RIIGI INFOSÜSTEEMI AMET

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

Teie 09.12.2024 nr 2-2/3131-1

Meie 31.01.2025 nr 1.1-20/251955

Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) kooskõlastamine

Austatud justiits- ja digiminister

Täname võimaluse eest esitada tagasisidet küberturvalisuse seaduse (KüTS) ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine). Teeme eelnõu teksti järgnevad märkused.

1. Terminoloogia

Eelnõu üleselt teeb Riigi infosüsteemi Amet ettepaneku kirjutada seaduses kasutatavad mõisted ja terminid lahti. Termonoloogiat 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.

1.1 Teeme ettepaneku läbivalt eelnõu § 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.

1.2 Eelnõu § 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 „laadimispunkti käitaja“ läbi ELTS tähenduse, võimalusel ELTS muudatusena.

1.3 Eelnõu § 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“.

1.4 Eelnõu § 1 lg 1^2 punktid 10-15 on võimalik läbivalt asendada maagaasiseaduse § 4 välja toodud „gaasiettevõtja“ mõistega.

1.5 Eelnõu § 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.“.

1.6 Eelnõu § 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 defineerida eelnevalt LennS-s, et tagada õigusselgus. Samuti palume seletuskirjas välja tuua kaalutlused, miks just need isikud/ettevõtted loetakse mõiste alla kuuluvaks.

1.7 Eelnõu § 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.

1.8 Eelnõu § 1 lg 1^2 punktid 2^2-2^3 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.

1.9 Eelnõu § 1 lg 1^2 punktid 48-50 ning eelnõu § 1 lg 1^3 p 1 võiks kaaluda näiteks „internetipõhise kauplemiskoha pakkuja“ asemel „internetipõhise teenuse osutaja“ kasutamist. Sama analoogiat võiks kasutada ka teiste välja toodud punktide subjektide osas.

1.10 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 § 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.

1.11 Teeme ettepaneku vaadata üle eelnõu § 2 p 1. Eelnõu sõnastuse kohaselt on ka füüsiline isik asutatud.

1.12 Teeme ettepaneku vaadata üle, kas on eraldi vaja mõistetena tuua eelnõu § 2 p 12 ning p 13 „keskvalitsuse avaliku halduse üksus“ ning „kohaliku tasandi avaliku halduse üksus“. Antud mõisteid on kasutatud eelnõu § 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.

1.13 Teeme ettepaneku eelnõu § 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.

1.14 Palume eelnõu § 5 lg 4 p-s 2 või selle mida on mõeldud “nõrga lüli” all, et seda oleks võimalik vältida.

1.15 Teeme ettepaneku selgitada täpsemalt, mida peetakse silmas eelnõu § 5 lg 5 p 7 mõiste „reaalajalähedase seire“ all.

1.16 Teeme ettepaneku sõnastada eelnõu § 5 lg 5 p 9 järgmiselt:
„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*.“.

1.17 Teeme ettepaneku sõnastada eelnõu § 5 lg 5 p 10 järgmiselt:
„10) kogub ja analüüsib digitaalkriminalistika-andmeid, analüüsib järjepidevalt riske ja küberintsidente, ning tagab küberturvalisuse alast olukorrateadlikkust.“.

1.18 Teeme ettepaneku selgitada eelnõu § 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.“.

1.19 Kavandatava 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.

1.20 Kavandatava eelnõu § 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.

1.21 Teeme ettepaneku tuua terminite loetelus välja “turvarikkemärk”, mida kasutatakse kavandatava eelnõu § 8 lg 4^1 p-s 1.

1.22 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.

1.23 Teeme ettepaneku kaaluda terminite esitamist tähestikulises järjekorras, et hõlbustada lugemist.

2. Seaduse subjektide selgem määratlemine

2.1. 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.

2.2. Teeme ettepaneku koondada kõik 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).

2.3. Seletuskirjast ei tulene, mis kaalutlustel on välja jäetud erakapitalil põhinev 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.

2.4. Teeme ettepaneku lisada seaduse 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 § 1 lg 1^1 või alternatiivselt avada seletuskirjas üheselt arusaadavad kaalutlused, miks tehakse eelnõus erisus erinevate tervishoiuteenuse osutajate vahel.

3. Eelnõu sõnastuslikud ettepanekud

Eelnõu tekst sisaldab erinevaid nõudeid, mille täitmine vajab meie hinnangul täpsustamist:

3.1. Teeme ettepaneku sõnastada eelnõu § 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.

3.2. Teeme ettepaneku sõnastada eelnõu § 1 lg 1^6 järgmiselt:
„(1^6) Vabariigi Valitsus võib käesoleva paragrahvi lõike 1^4 kriteeriumitest lähtuvalt määrata määrusega valdkonna või sektori, milles oleva üksuse suhtes kohaldatakse teenuse osutaja kohta sätestatut olenemata tema suurusest.“. Kui jäädakse üksuse sõnastuse juurde, siis siin on ilmselt silmas peetud üksust, mitte isikut.

3.3. Teeme ettepaneku ühildada omavahel eelnõu § 1 lõiked 1^3 ja 1^5. Mõlemas lõikes teenuse osutajate suhtes kohaldatakse käesolevat seadust olenemata nende suurusest.

