EESTI VEE-ETTEVÕTETE LIIT

ALATES 1995

Pr Liisa-Ly Pakosta
justiits- ja digiminister
Justiits- ja Digiministeerium
info@justdigi.ee

Meie: 31.01.2025 nr 2-2/170

Tagasiside küberturvalisuse seaduse ja teiste seaduste muutmise seadusele (küberturvalisuse 2. direktiivi ülevõtmine)

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.

Alljärgnevalt esitame oma ettepanekud eelnõule punktide kaupa:

1. 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 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.

2. 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.

Eesti Vee-ettevõtete Liit
Registrikood: 80091146
Järvevana tee 3, 10132 Tallinn
Tel: (+372) 511 5154
evel@evel.ee, www.evel.ee

Palume täpsustada eelnõus või vähemalt selgitada seletuskirjas, millised on need turvameetmed, mida teenuse osutaja peaks koostööpartneri lepingus 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)?

3. 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.

4. 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 KüTS § 8 lg 11 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.

5. 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 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

Eesti Vee-ettevõtete Liit
Registrikood: 80091146
Järvevana tee 3, 10132 Tallinn
Tel: (+372) 511 5154
evel@evel.ee, www.evel.ee

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?

6. 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?

Lugupidamisega

/allkirjastatud digitaalselt/

Raili Kärmas
Tegevjuht