17.09.2021

Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõu seletuskiri

1. Sissejuhatus

Eelnõuga korrastatakse teenuse osutajate ja avaliku sektori võrgu- ja infosüsteemide turvalisust reguleerivat õigusruumi ning rakendatakse kahte Euroopa Parlamendi ja nõukogu määrust – Euroopa Parlamendi ja nõukogu määrust (EL) nr 2019/881, mis käsitleb ENISA-t (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 07.06.2019, lk 15–69; edaspidi *küberturvalisuse määrus*) ning Euroopa Parlamendi ja nõukogu määrust (EL) nr 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus (edaspidi *pädevuskeskus*) ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 08.06.2021, lk 1-31; edaspidi *küberturvalisuse TTT määrus*).

1.1. Sisukokkuvõte

1.1.1. Kavandatav muudatus: E-ITS-i kehtestamine

Küberturvalisuse seaduse (edaspidi *KüTS*) ja teiste seaduste muutmise seaduse eelnõuga (edaspidi *eelnõu*) volitatakse Vabariigi Valitsust määrusega kehtestama süsteemide küberturvalisuse tagamiseks vajalikke nõudeid, millest üks osa on uus väljatöötamisel olev Eesti Infoturbestandard (edaspidi *E-ITS*). Muudatuste käigus tunnistatakse kehtetuks ka Vabariigi Valitsuse määruse volitusnorm avaliku teabe seaduses (edaspidi: AvTS) infosüsteemide turvameetmete süsteemi kehtestamiseks. Muudatustega kaasajastatakse ning viiakse infoturbe tagamine andmekogude põhiselt lähenemiselt võrgu- ja infosüsteemide (edaspidi *süsteem*) lähenemisele. Seega võimaldab muudatus aegunud infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi *ISKE*) asendada uue E-ITS-ga.

ISKE aluspõhimõtted, rakendamise loogika ning auditeerimise skeemid ei ole selle esmasest avaldamisest aastal 2003 alates ehk 17 aasta jooksul muutunud. E E-ITS-i volitusnorm on laiem kui andmekogude põhise ISKE oma – see lähtub võrgu- ja infosüsteemidest ning kohaldub kõikidele süsteemidele, sealhulgas andmekogudele AvTS-i tähenduses. E-ITS-i määrus planeeritakse vastu võtta aastal 2021, mistõttu on vajalik sellele eelnevalt volitusnormi uuendamine.

E-ITS-i määruse volitusnormi paiknemine KüTS-s ja selle rakendusaktides on avaliku teabe töötlemist ja küberturvalisust reguleerivaid õigusakte, nende omavahelisi seoseid ning struktuuri arvesse võttes mõistlik. Just KüTS-i eesmärgiks on ühiskonna toimimise seisukohast oluliste riigi ja kohaliku omavalitsuse üksuste süsteemide turvalisuse tagamine ning küberintsidentide ennetamise ja lahendamise koordineerimine (KüTS § 1 lg 1 kehtiv sõnastus).

Lisaks on praegu infosüsteemide turvameetmete süsteemi puudutav regulatsioon Justiitsministeeriumi vastutusalas, kuigi küberturvalisusega seotud regulatsioonid on Majandus- ja Kommunikatsiooniministeeriumi (edaspidi *MKM*) valitsemisalas. MKMi

haldusalas tegutseva Riigi Infosüsteemi Ameti (edaspidi *RIA*) põhimääruse kohaselt on RIA üks põhiülesannetest korraldada infosüsteemide turvameetmete süsteemi arendamist ja koordineerida infoturbemeetmete rakendamist. Seetõttu tehakse lisaks volitusnormi asukoha muutmisele ka täiendus Vabariigi Valitsuse seadusesse, mille tulemusena reguleeritakse selgelt, et MKMi valitsemisalas on avaliku sektori digiarengu ja üleriigilise küberturvalisuse tagamise juhtimine, korraldamine ja järelevalve.

1.1.2. Kavandatav muudatus: küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramine ja sellega seotud ülesannete korraldus

Eelnõuga rakendatakse küberturvalisuse TTT määrust. Eelnõuga sätestatakse volitusnorm, mille tulemusena on võimalik valdkonna eest vastutava ministri käskkirjaga määrata pädevuskeskuse nõukogu esindaja ja asendajaliige.

Eelnõuga määratakse ka, kes teostab sama määruse tähenduses riikliku koordineerimiskeskuse ülesandeid. Eelnõuga sätestatakse KüTS-s, et riikliku koordinatsioonikeskuse ülesandeid täidab Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuseks (edaspidi *TTT üksus*) määratud isik. Eelnõu ning selle lisaks oleva määruse kavandi järgselt määratakse TTT üksuseks RIA.

1.1.3. Kavandatav muudatus: küberturvalisuse sertifitseerimise korralduse reguleerimine

Eelnõuga rakendatakse ka küberturvalisuse määrust. Tegemist on otsekohalduva õigusaktiga, mis sisaldab sätteid, mille osas liikmesriikidel on kaalutlusõigus ning mis vajavad liikmesriigi õiguses reguleerimist.

KüTS-s ega muudes seadustes ei ole reguleeritud sertifitseerimist IKT-toodete, -teenuste ja protsesside valdkonnas. Seetõttu on KüTS-i muutmise eesmärgiks täita küberturvalisuse määruse artiklis 58 ja 65 liikmesriigi ülesannetena sätestatud kohustused, milleks on vastavalt riikliku küberturvalisuse sertifitseerimise asutuse määramine ning küberturvalisuse sertifitseerimise kavade rikkumise korral karistusnormide kehtestamine.

Eelnõuga sätestatakse riikliku küberturvalisuse sertifitseerimise asutusena Tarbijakaitse ja Tehnilise Järelevalve Amet (edaspidi *TTJA*) ning tema järelevalvevolitused. TTJA täidab tulevikus eelnõu kohaselt riikliku ja haldusjärelevalve ülesandeid küberturvalisuse määruses sätestatud nõuete täitmiseks. Riiklik küberturvalisuse sertifitseerimise asutus toetab akrediteerimisasutust, teostab järelevalvet vastavushindamisasutuse tegevuse üle ning riikliku vastavushindamisasutuse üle, kes annab vajadusel välja kõrgema taseme sertifikaate. Vastavate nõuete rikkumise korral on eelnõu kohaselt ette nähtud väärteokaristused, millede kohtuväliseks menetlejaks on samuti TTJA.

1.2. Eelnõu ettevalmistajad

Eelnõu ja seletuskirja koostasid Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse õigusnõunikud Raavo Palu (raavo.palu@mkm.ee) ja Oliver Grauberg (oliver.grauberg@mkm.ee) ning Riigi Infosüsteemi Ameti õigusosakonna juhataja Kristiina Laanest (kristiina.laanest@ria.ee) ja õigusnõunik Silver Lusti (silver.lusti@ria.ee). Eelnõu keelelise ekspertiisi teostas Majandus- ja Kommunikatsiooniministeeriumi riikliku küberturvalisuse osakonna küberturvalisuse

õigusnõunik Raavo Palu (raavo.palu@mkm.ee). Eelnõu ja seletuskirja osas tegi õiguslikke ettepanekuid õigusosakonna õigusnõunik Ave Henberg (ave.henberg@mkm.ee).

1.3. Märkused

Süsteemide turvameetmete, sh E-ITSi kehtestamiseks seotud muudatused ei ole seotud muu menetluses oleva eelnõuga ega Euroopa Liidu õiguse rakendamisega.

Eelnõuga viiakse Eesti õigus kooskõlla Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/887. Nimetatud määruse artikli 6 lõike 1 kohaselt määrab iga liikmesriik 29. detsembriks 2021. a ühe sama artikli lõike 5 nõudeid täitva asutuse, kes hakkab nimetatud määrust kohaldama riikliku koordinatsioonikeskusena.

