mingi üksus peab

	omab teises ettevõtjas üle 51%) tuleb aga künniste hindamisel arvestada kontserni vastavaid arve tervikuna. Selle tulemusena saavad KüTS-i subjektideks ka järgmised Elengeri Eestis asuvad tütarettevõtjad (arvandmed 31.12.2023 seisuga): • **OÜ Pärnu Päikesepark 1:** töötajaid 0, varad 1 005 725 eurot, müügitulu 138 858 eurot. • **OÜ Pärnu Päikesepark 2:** töötajaid 0, varad 995 532 eurot, müügitulu 136 810 eurot. • **OÜ Pärnu Päikesepark 3:** töötajaid 0, varad 969 305 eurot, müügitulu 126 682 eurot. • **OÜ Pärnu Päikesepark 4:** töötajaid 0, varad 971 918 eurot, müügitulu 127 648 eurot. • **Elenger Marine OÜ:** töötajaid 5, varad 6 864 026 eurot, müügitulu 22 474 629 eurot. Ükski neist ettevõtjatest ei kvalifitseeru iseseisvalt KüTS-i subjektiks – meie päikesepargid on mikroettevõtjad raamatupidamise seaduse tähenduses ja Elenger Marine OÜ väikeettevõtja. Kuna aga kooskõlastamisele esitatud eelnõus on tehtud viide ettevõtja määratlusele Euroopa Komisjoni soovituses ettevõtjate suuruse määratlemise kohta, oleksid nimetatud ettevõtjad KüTS-ist tulenevate kohustuste täiemahulisteks subjektideks. See on aga otseses vastuolus küberturvalisuse 2. direktiivi (NIS2 direktiiv) ettevalmistamisel taotletud eesmärgiga, mida ka	kohaldama Eesti infoturbestandardit või selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001 (vt eelnõude infosüsteemi toimikut 25-0715). Kui üksus ei pea kumbagi standardit rakendama, siis on tal jätkuvalt vajalik täita esmased nõuded, mis ei ole niivõrd detailsed kui eelmainitud standardid. Need nõuded peavad ära täitma kõik KüTSi teenuseosutajad. Vt siin ka Sotsiaalministeeriumi kommentaari 9.1 vastust. Samuti on eelnõud täiendatud sättega, mis sätestab, et KüTSis üksuse töötajate arvu, aastakäibe ja aastabilansi mahu kindlaksmääramisel ei arvestata partner- või sidusettevõtja andmeid Euroopa Komisjoni soovituse 2003/361/EÜ tähenduses, kui üksus on oma partner- või sidusettevõtjast teenuste osutamisel kasutatavate süsteemide osas sõltumatu. See asub eelnõu KüTS § 3 lõikes 7 (vt ka vastavaid selgitusi seletuskirjas).

	eelnõu seletuskirjas endas rõhutatud - „NIS2 direktiivi ette valmistamisel oli soov välistada olukord, kus mikro- ja väikeettevõtjad satuvad NIS2 direktiivi kohaldamisalasse.“. Elenger peab küberturvalisust väga oluliseks, kuid leiab, et mikro- ja väikeettevõtjatele Eesti infoturbestandardi või rahvusvahelise standardi ISO/IEC27001 sertifikaadi omamise ja regulaarse vastavusauditeerimise kohustuste kehtestamine on ebaproportsionaalne ja tekitab põhjendamatuid kulusid ning halduskoormust. Meile teadaolevalt on Läti ja Leedu praktika NIS2 direktiivi ülevõtmisel ka eelnõus esitatust oluliselt erinev: - Läti küberturvalisuse seadus[4] kohaldub ainult suurtele energiasektori ettevõtjatele (vähemalt 250 töötajat või aastakäive üle 50 miljoni eurot ja bilansimaht üle 43 miljoni euro); - Leedus laieneb küberturvalisuse seadus[5] energiasektori ettevõtjatele, millel on vähemalt 50 töötajat ja bilansimaht või aastakäive üle 10 miljoni euro. Meie teada Lätis ja Leedus ei võeta KüTS-i subjektide kindlaksmääramisel arvesse sidusettevõtjaid.	

[4] Leitav Nacionālās kiberdrošības likums
[5] XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas

