Justiits- ja Digiministeerium

Suur-Ameerika 1, Tallinn

info@justdigi.ee

 Meie: 31.01.2025

**Tagasiside küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõule**

Lugupeetud Justiits- ja Digiministeerium

Käesolevaga edastab Eesti Energia AS enda ettepanekud ja kommentaarid küberturvalisuse seaduse (edaspidi KüTS) eelnõule.

1. Esmalt juhime tähelepanu järgnevatele üldistele KüTS eelnõu kitsaskohtadele:
	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.
	2. Kuna KüTS eelnõuga (i) luuakse uusi täiendavaid kohustusi (nt KüTS § 7 lg 21 p 1) ja (ii) muudetakse KüTS rakendamine kohustuslikuks elutähtsa 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 elutähtsateenuse 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).
	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 13 punktis 3 tooduga. St soovitame määrata lõplikuks ajaks 18. oktoober 2029. aasta.
	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 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.
2. Teiseks edastame omad kommentaarid ja ettepanekud järgmiste KüTS eelnõu paragrahvide osas:
	1. **KüTS § 12 lg 39 ja lg 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.
	2. **KüTS § 2** - soovitame vaadata üle ja täpsustada järgnevad mõisted:
		1. 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.
		2. **KüTS § 2 lõikes 33**on mõiste „**risk“**. Teeme ettepaneku see mõiste defineerida järgmiselt:
3. variant - „risk“ – vaatlusaluse ohu potentsiaal ära kasutada mingi vara või vararühma nõrkusi ja tekitada seeläbi kahju;
4. variant - „risk“- võimalus, et küberintsidendi läbi tekib kahju või tõrge, väljendatakse kahju ulatuse mõju hinnangu ja realiseerumise esinemise võimalikkuse kombineeritud näitajana.
	* 1. **KüTS § 2 lõikes 35** on mõiste „**oluline küberoht“.** Palume seda mõistet vähemalt seletuskirjas 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).
		2. **KüTS § 2 lõikes 36** 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).
	1. **KüTS § 3 lg 31**- 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?
	2. Täiendavalt palume täpsustada, mida mõistetakse IP aadresside vahemiku all ja mis on selle eesmärk.
	3. **KüTS § 52 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.
	4. **KüTS § 61 lg 2 ja 3** – teeme ettepaneku, et juhtkonna koolitamine peaks toimuma riigi enda poolt (nt RIA), kuna sellega tagatakse, et koolitusel 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.
	5. **KüTS § 7 lg 21 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.
	6. **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.
5. Juhul kui eeltoodud kommetaaride või ettepanekute osas jääb midagi arusaamatuks, siis oleme lahkesti nõus Teiega koostööd tegema ja probleemkohti selgitama, et leida parim lahendus.

Lugupidamisega

Kaarel Tammiste

Õigusteenistuse juht

Eesti Energia AS

Kontakt:

Jekaterina Agu, õigusteenistuse kesksete teenuste valdkonnajuht

Mob: 58027169

e-mail: jekaterina.agu@energia.ee