Eelnõuga viiakse Eesti õigus kooskõlla Euroopa Parlamendi ja nõukogu määrusega (EL) nr 2019/881. Nimetatud määruse artikli 69 lõike 2 kohaselt kohaldatakse alates 28. juunist 2021. a sama määruse artikleid 58, 60, 61, 63, 64 ja 65. Eelnõu on seotud osade mainitud artiklite rakendamisega. Määruse nr 2019/881 tõttu on eelnõul seos toote nõuetele vastavuse seaduse ning seal viidatud Euroopa Parlamendi ja nõukogu määrusega (EÜ) nr 765/2008.

Eelnõu ei ole seotud muu menetluses oleva eelnõuga ega muu Euroopa Liidu õiguse rakendamisega. Eelnõul on teatav seos Vabariigi Valitsuse tegevusprogrammi ühe alaeesmärgiga, konkreetsemalt tegevusprogrammi alapunktiga nr 6.24: tagame, et Eesti on küberkaitstud riik ja teeme selleks tihedat koostööd liitlastega.

Eelnõuga muudetakse:

- küberturvalisuse seadust redaktsiooniga RT I, 22.05.2018;
- avaliku teabe seadust redaktsiooniga RT I, 15.03.2019, 11;
- elektroonilise side seadust redaktsiooniga RT I, 10.12.2020, 6;
- hädaolukorra seadust redaktsiooniga RT I, 18.06.2021, 3 (mis jõustub 01.01.2022);
- lennundusseadust redaktsiooniga RT I, 10.12.2020, 14;
- raudteeseadust redaktsiooniga RT I, 30.03.2021, 8;
- sadamaseadust redaktsiooniga RT I, 31.05.2021, 5;
- tervishoiuteenuste korraldamise seadust redaktsiooniga RT I, 18.06.2021, 9 (mis jõustub 01.01.2022);
- Vabariigi Valitsuse seadust redaktsiooniga RT I, 18.06.2021, 12.

Kehtiva küberturvalisuse seaduse rakendussätete muudatuste tõttu tehakse muudatused Eesti Rahvusringhäälingu seaduses (redaktsiooniga RT I, 22.12.2020, 5, mis jõustub 01.01.2022) ning tervishoiuteenuste korraldamise seaduses (redaktsiooniga RT I, 18.06.2021, 9, mis jõustub 01.01.2022).

Eelnevalt loetletud seaduste osas on Riigikogus menetluses või eelnõude infosüsteemis kooskõlastusel järgnevad seadused, millede sisu ei mõjuta käesolevat eelnõud:

- avaliku teabe seaduse puhul – Riigikogus on riigisaladuse ja salastatud välisteabe seaduse ning avaliku teabe seaduse muutmise seadus 410 SE ning avaliku teabe seaduse muutmise seadus 409 SE;
- elektroonilise side seaduse puhul – Riigikogus on elektroonilise side seaduse, ehitusseadustiku ja riigilõivuseaduse muutmise seadus 301 SE ning meediateenuste seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 327 SE;

- hädaolukorra seaduse puhul – eelnõude infosüsteemis on hädaolukorra seaduse muutmise seadus, konkreetsemalt selle seaduse muutmise seaduse väljatöötamiskavatsus (toimik nr 21-0172);
- lennundusseaduse puhul – eelnõude infosüsteemis on lennundusseaduse ja riigilõivuseaduse muutmise seadus (toimik nr 20-1044) ning lennundusseaduse ja relvaseaduse muutmise seadus (toimik nr 21-0870);
- sadamaseaduse puhul - eelnõude infosüsteemis on sadamaseaduse, meresõiduohutuse seaduse ja riigilõivuseaduse muutmise seadus (toimik nr 21-0383);
- tervishoiuteenuste korraldamise seaduse puhul – eelnõude infosüsteemis on tervishoiuteenuste korraldamise seaduse ja teiste seaduste muutmise seadus (toimik 20-1346) ning tervishoiuteenuste korraldamise seaduse, inimgeeniuuringute seaduse ja teiste seaduste muutmise eelnõu väljatöötamise kavatsus (toimik nr 21-0897);
- Vabariigi Valitsuse seaduse puhul – eelnõude infosüsteemis on Vabariigi Valitsuse seaduse muutmise seaduse eelnõu väljatöötamiskavatsus (toimik nr 20-0232).

Küberturvalisuse seaduse muutmiseks on eelnõude infosüsteemis kaks toimikut (nr-d 21-0125 ja 21-0684; vastutajateks MKM), millede sisu viiakse kokku käesolevasse eelnõusse ning ühe toimiku (nr 21-0125) alla.

Kuna eelnõuga muudetakse Vabariigi Valitsuse seadust, vajab eelnõu Eesti Vabariigi põhiseaduse § 104 punkti 8 tõttu seadusena Riigikogus vastuvõtmiseks Riigikogu koosseisu häälteenamust.

Eelnõule ei eelnenud seaduseelnõu väljatöötamiskavatsuse ja kontseptsiooni koostamist, kuna eelnõu käsitleb Euroopa Liidu õiguse rakendamist ning ISKE aegumisest tulenevalt on E-ITS'i kehtestamise vajadus kiireloomuline.

2. Seaduse eesmärk

Seaduse eelnõul on kolm peamist eesmärki:

1. ajakohastada küberturvalisuse seadust, et oleks võimalik kehtestada E-ITS ja muud ajakohastatud süsteemide küberturvalisuse nõuded ning seeläbi suurendada nende küberturvalisust;
2. reguleerida küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute riiklik koordineerimiskeskuse määramine ning selle ülesannete korraldus;
3. määratleda riiklik küberturvalisuse sertifitseerimise asutus, selle asutuse järelevalvevolitused ning sertifitseerimise nõuete rikkumisega seotud vastutus.

2.1. Eesti Infoturbestandardi kehtestamine

Seaduse eesmärk on uuendada infosüsteemide turvameetmete volitusnormi, et võimaldada vananenud andmekogudele keskendunud turvameetmete süsteemi ajakohastamine. Olukord, mida soovitakse saavutada, võimaldaks ühtsetel põhimõtetel paindlikult ja rakendajatele arusaadavalt rakendada tänapäevastele vajadustele vastavat turvameetmete süsteemi avalike ülesannete täitmiseks loodud äriprotsessidele.

Eesti infoturbealases õigusruumis on probleemiks üksnes andmekogudele fokusseeritud infoturbeparadigma, mis vajab lahendamist. Kehtiv regulatsioon on üles ehitatud andmekogude põhisele infoturbe tagamise süsteemile. ISKE-t rakendatakse andmekogudes sisalduvate

andmete töötlemiseks kasutatavatele infosüsteemidele ja seega keskendub ISKE kitsalt andmekogudes sisalduvate andmete kaitsmisele. See lähenemine on loonud olukorra, kus turvameetmete rakendamisel on rakendaja perspektiiv sageli ebaproportsionaalselt kitsas, jättes turvameetmed rakendamata paljude oluliste infosüsteemide osas, mis ei kujuta AvTS-i tähenduses andmekogu.

Asutused on praktikas sageli jätnud ISKE rakendamata, kui võrgu- ja infosüsteemi defineerimiseks oli võimalik leida mistahes muu definitsioon, kui „andmekogu" AvTS-i tähenduses. KüTS-i jõustumine küll leevendas olukorda, tuues Eesti õigusesse oluliselt laiema „võrgu- ja infosüsteemi (süsteemi)" termini koos sellega kaasneva riskianalüüsi nõudega, kuid KüTS süsteemide osas eriregulatsiooni kehtestamine AvTS-i määrusesse ei ole täna võimalik. Õigusselguse ja infosüsteemide turvalisuse tagamise huvides on siiski erisused andmekogude ning teiste süsteemide osas selgelt välja tuua ja korrektselt reguleerida.