	Palume Eestis NIS2 direktiivi ülevõtmisel kaaluda ettevõtjatele vähem koormavat lahendust ning välistada mikro- ja väikeettevõtjad KüTS-i subjektide ringist. Kui see eelnõu koostajate arvates on võimatu, arvestades Euroopa Komisjoni soovitust, palume selgitada, kuidas on teised Euroopa Liidu liikmesriigid saavutanud lihtsustatud ja oma ettevõtjaid enam kaitsva lähenemise. Üleliigne agarus Euroopa Liidu nõuete ülevõtmisel seab Eesti ettevõtjad naaberriikidega võrreldes ebasoodsasse konkurentsiolukorda ja suurendab põhjendamatult Eesti ettevõtjate kulusid ning halduskoormust.	
34.2	Punktis 1 esile toodud probleemiga haakub tihedalt ka küsimus eelnõu mõjuhinnangute adekvaatsusest. Eelnõu seletuskirja kohaselt on eelnõu uuteks subjektideks olevaid gaasiettevõtjaid terve Eesti peale kokku 1 ja elektritootjaid 3. Nagu eelnevast näha, siis juba pelgalt Elengeri grupi Eesti ettevõtjate seas oleks Euroopa Komisjoni soovituse rakendamise tõttu KüTS-i lisanduvateks subjektiks olevaid isikuid vastavalt 2 (gaasiettevõtjad) ja 4 (elektritootjad). See annab põhjust arvata, et eelnõu mõjuhinnangud on ekslikud ning eelnõust tulenevate nõuete rakendatavuse põhjendatus ning ka võimalikkus, samuti ajagraafikud vajavad uut hindamist.	Arvestatud – mõjude analüüs on üle vaadatud ja võimaluse korral täiendatud.
34.3	Lisaks soovime juhtida eelnõu koostajate tähelepanu eelnõu üleminekutähtaegade kehtestamiseks valitud viisi selgusele ja õiguslikule korrektsusele.	Arvestatud – vastavad sätted on eelnõu KüTS §-des 4^1 ja 28^1. Vt ka seletuskirja lisatud selgitusi nende sätete kohta.

	Eelnõu seletuskirja osa 1.1 kohaselt nähakse lisanduvatele organisatsioonidele ette üleminekuaeg kolm aastat. Nimetatud tähtaegu pole esitatud eelnõus, küll leiab need seletuskirjale lisatud KüTS § 7 lg 5 alusel antud määruse muudatuse kavandist. KüTS § 7 lg 5 alusel antud määruse rakendamise sätetega saab kehtestada tähtajad vaid selle sama määruse rakendamiseks, mitte aga seadusest vahetult tulenevate nõuete ja kohustuste rakendamiseks. Seega on seadusest endast seletuskirjas viidatud üleminekusätted puudu.	
35. Baltic RCC OÜ arvamus 30.01.2025 kiri		
35.1	KüTS SE § 1 lg 1^4 kohaselt kohaldatakse küberturvalisuse seadust üksuse suhtes olenemata tema suurusest kui üksus vastab vähemalt ühele punktides 1) kuni 4) kirjeldatud tingimusele. Eelnõu sõnastuse kohaselt on § 1 lg 1^4 iseseisev alus, millest tulenevalt muutub isik seaduse subjektiks, kui ta vastab ühele nimetatud tingimustest, kuigi isik ei ole KüTS SE § 1 teistes lõigetes nimetatud ega kuulu Vabariigi Valitsuse määrusega määratud valdkonda või sektorisse. Ettepanek on piirata isikute ringi NIS2 direktiivi lisades I ja II sätestatud liiki üksustega nagu on sätestatud NIS2 direktiivi artikkel 2 lg-s 2 ning lisada konkreetne viide Vabariigi Valitsuse määrusele, mis muudaks subjekti määramise selgemaks. Eesmärk on välistada olukord, kus isik vastab mõnele KüTS SE § 1 lg 1^4 punktides sätestatud tingimusele ning justkui oleks	Mittearvestatud ja selgitatud Kommenteeritud lõige on eelnõust eemaldatud. Selle asemel selgitatakse seletuskirjas konkreetse üksuse juures, kas ja kuivõrd kohalduvad selle üksuse puhul NIS2 direktiivi artikli 2 lõike 2 punktides b–e sätestatud kriteeriumid. Selline lahendus on loodetavasti KüTS-i rakendajatele selgem ja paremini hoomatavam. Seaduse rakendaja ei pea eraldi hindama (avalikul kooskõlastusringil olnud eelnõu) KüTS § 1 lg 1^4 eelduste täitmist, vaid piisab sellest, et ta vaatab, kas ta tegutseb valdkonnas, mis on (uuendatud eelnõu) KüTS §-s 3 nimetatud ning vastavalt sellele, kas konkreetse valdkonna puhul kohalduvad ka piirmäärad töötajatele ning käibele või bilansile, hinnata ka enda puhul nende piirmäärade täitmist. Eelnõu puhul tehakse nii, et seaduse ehk KüTSi tasandil on ära määratletud, millised üksused peavad tolle seaduse nõudeid järgima. Seetõttu esitatud konkreetset ettepanekut ei arvestata, kuid eelnõus üldiselt tehtud muudatused (KüTS §-d 1 ja 3) järgivad ettepaneku loogikat. Selgitame täiendavalt, et eelnõust on põhiseaduspärasuse osas tõstatatud küsimuste tõttu eemaldatud (avalikul kooskõlastusringil olnud eelnõu) KüTS § 1 lõike 1^6 alusel antava määruse volitusnorm.