3.4. Pöörame tähelepanu, et eelnõu § 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.

3.5. Teeme ettepaneku vaadata üle eelnõu § 3 lg 1^2 p 10 sõnastus. Bilansimaht peaks ületama 43 miljonit eurot ning aastakäive 50 miljonit eurot ehk vastupidi eelnõus sõnastatule.

3.6. Palume eelnõu § 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 § 4 lg 1 p 1-6 nimetatud andmete esitamise ning § 4 lg 1^2 tuleneva RIA-le pandud kohustuse täitmise korral.

3.7. Palun täpsustada eelnõu § 4 lõige 1 p 2 mõistet „asjakohasel juhul“. Hetkel jääb sättes ebamääraseks, mida täpsemalt teenuse osutajalt nõutakse.

3.8. Teeme ettepaneku jätta välja eelnõu § 5 lg 4 p 1-9 sätestatu ning lisada see Riigi Infosüsteemi Ameti põhimäärusesse, kuna sätted loetlevad RIA struktuuriüksuse ülesandeid.

3.9. Teeme ettepaneku sõnastada eelnõu § 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.

3.10. Teeme ettepaneku sõnastada eelnõu § 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 Regulaarselt/vähemalt kord x aasta jooksul sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“.

3.11. Teeme ettepaneku sõnastada eelnõu § 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 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 justkui täidetud, kuid turve ei paraneks, kui meetmete rakendamist ei toimu.

3.12. Teeme ettepaneku kustutada eelnõu § 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.

3.13. Teeme ettepaneku sõnastada eelnõu § 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.

3.14. Teeme ettepaneku sõnastada eelnõu § 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.

3.15. Teeme ettepaneku sõnastada eelnõu § 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.

3.16. Teeme ettepaneku sõnastada eelnõu § 7 lg 2^3 järgmiselt: „(2^3) Kui teenuse osutaja tuvastab, et 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.

3.17. Teeme ettepaneku täpsustada eelnõu § 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. 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.

3.18. 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.

3.19. Teeme ettepaneku sõnastada eelnõu § 8 lg 10 järgmiselt:
„(10) Julgeolekuasutus teavitab küberintsidendist asjakohast julgeolekuasutust, arvestades käesolevas paragrahvis sätestatud nõudeid.“;

3.20. Teeme ettepaneku vaadata üle eelnõu § 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.

3.21. Teeme ettepaneku vaadata üle eelnõu § 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 sästestatud nõudeid ning antud juhul ei ole vajalik tuua eraldi välja §-ides 7 ja 8 sätestatud nõudeid.

3.22. Teeme ettepaneku vaadata üle eelnõu § 14 lg 6 p 4. Antud õigus on korrakaitseorganil ka kehtivas õiguses.

3.23. Teeme ettepaneku vaadata üle eelnõu § 14 lg 7 ja 8 vajalikkus, kuivõrd antud põhimõtted tulenevad KüTS'i jaoks eriseadustest. Näiteks haldusmenetluse seadus, väärteomenetluse seadus jne.

3.24. Teeme ettepaneku vaadata üle eelnõu § 14 lg 9 p 1, p 4-9. Tegemist on sätetega, mille teostamise õigus on juba kehtivate seadustega RIA-l olemas.

3.25. Teeme ettepaneku sõnastada eelnõu § 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.“

3.26. Teeme ettepaneku sõnastada eelnõu § 14 lg 10 p 2 järgmiselt: „2) viib läbi sõltumatu organisatsioon või Riigi Infosüsteemi Amet;“.

3.27. Teeme ettepaneku vaadata üle eelnõu § 14 lg 11 ja lg 12 vajalikkus. Antud õigus on korrakaitseorganil ka kehtiva õiguse alusel.

3.28. Teeme ettepaneku võtta eelnõu § 15 lg 2 sõnastusest välja viide Euroopa Liidu õigusele ja vajadusel täiendada vastava sisuga seadust.

3.29. Teeme ettepaneku eelnõu § 18^4 täiendamiseks. Teeme ettepaneku laiendada seaduse nõuete rikkumisel teenuse osutaja juhtorgani või juhtorgani liikme poolset vastutust. Kehtiva seaduse § 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 seaduse § 18 lg 1 nõuete rikkumise korral analoogse karistuse määramise võimaluse. Hetkel on selline võimalus sätestatud piiratult eelnõu § 18^4 kontekstis eelnõu § 6^1 nõuete rikkumise eest.

3.30. Teeme ettepaneku eelnõu § 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.

3.31. Teeme ettepaneku eelnõu § 18^6 lõiked 1 ja 2 asendada „füüsilisest isikust seadusliku esindaja poolt „seadusliku esindaja poolt“. Seaduslik esindaja saab olla ainult füüsiline isik.

3.32. Teeme ettepaneku täiendada eelnõu § 19 lg 2 sõnastust. Kuivõrd antud ülesanne on Andmekaitse Inspektsiooni pädevuses. Seega peaks antud juhul kohtuväliseks menetlejaks olema Aandmekaitse Inspektsioon.

4. Üldised küsimused ja kommentaarid

4.1. 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.

4.2. 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.

Lugupidamisega

(allkirjastatud digitaalselt)

Joonas Heiter
peadirektor

Sander Pelisaar
Sander.Pelisaar@ria.ee