Infoturbe rakendamata jätmine ei ole tänases küberturbereaalsuses riigi ja kohaliku omavalitsuse üksuste süsteemide puhul aktsepteeritav. E-ITS loomisega soovitakse tänast olukorda muuta, tõstes andmeid töötleva süsteemi asemel turvameetmete rakendamise fookusesse avaliku ülesannet täitev organisatsioon, mille eesmärk on pakkuda otseseid avalikke teenuseid ja tugiteenuseid. Andmekogude pidamiseks kehtestatud turvameetmete süsteemilt üleminek organisatsiooni ja tema süsteemide põhisele infoturbe haldussüsteemile tuleb sätestada ka õigusaktides.

Eelnevale tuginedes on vältimatult vajalik luua uus regulatsioon, mis mh asendaks tänast AvTS § 43^9 lõike 1 punkt 4 volitusnormi. Eelnõuga täiendatakse KüTS-i ning muudetakse AvTS-i, mis loob eeldused ühtse ja ühetaolise süsteemide infoturbe haldussüsteemi rakendamiseks. Sama volitusnormiga on ka võimalik sätestada ka muid üldiseid nõudeid, mis kehtivad kõikidele KüTS-i mõistes teenuse osutaja süsteemidele.

2.2. Küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramine ja sellega seotud ülesannete korraldus

Euroopa Liidus on rohkesti eksperditeadmisi ja kogemusi küberturvalisuse teadusuuringute, tehnoloogia ja tööstusarengu alal, kuid tööstus- ja teaduskogukondade jõupingutused on killustatud ja ühtlustamata ning neil puudub ühine missioon, mis piirab konkurentsivõimet ning võrkude ja süsteemide tõhusat kaitsmist selles valdkonnas. Need jõupingutused ja eksperditeadmised tuleb koondada ja võrgustada ning neid tuleb kasutada tõhusalt, et tugevdada ja täiendada olemasolevat teaduslikku, tehnoloogilist ning tööstuslikku võimekust ja oskusi liidu ning liikmesriikide tasandil.[1]

Sellise pädevuskeskuse ja võrgustiku loomine, millel on volitused võtta meetmeid tööstustehnoloogia toetamiseks ning teadusuuringute ja innovatsiooni valdkonnas, on kõige sobivam viis küberturvalisuse TTT määruse eesmärkide saavutamiseks, pakkudes ühtlasi suurimat majanduslikku, sotsiaalset ja keskkonnamõju ning kaitstes seejuures liidu huve.[2]

Pädevuskeskus peaks olema liidu peamine vahend, et koondada küberturvalisuse teadusuuringutesse, tehnoloogiasse ja tööstusarengusse tehtavad investeeringud ning rakendada asjakohaseid projekte ja algatusi koos võrgustikuga. Pädevuskeskus peaks haldama Euroopa

[1] Euroopa Parlamendi ja nõukogu määrus (EL) nr 2021/887, pp 7.
[2] Euroopa Parlamendi ja nõukogu määrus (EL) nr 2021/887, pp 13.

Parlamendi ja nõukogu määrusega (EL) nr 2021/695 loodud teadusuuringute ja innovatsiooni raamprogrammist „Euroopa horisont“ (edaspidi *programm „Euroopa horisont“*) ning Euroopa Parlamendi ja nõukogu määrusega (EL) nr 2021/694 loodud programmist „Digitaalne Euroopa“ antavat küberturvalisusega seotud rahalist toetust ning olema asjakohasel juhul avatud muudele programmidele. See käsitusviis peaks aitama luua koostoimet ja koordineerida rahalist toetust, mis on seotud liidu algatustega küberturvalisusega seotud teadus- ja arendustegevuse, innovatsiooni, tehnoloogia ja tööstusarengu valdkonnas, ning peaks hoidma ära põhjendamatu dubleerimise. Pädevuskeskus peaks edendama ja koordineerima võrgustiku tööd. Võrgustikku peaks kuuluma üks riiklik koordineerimiskeskus igast liikmesriigist.[3]

Selleks, et küberturvalisuse TTT määruse eesmärke ja sisu täita, tuleb riigisiseselt määrata, milline asutus või juriidiline isik asub Eestis riikliku koordineerimiskeskuse ülesandeid täitma. Seetõttu reguleeritakse eelnõuga küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramise ning selle isiku ülesannete täitmise korraldusega seotud asjaolud. Selle käigus reguleeritakse ka tööstuse, tehnoloogia ja teadusuuringute teemadega seotud Euroopa pädevuskeskuse nõukogu esindaja ja asendajaliikme määramise korraldus. Selleks antakse volitusnormid ministri määruse ja käskkirja kehtestamiseks.

2.3. Küberturvalisuse sertifitseerimise korralduse reguleerimine

Digiteerimisel ning võrgu- ja infosüsteemidel on ühiskonnas väga tähtis roll. Nii füüsilised isikud, ettevõtted kui ka muud organisatsioonid kasutavad laialdaselt digilahendusi oma tegevuste alustalana, samuti kasutatakse info- ja kommunikatsioonitehnoloogia (IKT) tooteid, -teenuseid ja -protsesse ka elutähtsate teenuste pakkumisel. Sellised teenused on seotud näiteks tervishoiu, energeetika, transpordi ja julgeoleku valdkondadega ning nende teenuste toimimine sõltub üha suuremal määral IKT lahendustest. Sealjuures on tähtis võrgu- ja infosüsteemide võimalikult suur turvalisus ja kaitse küberohtude eest.[4]

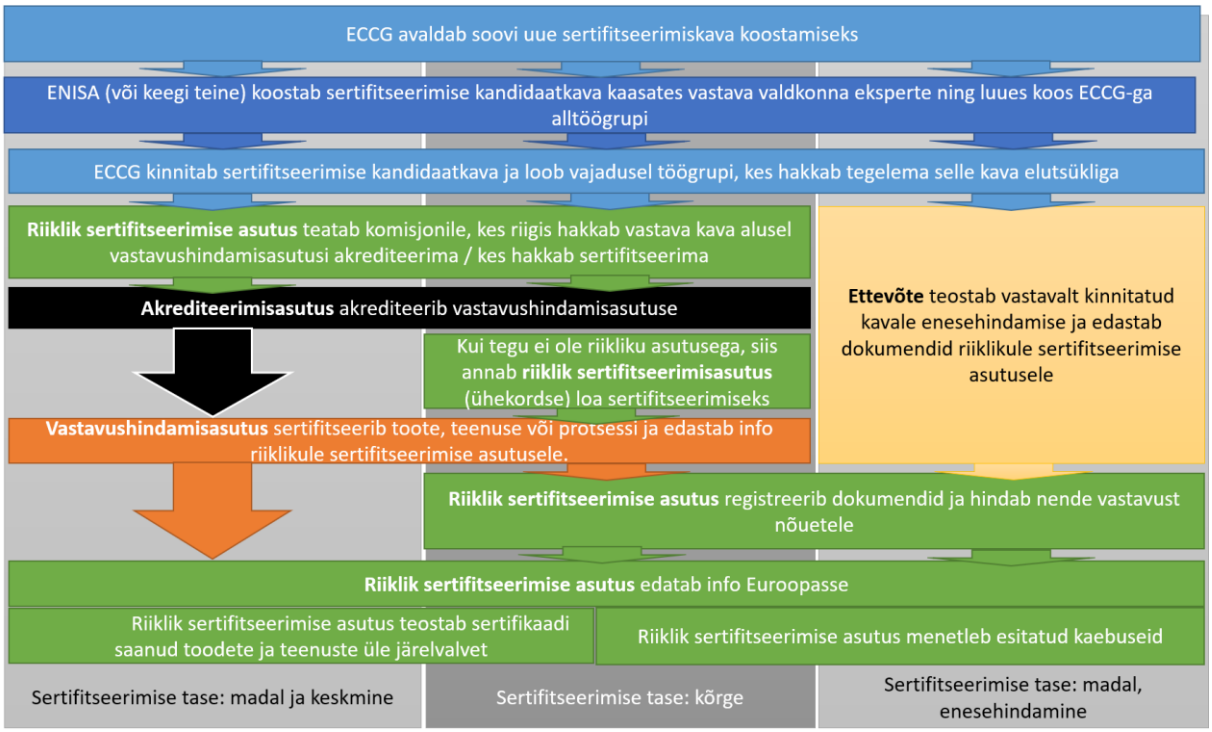
Küberturvalisuse määrusega kehtestatava Euroopa Liidu (edaspidi *EL*) küberturvalisuse sertifitseerimise raamistiku üheks eesmärgiks on samuti usalduse suurendamine Euroopa küberturvalisuse sertifitseerimise kavade kohaselt sertifitseeritud IKT-toodete, -teenuste ja protsesside vastu. Teiseks peaks see aitama vältida üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifitseerimise kavade paljusust ja seeläbi vähendama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid.[5] Luuakse liiduüleselt ühtne sertifikaatide tunnustamise süsteem ning ettevõtjatele võimalus taotleda küberturvalisuse sertifitseerimist. EL-i ülene küberturvalisuse sertifitseerimise kava aitab suurendada internetipõhiste teenuste ja tarbijaseadmete küberturvalisust ning lihtsustab seeläbi ka ettevõtete tegevust, sest ühtne sertifitseerimise süsteem võimaldaks sertifikaatide tunnustamist teistes liikmesriikides.