	kohustatud küberturvalisuse seadust järgima, samas ükski teine subjektiks kvalifitseerumise nõue ei ole täidetud. Sõnastuse ettepanek: KüTS SE § 1 lg 1^4 *„Käesolevat seadust kohaldatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 lisas I või II osutatud liiki üksuse suhtes olenemata tema suurusest, kui üksus kuulub käesoleva paragrahvi lõikes 1^6 nimetatud Vabariigi Valitsuse määrusega määratud valdkonda või sektorisse ja vastab vähemalt ühele järgmisele tingimusele:*“	
36. Eesti Energia AS arvamus 31.01.2025 kiri		
36.1	Teeme ettepaneku KüTS eelnõus lahti kirjutatud erinevate terminite definitsioonid ja selgitused, mitte viidata EL õigusaktidele. Hetkel on eelnõus äärmiselt palju viiteid EL õigusaktidele ning on tekitatud olukord, kus õigusakti kohuslasel on äärmisel keeruline seadust mõista ehk tagatud pole seaduse õigusselgus. Sellest on tingitud ka osad meie kommentaarid, kuna on keeruline mõista seaduse paragrahvi täpset sisu ja eesmärki.	Mittearvestatud ja selgitatud Eelnõus on tehtud viiteid EL õigusele ja seal olevatele mõistetele - eelnõu koostamisel on kaalutud küll võimalust viidete täpsemaks defineerimiseks, kuid jõutud siiski järeldusele neid ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137). Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
36.2	Kuna KüTS eelnõuga (i) luuakse uusi täiendavaid kohustusi (nt KüTS § 7 lg 2^1 p 1) ja (ii) muudetakse KüTS rakendamine kohustuslikuks elutähtsa	Arvestatud ja selgitatud

	teenuse osutaja (edaspidi **ETO**) **kogu tegevuse** raames (sõltumata, kas see tegevus on elutähtsa teenuse osutamine või mõni muu kõrval tegevus, nt muu tulus äritegevus, mis ei ole elutähtis teenus) (kehtivas KüTSi kohaselt on elutähtsa teenuse osutaja kohustatud KüTS rakendama üksnes elutähtsa teenuse osutamisel), siis peaks eelnõus olema ette nähtud ülemineku periood, et elutähtsa teenuse osutaja saaks viia oma protsessid ja süsteemid uue KüTSiga vastavusse. Teeme ettepaneku, et vastav ülemineku periood peaks olema võrdne uute KüTS kohuslaste ülemineku perioodiga (hetkel kehtestaks ministri määrusega selleks 3 aastat).	Vastavad üleminekusätted juba kehtiva KüTS-i subjektidele on nähtud ette eelnõukohases KüTS §-s 28^1. Täiesti uued subjektid saavad kohaldada eelnõukohast KüTS § 4^1. Vt ka seletuskirja lisatud selgitusi nende sätete kohta.
36.3	Tuginedes eelmises punktis viidatud ministri määrusele ja 23.01.2025 toimunud Kärajate kohtumisele, siis soovitame Vabariigi Valitsuse 9. detsembri 2022. a määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 14 muudatuse teha selliselt, et mõlema üleminekute aeg oleks võrdne hädaolukorra seaduse § 38 lõige 1^3 punktis 3 tooduga. St soovitame määrata lõplikuks ajaks 18. oktoober 2029. aasta.	Mittearvestatud ja selgitatud Eelnõus on sätestatud, et üksusele, kes ei ole elutähtsa teenuse osutaja, on üleminekuaeg 3 aastat. Eelnõu kooskõlastamise järgselt on analüüsitud ja kaalutud erinevaid üleminekuperioode ning eelnõu täiendatud KüTS §-ga 28^1 ja 4^1, mis näevad ette 3-aastase aja nõuete rakendamiseks. Pikemat perioodi ei saa KüTS-i eesmärke arvestades pidada põhjendatuks. Üksnes elutähtsa teenuse osutajad, kellel tekkis esmakordselt KüTS järgmise kohustus pärast 2024. a 18. oktoobrit, on õigus tugineda hädaolukorra seaduse § 38 lõige 1^3 punkti 3 kohaselt määratud üleminekuajale. See on vajalik selleks, et tagada elutähtsa teenuse osutajatele ühtne regulatsioon.
36.4	KüTS eelnõu seletuskirja lk 3 nähakse ette EL taasterahastust ja uute subjektide rahastust. Samas ei ole välja toodud, kas rahastus võib laieneda ka alltöövõtjatele, nt on mitmeid ettevõtteid, kellele KüTS nõuded hakkavad kohalduma läbi KüTS kohuslasele teenuse osutamise. Seega, et KüTS kohuslane ei peaks loobuma oma koostööpartnerist, kes peab vastama samadele tingimustele, siis võiks vastav rahastus ka neile	Selgitatud Eesmärk on anda toetust ka teistele üksustele kui teenuseosutaja – vt eelnõu KüTS § 28^2.

	laieneda läbi KüTS kohuslase taotluse. See kergendaks oluliselt ka KüTS kohuslaste olukorda ning ei tekiks kohuslastes olukorda, et kohuslased ei saa kasutada teatud teenuseid, kuna need ei ole vastavuses. Läbi selle toetaks riik erinevaid teenuse osutajaid ja ettevõtteid ning tagaks pakutavate teenuse turvalisuse.	
36.5	KüTS [§ 1 lg 1^2 p-d 39 ja 40] - teeme ettepaneku vähemalt seletuskirjas avada vastavad punktid põhjalikumalt, et tagada õigusselgus. Hetkel jääb arusaamatuks, millised ettevõtted jäävad vastavate punktide skoopi. Nt kas vastavasse skoopi jäävad ka kontserni emaettevõtted, kes üle kontserni pakuvad IT teenuseid.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.21 vastust.
36.6	KüTS § 2 - soovitame vaadata üle ja täpsustada järgnevad mõisted: Kirjutada mõistena lahti, mida mõeldakse täpselt „küberturvalisuse alase tegevuse“ alla. Siinkohal on oluline, et vastav mõiste oleks maksimaalselt piiritletud, et hilisemalt ei tekiks ülemäärast tõlgendamise ruumi.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.12 vastust.
36.7	KüTS § 2 lõikes 3^3 on mõiste „risk“. Teeme ettepaneku see mõiste defineerida järgmiselt: 1. variant - „risk“ – vaatlusaluse ohu potentsiaal ära kasutada mingi vara või vararühma nõrkusi ja tekitada seeläbi kahju; 2. variant - „risk“- võimalus, et küberintsidendi läbi tekib kahju või tõrge, väljendatakse kahju ulatuse mõju hinnangu ja realiseerumise esinemise võimalikkuse kombineeritud näitajana.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.12 vastust, Kaitseministeeriumi kommentaari 2.1 ja Riigi Infosüsteemi Ameti kommentaari 17.23 vastust.
36.8	KüTS § 2 lõikes 3^5 on mõiste „oluline küberoht“. Palume seda mõistet vähemalt seletuskirjas	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.32 vastust.

	õigusselguse tagamiseks täpsustada . Oluline on tuua välja, milline on tõsine mõju. Nt kaua süsteem peaks maas olema (nt süsteemi ei ole töökorras 48 tundi), kui suurel hulgal kasutajad peaksid olema mõjutatud (nt 50% kasutajat on mõjutatud), mis on märkimisväärne kahju (nt aastakäibest selline protsent).	
36.9	KüTS § 2 lõikes 3^6 on mõiste „nõrkus“._Teeme ettepaneku see mõiste defineerida järgmiselt: „nõrkus“ - vara või meetme nõrk koht, mille saab ära kasutada üks või mitu ohtu (ISO 27001 sõnastus).	Vt Riigi Infosüsteemi Ameti kommentaari 17.11 vastust.
36.10	KüTS § 3 lg 3^1 - KüTS kohuslane peab edastama kõnealuse lõike alusel kontaktteabe Riigi Infosüsteemi Ametile (edaspidi RIA), kuid eelnõu ja seletuskirja kohaselt jääb arusaamatuks, kas esmase pöördumise teeb RIA ja teavitab osapoolt, et ta on kohuslane ning siis edastab KüTS kohuslane vastava teabe või peab ta hindama ise, et on kohuslane ja ilma RIA pöördumiseta edastama vastava teabe ning sellisel juhul mis on esialgne teabe edastamise tähtaeg? Täiendavalt palume täpsustada, mida mõistetakse IP aadresside vahemiku all ja mis on selle eesmärk.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.41 ning Regionaal- ja Põllumajandusministeeriumi kommentaari 7.6 vastust.
36.11	KüTS § 5^2 lg 2 – Teeme ettepaneku määrata konkreetne pädev asutus, ilma edasivolituse õiguseta. Sellisel juhul on osapooltele selge, kes on vastav pädev asutus ja kellega vastava paragrahvi alusel vastav suhtlus toimub.	Vt Riigi Infosüsteemi Ameti kommentaari 17.37 vastust.
36.12	KüTS § 6^1 lg 2 ja 3 – teeme ettepaneku, et juhtkonna koolitamine peaks toimuma riigi enda poolt (nt RIA), kuna sellega tagatakse, et koolitusel	Selgitatud Koolituse teemal – vt Rahandusministeeriumi kommentaari 6.1 vastust ja Advokatuuri kommentaari 20.9 vastust.