Küberturvalisuse sertifitseerimise objektideks saavad olla IKT-teenused, -tooted ja -protsessid. Sertifitseerimine toimub Euroopa küberturvalisuse sertifitseerimise kavade alusel. Sertifitseerimise aluseks olevate küberturvalisuse sertifitseerimise kavasid hindab Euroopa Komisjon (EK) regulaarselt, sealjuures viiakse esmane hindamine läbi hiljemalt 31. detsembriks 2023. a ning pärast seda iga kahe aasta järel. Sertifitseerimine on vabatahtlik, kuid hindamise käigus võib EK õigusaktiga muuta küberturvalisuse sertifitseerimise kava(d)

[3] Euroopa Parlamendi ja nõukogu määrus (EL) nr 2021/887, pp-id 14 ja 25.
[4] Küberturvalisuse määrus, pp-d 1-4.
[5] Küberturvalisuse määrus, pp 69.

kohustuslikuks, et tagada EL-s IKT-toodete, -teenuste ja -protsesside küberturvalisuse piisav tase ning parandada siseturu toimimist.[6] Seletuskirja koostamise seisuga on ENISA valmistanud ette pilveandmetöötlusteenustega seotud küberturvalisuse sertifitseerimise kava ning ettevalmistamisel on eraldi küberturvalisuse sertifitseerimise kava ka 5G mobiilsidevõrgu standardi funktsiooniga võrkudega jaoks.[7]

Küberturvalisuse sertifitseerimise korraldus on sätestatud küberturvalisuse määruse III jaotises ja lisas (lisa sisustab vastavushindamisasutuste suhtes kehtivad nõuded). Euroopa Liidu üleselt ja Eesti siseselt toimub sertifitseerimise korraldus järgnevalt:



ECCG ehk *European Cybersecurity Certification Group* on töörühm, mis aitab tagada küberturvalisuse määruse ühtlast üle võtmist ja rakendamist.[8]

Skeem ilmestab, kuidas peaks toimuma sertifitseerimiskava koostamine, vastavushindamisasutuse akrediteerimine, vastavushindamisasutuse teostatav sertifitseerimine ning selle kohta info Euroopasse edastamine ning kuidas toimub järelevalve teostamine. See kõik on erinevate sertifitseerimise tasemete lõikes – nendeks on madal, keskmine ja kõrge. Siiski, ei ole seda kõike võimalik teostada ainult küberturvalisuse määruse alusel – teatavad muudatused tuleb teha ka siseriiklikus õiguses.

EL-i määrused on liikmesriikidele otsekohalduvad, mistõttu on määruste ülevõtmine liikmesriigi õigusesse üleliigne ja ka Euroopa Kohtu tõlgenduse alusel vastuolus EL õigusega.[9]

---

[6] Küberturvalisuse määruse artikkel 53 ning 56 lg-d 2 ja 3.

[7] Leitavad vastavalt: https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes/ ning https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.

[8] Lisainfot ECCG, sh tema ülesannete kohta leiab siit: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group.

[9] Euroopa Kohtu 07.02.1973 otsus, Euroopa Komisjon *vs* Itaalia, C-39/72, ECLI:EU:C:1973:13 ja Euroopa Kohtu 02.02.1997 otsus, Amsterdam Bulb BV vs. Produktschap voor Siergewassen, C-50/76, ECLI:EU:C:1977:13.

Kuivõrd küberturvalisuse määruses on liikmesriigile teatud küsimustes antud kaalutlusruum, siis nende aspektide osas, mida küberturvalisuse määrus ei reguleeri, on vaja liikmesriigil oma õigusesse sisse viia kaalutlusruumi tulemusel tehtud otsused. Praegusel juhul ei saa pidada mitteregulatiivsete meetmete kasutamist võimalikuks, sest karistusi reguleerivad normid ning erinevatele asutustele kohustuste ja ülesannete määramine tuleb kehtestada õiguslike muudatustega.

Eelnõuga viiakse Eesti õigus kooskõlla EL-i õigusega ning küberturvalisuse määruses sätestatud eesmärkide ja nõuetega liikmesriikidele. KüTS-i muutmise tulemusena on võimalik täita küberturvalisuse määruse artiklites 58 ja 65 liikmesriigi ülesannetena sätestatud kohustused, milleks on vastavalt riikliku küberturvalisuse sertifitseerimise asutuse määramine ning küberturvalisuse sertifitseerimise kavade rikkumise korral karistusnormide kehtestamine. Selleks tehakse vastavad täiendused KüTS-s. Eelnõus pakutud sätted annavad selguse, mis asutus täidab riikliku küberturvalisuse sertifitseerimise asutuse ehk järelevalve rolli ning millised on karistusnormid. Sellisel juhul ei tekiks olukorda, kus tuleb omavahel kõrvutada nii Eesti õigusesse toodud sätteid kui ka küberturvalisuse määrust. Eelnõuga tehtav muudatus võimaldab TTJA-l täita riikliku küberturvalisuse sertifitseerimise asutuse ülesandeid, mis asuvad küberturvalisuse määruse artiklis 58. KüTS-s muudatusi tegemata ei ole võimalik TTJA-l neid ülesandeid täita.

Eelnõule eelnevalt pole Eestis küberturvalisuse valdkonnas sertifitseerimist reguleeritud, mistõttu ei ole võimalik anda ülevaadet kehtivast õiguslikust regulatsioonist ning rakendamise praktikast.

3. Eelnõu sisu ja võrdlev analüüs

3.1. Eelnõu

Eelnõu §-ga 1 muudetakse küberturvalisuse seadust.

Eelnõu § 1 punktiga 1 muudetakse KüTS § 1 lõike 1 sõnastust.