	jagatud teave on piisav ning ka asja-ja ajakohane. Lisaks tagatakse ka üleriigiliselt ühtne arusaam. Täiendavalt palume vähemalt seletuskirjas selgitada, kes täpsemalt juhtorgani alla lähevad, kas ainult juhatus või ka nõukogu.	Eelnõukohase KüTS § 6^1 sõnastust on täpsustatud selliselt, et eelnõus on otsesõnu viidatud juhatusele. Erandina on lõikes 4 nähtud ette, et kui teenuseosutajal ei ole oma juriidilisest vormist või struktuurist tulenevalt juhatuse liiget, kohaldatakse juhatuse liikme kohta käivat ka muule isikule, kes on seaduse, põhimääruse või muu õigusakti kohaselt määratud asjaomase teenuseosutaja juures juhtimisülesandeid täitma. Kui teenuseosutaja on füüsilisest isikust ettevõtja, kohaldatakse teenuseosutaja juhatuse liikme kohustuste kohta sätestatut asjaomasele füüsilisele isikule
36.13	KüTS § 7 lg 2^1 p 1 ja p 2 – Teeme ettepaneku vastavad punktid eemaldada, kuna need dubleerivad E-ITSi tingimusi ning ei ole vajalikud NIS 2 artikli 21 p-de 1 ja 2 ülevõtmiseks. Hetkel luuakse olukord, kus on kohuslased kohustatud täitma kindlasti E-ITS standardist tulenevaid kohustusi, isegi kui nad on otsustanud ISO 27001 kasuks. See tekitab kohuslastele täiendavaid väljaminekuid, mida ei ole hetkel seletuskirja kohaselt analüüsitud.	Vt Riigi Infosüsteemi Ameti kommentaari 17.40 vastust ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.3 vastust.
36.14	KüTS § 14 lg 10 p 4 – Teeme ettepaneku see punkt KüTS eelnõust eemaldada, kuna NIS 2 ülevõtmisega ei ole kohustust kehtestada kulude katmise osa, või muuta kõnealuse punkti selliselt, et vastavad kulud katab RIA, kuna tema tellib vastava sihtpärase turvaauditi. Eelnõus oleva sõnastuse puhul ei ole analüüsitud, ka milliseid väljaminekud võiksid kohuslasele tekkida vastava sihtpärase turvaauditiga ning jätab võimaluse RIA-le põhjendamata tellida kohuslasele turvaaudit ja nõuda kohuslasel selle tasumist.	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 24.64 vastust.
37. Eesti Interneti SA arvamus 31.01.2025 kiri nr 2-3/2025-2		
37.1	Eesti Interneti SA hinnangul on domeeninduse valdkond, mida reguleerib eelkõige NIS2 direktiivi	Võetud teadmiseks

	artikkel 28, kohaselt üle võetud EISi Nõukogu poolt ning viidud kooskõlla .ee Domeenireeglite ja Registrilepinguga. Selles osas EIS kooskõlastab seletuskirja lisas 1 vastavustabeli lk 6 art 28 ülevõtmise.	
37.2	NIS2 direktiiv reguleerib domeeninduse valdkonda kolme teenuseosutaja suhtes: domeeninimede registreerimise teenuseid osutavad üksused, tippdomeeninimede registrite pidajad ja domeeninimede süsteemi teenuse osutajad. Viimased kaks teenuseosutajat muutuvad olenemata nende suurusest elutähtsa teenuse üksuseks. Siinkohal peab EIS vajalikuks välja tuua, et kui EIS on käsitletav tippdomeeninimede registri pidajana, siis .ee domeeninimede registreerimine on Eestis korraldatud läbi .ee akrediteeritud registripidajate, keda tegutseb kokku Eestis 24 ja välismaalt lisaks 27. Käesolevas seletuskirjas on aga välja toodud, et domeeninimede registreerimise teenuseid osutavaid üksusi on kokku 10, mis tegelikult ei vasta tõele, sest hetkel teostab EIS kokku 51 akrediteeritud .ee registripidaja teenuse osutamise suhtes järelevalvet läbi nendega sõlmitud Registrilepingu. Seega tegutseb Eestis hetkel kokku 24 domeeninimede registreerimise teenuseid osutavaid üksusi. Samuti olete leidnud, et DNS teenuse osutajaid on Eestis kokku ca 600. Siinkohal pole EISile selge, kust antud numbrid on leitud ja palume selles osas seletuskirjas rohkem põhjendusi. Küll aga on selge, et need 51 akrediteeritud registripidajat muutuvad	Arvestatud ja selgitatud Eelnõu seletuskirjas olev arv 10 oli esialgne Riigi Infosüsteemi Ameti hinnang nende üksuste osas. Seletuskirja on parandatud kommentaaris esitatud arvudega. Esitatud ettepaneku osas juhime tähelepanu NIS2 direktiivi artikli 21 lõike 5 alusel vastu võetud rakendusmäärusele 2024/2690, millega kehtestatakse seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite […] , direktiivi (EL) 2022/2555 kohaldamise eeskirjad, mis puudutavad küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid ja selliste juhtude täpsemat kindlaksmääramist, mille korral peetakse intsidenti oluliseks. Ehk too rakendusmäärus sätestab riskijuhtimismeetmed (eelnõus turvameetmed), mida peavad järgima domeeninimede süsteemi teenuse osutajad kui ka tippdomeeninimede registrid. Seega nimetatud üksused ei pea järgima KüTS § 7 alusel kehtestatud Eesti infoturbestandardit ega selle alternatiiviks olevat rahvusvahelist standardit ISO/IEC 27001. Seda kinnitab ka eelnõu KüTS § 7 lõige 7, mis sedastab, et eelmainitud rakendusaktis mainitud üksus lähtub rakendusaktis mainitud teenuse puhul rakendusaktiga kehtestatud nõuetest. Saame aru, et .ee akrediteeritud registripidajad on hõlmatud domeeninimede registreerimise teenuse osutajate mõistesse ehk tegemist on „tippdomeeninimede registri pidaja nimel tegutseva isikuga, näiteks registreerimisega seotud privaatsusteenuse või proksiteenuse osutaja või edasimüüjaga“. Selgitame, et domeeninimede registreerimise teenuse osutajad ei ole eelnõu kohaselt teenuseosutajad ehk nad ei ole üliolulised üksused ega olulised üksused (avalikul kooskõlastusringil olnud eelnõu sõnastuse mõttes elutähtsad üksused ega olulised üksused). Seega neile ei kohaldata ka KüTS §-s 7 olevaid nõudeid. Samas kohalduvad neile ainult üksikud KüTSi sätted – vt selles osas ka vastava mõiste selgitust eelnõu KüTS §-s 2. Kui oleme valesti aru saanud ning eelmainitud olukorrad ning selgitused ei kehti, siis vt ka Sotsiaalministeeriumi kommentaari 9.1 vastust.

	NIS2 kohaselt elutähtsa teenuse üksuseks, sest lisaks domeeninimede registreerimise teenuste osutamisele läbi Registrilepingu, osutavad nad lõppkliendile ka nimeserveriteenust. Enamasti käib .ee domeenninimede registreerimise teenus käsikäes nimeserveri teenuse osutamisega, sest registripidajad pakuvad lõppkasutajatele enda nimeservreid selleks, et domeen oleks internetis kättesaadav ja kasutatav - tavakasutaja ei oma teadagi kodustes tingimustes servereid. Nii pakuvad EISile teadaolevalt pea kõik .ee akrediteeritud registripidajad ka DNS teenust, mis tähendab, et kõik .ee registripidajad muutuvad sisuliselt elutähtsa teenuse üksuseks. EISi murekoht peitub selles, et enamik .ee akrediteeritud registripidajaid on Eesti turul väikeettevõtjad. Kokku on 28.01.2025 seisuga registreeritud 173 367 .ee domeeni, siis enamik .ee akrediteeritud registripidajast (44 registripidajat) omab enda haldusalas alla 5000 .ee domeeni. Sellest 44st registripidajast pea 9 omab enda haldusalas alla 2000 .ee domeeni. Seega enamik .ee akrediteeritud registripidajatest on Eesti mõistes väikeettevõtjad ja teenindavad ca 2000 - 5000 .ee domeeni, kuid muutuvad NIS2 mõistes elutähtsa teenuse üksuseks ja nendelt plaanitakse nõuda eelnõu järgi muuhulgas enda küberturvalisuse auditeerimist. EISi hinnangul ei ole see proportsionaalne meede, arvestades nende registripidajate suurust ja võimalike küberintsidentide esinemise tõsidust kui ka tõenäosust. Samuti ei ole EIS enda järelevalvet	

	teostades seni tuvastanud, et .ee domeenidega oleks toimunud selliseid Eesti küberturvalisust ohustavaid juhtumeid, mille ühiskondlik ja majanduslik mõju oleks olnud suur. Nii teeb EIS ettepaneku kohaldada kuni 5000 domeeniga .ee akrediteeritud registripidajale samasuguseid reegleid nagu domeeninimede registreerimise teenuse osutajale või minimaalsuse nõuded, mida NIS2 võimaldab. Mõistame, et NIS2 ei võimalda DNS teenuse osutajad olenemata nende suurusest kohaldamisalast välja jätta, kuid EISi hinnangul on NIS2 artiklis 21 selgelt antud seadusandjale võimalus kohaldada teatud juhtudel madalamaid kriteeriume ning meetmeid saab riik hinnata vastavalt proportsionaalsuse põhimõttele: "*Võttes arvesse kaasaegseid ning, kui see on kohaldatav, asjakohaseid Euroopa ja rahvusvahelisi standardeid ja rakendamiskulusid tagatakse esimeses lõigus osutatud meetmetega ähvardavale ohule vastav võrgu- ja infosüsteemide turvalisuse tase. Nende meetmete proportsionaalsuse hindamisel võetakse igakülgselt arvesse üksuse riskidele avatuse määra, üksuse suurust ning intsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.*" Arvestades .ee akrediteeritud registripidajaid, kelle haldusalas on kuni 5000 domeeni, on nende ühiskondlik ja majanduslik mõju oluliselt väiksem, et nendele ei peaks kohaldama kõiki rahvusvahelisi küberturvalisuse standardeid. Samuti ei ole nende üksuste riskidele avatuse määr suur. EISi hinnangul	