Muudatuse sisuks on reguleerimisala konkretiseerimine. Jätkuvalt kohaldatakse seadust olulistele võrgu- ja infosüsteemidele ning olulisus defineeritakse läbi selle teenuse olemuse, mida isik osutab (vt kavandatavat KüTS § 3 lg 1). Seaduse kohaldamisala aga laiendatakse ja konkretiseeritakse avaliku sektori süsteemide osas: „riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide“ asemel sätestatakse, et seadust kohaldatakse „avaliku sektori võrgu- ja infosüsteemide“ suhtes. Seaduse eesmärk on tagada kogu avaliku sektori võrgu- ja infosüsteemide turvalisus, mitte vaid riigi ja kohaliku omavalitsuse üksuse ja nende asutuste süsteemide turvalisus. Täpsemalt on kohaldamisala määratletud loetelude alusel, mis on toodud edaspidi KüTS § 3 lõigetes 1 ja 4, sest kehtivas õiguslikus raamistikus jaguneb suur osa avalikust sektorist ka erinevateks asutusteks ja muudeks üksusteks. Reguleerimisala defineerimine aga „riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide“ kaudu saab tekitada tarbetuid vaidlusi, et kas ühe või teise asutuse võrgu- ja infosüsteemid on konkreetselt riigi süsteemid. Terminit „avalik sektor“ eelnõus täiendavalt ei kasutata, kuivõrd sellekohane subjektide ring on täpsema loetelu kaudu määratletud (vt eelnõu § 1 punkti 4).

Eelnõu § 1 punktiga 2 lisatakse KüTS § 2 punktiga 9 seaduses kasutatava termini „turvameetmed“ definitsioon. Ei määratleta konkreetseid turvameetmeid kitsalt, vaid pigem vastupidi esitatakse lai määratlus, et turvameetmed võivad olla nii organisatsioonilised, füüsilised kui ka infotehnilised toimingud või vahendid, mis täidavad andmete ja süsteemide

turvalisuse saavutamise ning säilitamise eesmärke. Turvameetmed on üldjuhul kogum toimingutest ja vahenditest, mille täpne jaotus sõltub süsteemi turvalisuse saavutamiseks ning säilitamiseks vajalikust ja turvameetmete rakendaja kaalutlustest nende rakendamisel.

Eelnõu § 1 punktiga 3 muudetakse KüTS § 3 lõiget 1 ja täpsustatakse seaduse kohaldamisala.

Esiteks eemaldatakse kohaldamisala piirang, et loetelus nimetatud isik on teenuse osutaja vaid loetelus nimetatud teenuse osutamisel. Muudatuse järgi defineeritakse teenuse osutaja nimetatud piiranguta. Nii tagatakse parem kooskõla teenuse osutaja määratluse ning talle seadusest tulenevate kohustuste eesmärgipärase täitmise vahel. Täitmaks eesmärki tagada võrgu- ja infosüsteemide küberturvalisus ühiskonna seisukohast oluliste teenuste osutamiseks, on aina rohkem läbipõimunud infotehnoloogia taristuid arvestades vajalik välistada võimalusi eirata üht osa kasutatava infotehnoloogia taristust teenuste kaardistamisel, küberriskide analüüsimisel ning turvameetmete rakendamisel. See on kooskõlas ka KüTS § 6 punktis 1 sätestatud isiklikkuse põhimõttega, mille eelduseks on, et iga infoühiskonna osaline vastutab oma valduses olevate infosüsteemide turvalisuse eest. Samuti ei ole KüTS-s sätestatud nõuded teenuse osutajale muudes sätetes piiratud vaid teenuse osutamiseks kasutatava süsteemidega. Käesoleva eelnõu üks eesmärkidest on ka kehtiva ISKE asendamine E-ITS-ga ning kuivõrd ISKE oli koostatud andmekogude kui infosüsteemide ühe liigi küberturbe vaatepunktist, siis E-ITS on koostatud organisatsiooni kui terviku küberturbe vaatepunktist. Arvestades, et käesoleva eelnõu eesmärk on sätestada E-ITS rakendamise kohustus ka teenuse osutajale, tekitaks eelmainitud teenuse osutaja määratluse piirangu sisse jätmine ka soovimatuid vastuolusid E-ITS-i rakendamisel. Õigusselguse huvides on, et teenuse osutaja määratlus ei oleks süsteemi kasutuseesmärgiga piiratud, kuivõrd selline piirang puudub ka avalikul sektoril ning digitaalse teenuse osutajatel.

Teiseks, lisatakse teenuse osutajaks AvTS-i tähenduses andmekogu vastutav töötleja ning volitatud töötleja. Käesolev eelnõu asendab AvTS alusel kehtestatud ISKE KüTS-i alusel kehtestatud E-ITS-ga ning selleks, et tagada andmekogude küberturvalisus, tuleb seega ka täpsustada KüTS kohaldamisala. Seetõttu hõlmatakse ka andmekogude vastutavad ja volitatud töötlejad KüTS-i teenuse osutajate määratlusse. Näiteks on selle tõttu teenuse osutajaks ka Liikluskindlustuse Fond, mis on AvTS-i mõistes andmekogu vastutav töötleja.

Kolmandaks asendatakse relevantsetes kohtades termin „sätestatud“ terminiga „tähenduses“ või selle asjakohase ekvivalendiga. Loetelus kasutatakse mitmes kohas viiteid teistes seadustes sätestatud terminitele, kuid need terminid erinevate teenuste osutajate kohta ei nimetanud konkreetseid füüsilisi või juriidilisi isikuid, mistõttu on korrektsem tugineda seaduses viidatud termini tähendusele subjektide loetlemisel.

Ühe sisulisema muudatusena muudetakse ka KüTS § 3 lõike 1 punkti 4. Esiteks vähendatakse sadamateenuse osutajate ringi, keda KüTS § 3 lõike 1 punkti 4 alusel teenuse osutajana käsitletakse. Täpsemalt on seotud muudatus teenindavate laevade loetelu muutmisega, kuivõrd kehtivas sadamaseaduses on viimase revisjoni käigus võetud turvanõuete kohaldamisalast välja kohalikke rannasõite sõitvad üle 250 reisijaga (kuid alla 500-se kogumahutavusega) laevu teenindavad sadamad ehk nn väiksemad siseriiklike liinide sadamad. KüTS on tuginenud selle kohaldamisala määramisel sadamaseaduse määratlusele ning käesolev eelnõu kaasajastab ka seega küberturvalisuse nõuete kohaldamisala vastavalt.

Eelnõu § 1 punktiga 4 muudetakse KüTS § 3 lõiget 4 ja täpsustatakse KüTS nõuete kohaldamisala avalikule sektorile.

Eemaldatakse sõnastus, et loetelule kohaldatakse teenuse osutaja kohta sätestatut KüTS § 9-s sätestatud erisusega. Eelnõu § 1 punktiga 10 tunnistatakse nimetatud paragrahv kehtetuks, mida käesolevas seletuskirjas selle punkti all ka täpsemalt käsitletakse.

Punktiga täpsustatakse kohaldamisala loetelu. Kehtiva KüTS-i järgi kohaldatakse teenuse osutaja kohta sätestatut riigile ja kohaliku omavalitsuse üksusele (vald või linn). Arvestades aga, et riigi- või kohaliku omavalitsuse üksuse asutused ei ole juriidilised isikud ning tegutsevad kas riigi või kohaliku omavalitsuse üksuse esindajana, tekitas senine loetelu tarbetuid vaidlusi, et kas KüTS-i nõudeid kohaldatakse konkreetsele asutusele või mitte. Küberturvalisuse nõuete sätestamine kogu avaliku sektori süsteemidele kannab endas eesmärki tagada avalike teenuste osutamiseks kasutatavate süsteemide ning nendes olevate andmete turvalisus ning ka kehtiva KüTS-i eelnõu seletuskirja[10] kohaselt on eesmärk ennekõike laiendada küberturvalisuse nõudeid andmekogudelt AvTS mõistes kõikide avaliku sektori asutuste süsteemidele. Seepärast on loetelust kaotatud riik kui eraldi subjekt ning loodud oluliselt täpsem ja paremat õigusselgust tagav loetelu.

Loetelu esimene punkt on Riigikogu Kantselei. Eesmärk on tagada riigi seadusandliku võimu rakendamisel kasutatavate süsteemide ja selles olevate andmete turvalisus. Seetõttu kohaldatakse teenuse osutaja kohta sätestatut ka Riigikogu teenindavale Riigikogu Kantseleile.

Loetelu teine punkt on riigi valimisteenistus. Riigi valimisteenistus on küll Riigikogu Kantselei struktuuriüksus, kuid Riigikogu valimise seaduse § 14 lõike 1 alusel on riigi valimisteenistus oma ülesannete täitmisel iseseisev. Eelnõu eesmärk on tagada ka valimiste korraldamisel kasutatavate süsteemide ja andmete turvalisus, mistõttu on õigusselguse huvides eraldi välja toodud ka riigi valimisteenistus kui Riigikogu Kantselei struktuuriüksus. Eelduslikult kohaldatakse küberturvalisuse nõudeid kõikide subjektide kõikidele struktuuriüksustele, kuid käesolev punkt loetelus on loodud õigusselguse tagamise eesmärgil, kuna riigi valimisteenistus on oma ülesannete täitmisel iseseisev.

Loetelu kolmas punkt on Riigikogus esindatud erakond erakonnaseaduse tähenduses. Erakonnad kui mittetulundusühingud on eraõiguslikud juriidilised isikud, kuid Riigikogus esindatud erakondadele makstakse riigieelarvest eraldisi ning nad kannavad avalikus sektoris olulist funktsiooni seadusloomes, mh ka fraktsiooni tegevuse kaudu. Seega kui Riigikogus esindatud erakond kasutab võrgu- ja infosüsteeme, on nendele süsteemidele ka avaliku sektori toimimise tagamise seisukohalt kõrgendatud kaitsevajadus.

Loetelu neljas punkt on kohtuasutus kohtute seaduse tähenduses. Kohtute seaduse § 7 lõike 1 alusel on kohtuasutused maakohus, halduskohus, ringkonnakohus ja Riigikohus. Eesmärk on tagada riigi kohtuvõimu rakendamisel kasutatavate süsteemide ja andmete turvalisus.

Loetelu viies punkt on valitsusasutus ja valitsusasutuse hallatav riigiasutus. Valitsusasutused on määratletud Vabariigi Valitsuse seaduse (edaspidi *VVS*) §-s 39 ning valitsusasutuse hallatav riigiasutus VVS §-s 43. Eesmärk on tagada riigi täidesaatva võimu rakendamisel kasutatavate süsteemide ja andmete turvalisus. Tegemist on sisult laia loeteluga, kuivõrd valitsusasutusena

[10] Küberturvalisuse seadus 597 SE seletuskiri lk 19 jj, kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus.

käsitletakse ministeeriume, kaitseväge, Riigikantseleid, riigiameteid ja inspektsioone ning valitsusasutuste hallatavate riigiasutustena käsitletakse erinevate valitsusasutuste valitsemisalas olevaid asutusi, nagu näiteks erinevad riigikoolid, instituudid ja vanglad.

Loetelu kuues punkt on kohaliku omavalitsuse üksuste liit, nt Harjumaa Omavalitsuste Liit ning kohaliku omavalitsuse üksus ehk vallad ja linnad. Selle ning loetelu järgneva punkti eesmärk on täpsustada kohaldamisala kohaliku omavalitsuse üksuse kontekstis, kus sarnaselt riigiasutustega on õigusselguse huvides vajalik määratleda avalik sektor täpsemalt kui juriidilise isiku tasandil.

Loetelu seitsmes punkt on valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald ning linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus, omavalitsusüksuste ühisamet ja -asutus. Sarnaselt ka loetelu viiendale punktile on siinkohal tegemist sisult laia loeteluga, kuivõrd punkti eesmärk on tagada kogu kohaliku elu korraldamisega seotud ülesannete täitmisel ning avalike teenuste osutamisel kasutatavate süsteemide ja andmete turvalisus.

Loetelu kaheksas punkt on Vabariigi Presidendi Kantselei ning üheksas punkt Õiguskantsleri Kantselei. Nimetatud kantseleid teenindavad põhiseaduslikke institutsioone oma ülesannete täitmisel, mistõttu on vajalik tagada nende poolt kasutatavate süsteemide ja andmete turvalisus.

Loetelu kümnes punkt on Riigikontroll ja üheteistkümnes punkt on Eesti Pank. Sarnaselt loetelu kahele eelmisele punktile on jällegi tegemist põhiseadusliku institutsiooni süsteemide ja andmete turvalisuse tagamise eesmärgiga, kuid kuivõrd institutsioon ise ei koosne ühest isikust, siis on otstarbekam kohaldada nõudeid institutsioonidele otse.

Loetelu kaheteistkümnes punkt on Riigimetsa Majandamise Keskus. Eelnõu koostamise hetkel on Riigimetsa Majandamise Keskus ainus riigitulundusasutus Eestis. Kahjuks aga ei ole eelnõu koostamise hetkel kehtivas õiguses riigitulundusasutuse tähendust määratletud ning puudub ka võimalus Riigimetsa Majandamise Keskust muud moodi määratleda. Kuni 01.01.2010 kehtinud riigivaraseaduse § 6 lõike 1 alusel on riigitulundusasutus riigiasutus, mis võib osutada tasulisi teenuseid ja saada selle eest tulu. Ka eelnõu koostamise hetkel kehtivas riigivaraseaduses on korduvalt riigitulundusasutuse terminit kasutatud, kuid puudub eraldi säte termini määratlemiseks. Kehtiva riigivaraseaduse eelnõu seletuskirja[11] kohaselt ei peetud õigeks sätestada asutuse vorm riigivaraseaduses ning soovitati seda teha VVS-s või näiteks sellest asutuse vormist loobuda. Käesoleva eelnõu koostamise hetkeks kumbagi aga tehtud ei ole. Sellest hoolimata on aga vajalik tagada Riigimetsa Majandamise Keskuse süsteemide turvalisus, kuivõrd tema teenused ning selleks kasutatavad andmed on avaliku sektori toimimiseks vajalikud.

Loetelu kolmeteistkümnes punkt on seaduse alusel loodud avalik-õiguslik juriidiline isik, nt Eesti Haigekassa, Notarite Koda või erinevad ülikoolid. Eranditult kannavad kõik avalik-õiguslikud juriidilised isikud olulist osa avaliku sektori toimimisel, olgu tegemist ühenduse, asutuse või fondiga. Küberturvalisuse nõuded kohaldusid mitmele avalik-õiguslikule juriidilisele isikule ka varasemalt kui andmekogu vastutavale või volitatud töötlejale. Kuivõrd avalik-õiguslikel juriidilistel isikutel on reeglina arvestatav ligipääs erinevatele andmekogudele ning nende osutatavad reguleeritud teenused on ühiskondlikult tähtsad, siis on ka käesoleva

[11] Riigivaraseadus 437 SE seletuskiri lk 14, kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/bd686b3c-a592-2d90-dc53-12d484999745/Riigivaraseadus.

eelnõu punkti eesmärk avalikule sektorile mõeldud kohaldamisala täpsustada avalik-õiguslike juriidiliste isikute suhtes.

Käesolevast loetelust on välja jäetud kapitaliühingud, mittetulundusühingud ja sihtasutused, mis on näiteks asutatud riigi, valla või linna osalusel või täidavad muul alusel avalikke ülesandeid. Kuivõrd eesmärk on KüTS kohaldamisala täpsustada avaliku sektori suhtes, siis välditakse küberturvalisuse nõuete kohaldamist isikutele ebatäpsete kriteeriumite alustel. Kapitaliühingud, mittetulundusühingud ja sihtasutused, mis on ühiskonna toimimise seisukohast olulised (nt Riigi Infokommunikatsiooni SA, Eesti Energia AS, erinevad haiglad, vee- ja soojusettevõtted) on ka teenuse osutajad KüTS § 3 lõike 1 alusel.