	tuleks nendelt nõuda üksnes NIS2 art 21 lg 2 minimaalsete tingimuste täitmist. Seega teeme ettepaneku KüTS eelnõud muuta selliselt, et kuni 5000 domeeniga registripidajalt nõuab seadusandja küll küberturvalisuse riskijuhtimismeetmete tagamist, kuid üksnes minimaalses ulatuses ja piirdudes NIS2 direktiivi artikliga 21 lg 2. EIS palub, et seadusandja rakendab seda viisil, et selleks ei pea väiksemad registripidajad kaasama küberturvalisuse auditeerimist ja saama ISO 27001 või samaväärset sertifikaati, vaid asutus ise dokumenteerib nõutud dokumendid, kuid auditeerimiskohustust ja võimalike trahve sertifikaati mitteomades ei kaasne. Sisuliselt sarnane GDPR määruse nõuete täitmisega, millega ei kaasnenud väiksematele subjektidele auditeerimiskohustust (kuid trahvid nõuete täitmata jätmise suhtes püsivad). Lisaks juhime tähelepanu, et väikeettevõtjatele on ka küberturvalisuse auditeerimise kulust tulenev majanduslik mõju väga suur. Auditeerimiskulu ületab kordades väikeettevõtjate aasta tulu domeeninduse valdkonnas ja mida teenitakse .ee müügist või nimeserveriteenusest. See omakorda tähendab, et säärase kohustuse panemine võib viia väikeettevõtjad sulgemiseni ja läbi mille piiratakse turuolukorda, konkurentsivõimet. See mõjutaks otseselt juba negatiivselt domeenivaldkonda Eestis. **Seega palub EIS KüTS eelnõud muuta ja kuni 5000 domeeniga akrediteeritud .ee registripidajad vabastada rahvusvahelise või**	

	Euroopa küberstandarditele vastamise kohustusest.	
	38. Guardtime arvamus 24.01.2025 e-kiri	
38.1	Palun põhjendada vajadust kohaldada KüTS kõikidele usaldusteenuse osutajatele (palun siin eristada kvalifitseeritud usaldusteenuse osutaja mitte-kvalifitseeritud usaldusteenuse osutajast).	Selgitatud NIS2 direktiiv ise näeb ette, et usaldusteenuse osutajatele kohaldatakse seda, riigisiseselt ei ole võimalik osasid usaldusteenuse osutajaid KüTS kohaldamisalast välja jätta – vt artikkel 2 (2) a) ii). Samamoodi eristab direktiiv, millisesse gruppi vastav usaldusteenuse osutaja satub: kvalifitseeritud usaldusteenuse osutajad on direktiivi art 3 lg 1 punkti b tõttu üliolulised üksused (direktiivi tekstis elutähtsad üksused) ning muud ehk mitte-kvalifitseeritud usaldusteenuse osutajad on direktiivi art 3 lg 2 koosmõjus direktiivi I lisa punkti 8 (digitaristu) alapunktiga 7 olulised üksused.
38.2	Kvalifitseerimata usaldusteenuse pakkuja ei peaks olema kohustatud viima oma protsesse vastavusse standarditega E-ITS või ISO27001, mistõttu palume teha muudatus eelnõusse ja eemaldada mitte-kvalifitseeritud usaldusteenuse osutajad või selgesõnaliselt viidata usaldusteenuse osutajale kui kvalifitseeritud usaldusteenuse osutajale.	Selgitatud Kvalifitseeritud usaldusteenuse osutajatele kohaldub NIS2 direktiivi artikli 21 lõike 5 alusel antud rakendusakt - seetõttu ongi tekitatud eelnõus KüTS § 7 lõige 7.
	39. Riigimetsa Majandamise Keskuse arvamus 23.01.2025 e-kiri	
39.1	RMK kooskõlastab seaduse eelnõu, kuid pöörame tähelepanu järgnevale: 1) Eelnõu § 6^1 muudatus: Seletuskirja kohaselt palub eelnõu koostaja tagasisidet juhatuse koolitustegevuse välba määratluse osas. RMK hinnangul ei ole mõistlik antud välpa seadusesse sisse kirjutada, vaid lahendada organisatsiooni siseselt. 2) Täiendavalt soovime pöörata tähelepanu eelnõu punktidele, mis käsitlevad RIA tegevusi. Nimelt on seaduses väga laialdaselt kirjeldatud RIA	Vastused on esitatud vastavalt esitatud kommentaari punktidele: 1) Arvestatud – siin vt ka Rahandusministeeriumi kommentaari 6.1 vastust. 2) Osaliselt arvestatud – vt siin ka Riigi Infosüsteemi Ameti kommentaari 17.36 vastust. 3) Mittearvestatud ja selgitatud: Eelnõus on tehtud viiteid EL õigusele ja seal olevatele mõistetele - neid ei ole võimalik taasesitada või korrata Eesti õiguses. Euroopa Kohus on märkinud, et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete siseriiklikusse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 07.02.1973 otsuse asjas 39/72: Komisjon vs. Itaalia. EKL 1973, lk 101; 02.02.1977 otsuse asjas 50/76: Amsterdam Bulb BV vs. Produktschap voor Siergewassen. EKL 1977, lk 137).