Eelnõu § 1 punktiga 5 lisatakse seadusesse § 5^1. Nimetatud paragrahviga sätestatakse küberturvalisuse TTT määruse tähenduses küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse nõukogu esindaja ja asendajaliikme nimetamine ning riikliku koordineerimiskeskuse määramine ja ülesannete korraldus.

Küberturvalisuse TTT määrus sätestab artikli 6 lõikes 1 liikmesriikidele 29. detsembriks 2021 kohustuse määrata määruse tingimustele vastava asutuse riiklikuks koordineerimiskeskuseks ning artiklis 12 kohustuse nimetada liikmesriigi esindaja ja asendusliige Euroopa pädevuskeskuse nõukogusse. Käesoleva eelnõu punkti eesmärk on nende kohustuste täitmine.

Paragrahvi **esimese lõike** alusel volitatakse valdkonna eest vastatuvat ministrit (kelleks eelnõu koostamise hetkel on ettevõtlus- ja infotehnoloogiaminister) nimetama käskkirjaga Euroopa pädevuskeskuse nõukogusse Eesti Vabariigi esindaja ja asendusliikme. Küberturvalisuse TTT määruse artikli 12 lõigete 1 ja 2 kohaselt kuuluvad küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (edaspidi pädevuskeskus) nõukogusse üks esindaja igast liikmesriigist ja komisjonist kaks esindajat, kes tegutsevad liidu nimel; ning igal pädevuskeskuse nõukogu liikmel on asendusliige. Sama artikli lõike 3 kohaselt peavad pädevuskeskuse nõukogu liikmed ja asendusliikmed olema *„liikmesriigi avaliku sektori töötajad, kes nimetatakse ametisse lähtuvalt nende teadmistest küberturvalisuse teadusuuringute, tehnoloogia ja tööstuse valdkonnas, võimest tagada meetmete ja seisukohtade koordineerimine vastava riikliku koordineerimiskeskusega või nende asjakohastest juhtimis-, haldus- ja eelarvealastest oskustest“*.

Paragrahvi **teine lõige** sätestab, et küberturvalisuse TTT määruse tähenduses riikliku koordineerimiskeskuse ülesandeid täidab TTT koordineerimisüksus. Riikliku koordineerimiskeskuse ülesanded on sätestatud küberturvalisuse TTT määruses. Nimetatud artikli lõike 5 kohaselt on riiklik koordineerimiskeskus avaliku sektori asutus või liikmesriigi enamusosalusega asutus, kes täidab liikmesriigi õiguse alusel avaliku halduse ülesandeid, sealhulgas delegeerimise kaudu, ja kellel on suutlikkus toetada pädevuskeskust ja võrgustikku nende käesoleva määruse artiklis 3 sätestatud missiooni elluviimisel. Asutusel peavad olema teaduse ja tehnoloogia alased eksperditeadmised küberturvalisuse valdkonnas või juurdepääs sellistele teadmistele. Asutus peab suutma pidada tulemuslikku dialoogi ja koordineerida oma tegevust tööstuse, avaliku sektori, akadeemilise ja teaduskogukonnaga ning kodanikega, sealhulgas direktiivi (EL) 2016/1148 kohaselt määratud asutustega.

Paragrahvi **kolmanda lõike** alusel volitatakse valdkonna eest vastutavat ministrit (kelleks eelnõu koostamise hetkel on ettevõtlus- ja infotehnoloogiaminister) määrama TTT koordineerimisüksuse ning kehtestama tema ülesannete täitmise korra määrusega. Arvestades

eelmises lõigus kirjeldatud koordineerimiskeskuse ülesandeid saab koordineerimisüksuses olla valitsusasutus, valitsusasutuse hallatav asutus või riigi enamusosalusega äriühing. Määruse kavand on seletuskirja lisas. Käesoleva eelnõu koostamise hetkel kavandatakse määrata RIA TTT koordineerimisüksuseks. Nimetatud asutuse määramine on sobilik teha määruse tasandil, kuna ka samas määruses sätestatakse TTT koordineerimisüksuse ülesannete korraldus. Volitusnormi sisu ja ulatus on vastavuses kavandatava määrusega.

Üleüldiselt on TTT koordineerimisüksusel kohustus oma ülesannete täitmisel lähtuda küberturvalisuse TTT määrusest, KüTS-st, muudest seadustest ja nende alusel kehtestatud õigusaktidest. Nende alusel kehtestatud õigusaktide all on mõeldud ka KüTS § 5^1 lõike 3 alusel kehtestatud ministri määrust. Kehtestatava ministri määruse kavand on lisatud käesolevale eelnõule.

Eelnõu § 1 punktiga 6 eemaldatakse KüTS § 7 lõikest 1 sõnad „organisatsioonilisi, füüsilisi ja infotehnilisi“, kuivõrd eelnõuga lisatav turvameetmete definitsioon hõlmab muuhulgas ka sellist liigitust. Tegemist on tehnilise muudatusega.

Eelnõu § 1 punktiga 7 tunnistatakse kehtetuks KüTS § 7 lõike 2 punktid 5 ja 6 ning lõige 4.

KüTS § 7 lõike 2 punktides 5 ja 6 sätestatud kohustused ei omaks eelnõu vastuvõtmise korral sisulist mõju, kuivõrd turvameetmete rakendamise piisavuse kontroll on olemuslikult kohustuslikuks osaks E-ITS tingimuste järgimisel (auditeerimiskohustus). Punktid tunnistatakse kehtetuks et vältida olukordi, kus teenuse osutaja peaks sama tegevust läbi viima eraldi sätete alusel.

KüTS § 7 lõike 4 alusel kehtestatud määruse nõuded kattuvad olemuslikult E-ITS nõuetega, mistõttu KüTS § 7 lõike 4 alusel kehtestatud määrus asendatakse eelnõu § 1 punkti 8 alusel kavandatava Vabariigi Valitsuse määrusega.

Eelnõu § 1 punktiga 8 lisatakse KüTS §-le 7 lõige 5. Tegemist on volitusnormiga KüTS §-s 7 sätestatud kohustuste sisu ehk kohustuse täitmiseks koostatavate riskianalüüside, rakendatavate turvameetmete täpsustamiseks ning infoturbe halduse nõuete ja juhendite kehtestamiseks. Määruse kavand on seletuskirja lisas.

Kehtestatava(te) määrus(t)e alusel sätestatavate nõuete eesmärk on tagada KüTS § 7 alusel sätestatud kohustuste täitmine kohustatud subjekti poolt ning süsteemi (ja selles käideldavate andmete) küberturvalisus. Volitusnormi sisulised piirid sätestab KüTS § 7, kuivõrd nõuded on kohaldatavad turvameetmete rakendamisel ning rakendamisega kaasnevate kohustuste täitmisel.

Eelnõu punktiga sätestatud volitusnorm jaotub volituseks kehtestada kolme liiki regulatsioone.

Kehtestatava lõike esimene volitus kohaldub E-ITS-i kehtestamisele. Eelnõu koostamise hetkel kavandatav Vabariigi Valitsuse määrus sätestab kohustuse järgida E-ITS-i ning rakendada selle järgimisest tulenevaid turvameetmeid, kusjuures E-ITS-i järgimine seisneb E-ITS tingimuste täitmises infoturbe halduse käivitamisel, rakendamisel, käigushoidmisel ning täiustamisel ja E-ITS-i tingimuste täitmise auditeerimises.