	ülesandeid. RMK ettepanek on RIA-ga seotud ülesannete täpsustamine viia asutuse põhimäärusesse ning eelnõus kajastada vaid olulisemat ehk RIA õigust sekkumiseks. 3) Õigusselguse huvides, soovitame vähendada eelnõus EL-õigusaktide viiteid ning neid rohkem lahti kirjutada, mis tagab eelnõu selguse ja ühtse arusaama.	Olukorras, kus termini definitsioon on esitatud EL määruses, tuleb definitsioon ka riigisisese õiguse kohaselt esitada viiteliselt (Vabariigi Valitsuse 22.12.2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 18 lg 2). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte - siin on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja EL õiguse vahel.
40. Eraisiku arvamus 24.01.2025 e-kiri		
40.1	Teen ettepaneku KüTS muutmise seaduse (NIS2 ülevõtmine) § 1 lg 1^5 punkt 9 eelnõust täies mahus kustutada. Põhjendusena, et punkti säilitamise põhjendused on ära langenud või väärad. Kehtiv KüTS § 3 lg 1 p 7 (seletuskirjas vale viide lõikele 3) ei tulene esialgse NIS1 direktiivi ülevõtmise vajadusest ning seda polnud 2018. aastal välja töötatud seaduseelnõus. Kõik perearstid lisati nimekirja 597 SE II lugemisel. Riigikogu seletuskirja järgi oli riigikaitsekomisjoni muudatusettepaneku eesmärk järgmine: *Kui statsionaarne eriarstiabi oli varasemalt elutähtis teenus, siis küberturvalisuse tagamise kohustusi peavad tulevikus järgima ka perearstid üldarstiabi osutamisel. Perearstide puhul on vajalik ühtlustada nende poolt kasutatavate infosüsteemide turvanõudeid vältimaks näiteks isikuandmete lekkeid või andmete krüpteerimist lunavara rünnakute käigus. Paljudel perearstidel on nimistus sadu, kui mitte tuhandeid inimesi ning võimalus sellises mahus isikuandmete lekkimiseks*	Vt Sotsiaalministeeriumi kommentaari 9.1 vastust.

	küberrünnaku käigus, on tänapäeval täiesti arvestatav. Nagu näha lisati kõik perearstid nimekirja, kuna eeldati, et nende osutatav teenus on võrdväärne elutähtsa teenusega ning see oli riigikogu komisjoni kaalutlusotsus ega tulenenud NIS1 direktiivist. Ka NIS2 direktiiv hõlmab arstiabi osutajad skoopi klausliga, et neile kehtib keskmise või suure ettevõtja klausel (artikkel 2, punkt 1). Neid ei pea skoopi hõlmama olenemata suurusest. Kuna nüüd on hädaolukorra seaduse alusel välja toodud (või plaanitakse välja tuua) elutähtsat teenust osutavad perearstikeskused, ei ole 597 SE II seletuskirja järgne põhjendus kõigi perearstide puhul enam pädev ega kehtiv. Perearstide kaasamisel olenemata suurusest on eelnõus viidatud, et nad vastavad kaalutlusotsuse alusel vähemalt ühele punktidest 1^4 punkt 1,2,3,4. Paraku ei õnnestu tuvastada, millise punkti alusel perearstid sinna sisse on siis arvatud. On suhteliselt ilmne, et väga väikse perearstinimistu kompromiteerimine ei ole kriitilise ühiskondliku tähtsusega, teenuse häire puhul ei ole olulist mõju rahva tervisele, süsteemset ja piiriülest mõju pole ning piirkondlikul tasandil pole tegemist kriitilise tähtsusega teenusliigiga. Seda kõike tõendab veelkord riigi kavatsus määrata piirkondades elutähtsat teenust osutavad perearstid, mis seletuskirja järgi on ainult 5% üldarstiabi osutajatest, mitte eranditult kõik.	

	Seaduse soov perearstiteenuse turvataset tõsta on arusaadav. Soome Valvira kasutab selleks nt tervisetarkvarade sertifitseerimise skeemi, kus terviseandmetele saab ligi ainult sertifitseeritud tarkvara kasutades. Sarnase skeemi kasutamisel ka Eestis oleks võimalik perearstidel näiteks otsida turvanõuetele vastav SaaS-pilveteenuse osutaja, kelle teenus tagaks andmete turvalisuse. Seejuures jääks ära E-ITS või ISO-ga kaasnev bürokraatia, mis ei ole väikestes perearstipraksistes mõistliku pingutusega ja praeguse tegutsemismudeliga saavutatav.	