Eelnõu lisaks olev kavandatav Vabariigi Valituse määrus annab üleriigilise küberturvalisuse tagamise korraldamise eest vastutavale ministrile (kelleks eelnõu koostamise hetkel on ettevõtlus- ja infotehnoloogiaminister) volituse kehtestada E-ITS (kui dokument ise)

määrusega. Selleks sätestatakse käesoleva eelnõu punktiga ka edasivolituse võimalus. E-ITS kehtestamine on otstarbekam läbi viia edasivolituse alusel ministri määrusega, sest praktikas võimaldab ministri määruse kehtestamine vastavalt vajadusele dokumenti ajakohastada pidevalt muutuvast IKT raamistikust tulenevalt. „Valdkonna eest vastutav minister“ täpsustuse tegemise vajalikkus kavandatavas Vabariigi Valitsuse määruses tuleneb sellest, et kavandatavas määruses sätestatakse ka volitusnorm erinevate valitsusalade ministritele ning sellises olukorras valdkonna täpsustamata jätmine võib tekitada õigusselgusetust. E-ITS kehtestamine käskkirjaga ei ole võimalik, kuivõrd E-ITS-i kehtestamine ei ole käsitletav üksikjuhtumi reguleerimisena.

Kehtestatava lõike teine volitus kohaldub turvameetmete üldnõuete kehtestamisele. Tegemist üldnõuetega turvameetmete rakendamisel, mida teenuse osutaja peab järgima sõltumata valitud turvameetmetest, erinevate standardite järgimisest või kaitstavate süsteemide iseloomust. Eelnõu koostamise hetkel kavandatav Vabariigi Valitsuse määrus hõlmab selle peatüki all kohustust dokumenteerida teenused, teenuste haldamiseks asjakohased süsteemid, riskianalüüsi ja süsteemidele rakendatavad turvameetmed ning võib tulevikus näiteks reguleerida ka konkreetsete andmekoosseisude suhtes pilveteenuste kasutamise nõudeid.

Kehtestatava lõike kolmas volitus kohaldub eriliigiliste süsteemide turvameetmete erinõuete kehtestamisele. Siinkohal on mitmuse „süsteemid“ kasutamine taotuslik, kuivõrd selle volituse alusel kehtestatavad nõuded kohalduvad vaid vastavas peatükis kirjeldatud süsteemidele.

Käesoleva eelnõu koostamise hetkel kavandatav Vabariigi Valitsuse määrus sätestab esiteks erinõuded andmekogudele, mis seisnevad eelkõige ISKE-st pärit ja AvTS-i tähenduses andmekogude põhimäärustes sätestatud turvaklasside säilitamises ning nende kasutamises E-ITS-i järgimisel.

Teiseks sätestab kavandatav määrus ka avalike ülesannete täitmist oluliselt mõjutavate süsteemide loetelu ning nende pidamise nõuded, ennekõike kohustus varundada loetletud süsteemide andmekoosseis välisriigi andmekeskusesse (andmesaatkonda).

Kolmandaks volitab kavandatav määrus riigikaitse korraldamise eest vastutava ministri (kelleks eelnõu koostamise hetkel on kaitseminister) kehtestama määrusega rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvameetmete kirjelduse ning sätestab, et nende süsteemide osas kavandatavas määruses sätestatud turvameetmete üldnõudeid ja E-ITS-i järgimise kohustust ei kohaldata. Eelnõu § 1 punktiga 10 tunnistatakse KüTS § 9 kehtetuks ning selle punktiga viiakse KüTS § 9 lõige 3 üle kavandatavasse Vabariigi Valitsuse määrusesse.

Volitusnormi sisu ja ulatus on vastavuses kavandatavate Vabariigi Valitsuse ja ministrite määrustega.

Eelnõu § 1 punktiga 9 lisatakse KüTS § 8-le lõige 1^1 sätestamaks teenuse osutajale kohustuse tagada küberintsidendist teavitamine ka juhul, kui süsteemi haldamine või majutamine volitatakse teisele isikule. KüTS § 7 lõike 3 alusel on teenuse osutajal kohustus tagada süsteemi turvameetmete rakendamine ka juhul, kui süsteemi haldamine või majutamine volitatakse teisele isikule ning käesoleva punkti eesmärk on tagada samasuguses olukorras ka küberintsidendist teavitamine teenuse osutajale.

Ka turvameetmete rakendamise korral on küberintsidendi tekkimine võimalik ning teenuse osutaja peab seega tagama, et ta oleks teadlik süsteemi küberintsidendist sõltumata sellest, kas

süsteemi majutab või haldab tema või kolmas isik. Kui küberrünnaku läbiviija otsustab võtta sihtmärgiks süsteemi haldamiseks volitatud isiku, siis KüTS-i muutmata ei pruugi teenuse osutaja ega seega ka RIA taolisest küberintsidendist üldse teada saada, kuna KüTS-s puudub vastav teavitamiskohustus. Käesolev eelnõu punkt sätestab teenuse osutajale kohustust tagada süsteemi haldaja või majutaja teenuste kasutamisel küberintsidentidest teavitamine. Küberintsidendist teavitamine aitab kiirendada selle lahendamist ning vähendab võimaliku kahju (nii varalise kui mittevaralise kahju) tekkimist või suurenemist. Näiteks aitab vastav teavitamine kasutusele võtta meetmed, mis välistavad või piiravad küberintsiendi mõju avaldumist teenuse osutaja teistes süsteemides; või nende mõju kandumist oma partnerasutuste ja -ettevõtete süsteemidesse.

Kui teenuse osutajat on KüTS § 7 lõike 3 tähenduses teise isiku poolt teavitatud küberintsidendist hiljemalt 24 tunni jooksul pärast selle isiku poolt küberintsidendist teada saamist, on teenuse osutaja täitnud oma kohustuse KüTS § 8 lõike 1^1 alusel. Ajahetk, mil nimetatud teine isik teenuse osutajat küberintsidendist teavitab, loetakse teenuse osutaja teadasaamiseks küberintsidendist KüTS § 8 lõike 1 tähenduses.

Eelnõu § 1 punktiga 10 tunnistatakse KüTS § 9 kehtetuks.

Paragrahv tunnistatakse kehtetuks, kuivõrd eelnõu teiste punktide jõustumisel kaotab nimetatud paragrahv regulatiivse mõju.

KüTS § 9 lõige 1 vabastas avaliku sektori KüTS § 7 lõike 4 alusel kehtestatud nõuete järgimisest ning KüTS § 9 lõige 2 lisas täiendava nõudena ISKE järgimise kohustuse (kuigi üleminekuperioodil on AvTS-i nõuete tõttu ISKE jätkuvalt kohustuslik andmekogude korral kuni 31. detsembrini 2022. a). Käesolev eelnõu asendab ISKE E-ITS-ga ning E-ITS-i tingimuste järgimine on ühetaoliselt kohustuslik nii teenuse osutajatele kui ka avalikule sektorile.

KüTS § 9 lõige 3 sätestas volitusnormi kaitseministrile sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvanõuete kehtestamiseks. Käesolev eelnõu näeb ette sama volituse eelnõu § 1 punkti 8 alusel kavandatavas Vabariigi Valitsuse määruses edasivolituse kaudu.

Eelnõu § 1 punktiga 11 lisatakse seadusesse peatükk 3^1 „Küberturvalisuse sertifitseerimine“. Peatükki lisatakse paragrahvid 13^1 ja 13^2 . Lisanduse eesmärk on eelnõuga KüTS-s luua eraldi peatükk, mis täpsustab küberturvalisuse määruses sätestatud küberturvalisuse IKT toodete, teenuste või protsesside sertifitseerimise temaatikat.

KüTS §-ga 13^1 sätestatakse, et TTJA on riiklik küberturvalisuse sertifitseerimise asutus küberturvalisuse määruse art 58 lõike 1 tähenduses.

Liikmesriigile on küberturvalisuse määruse 3. jaotises antud kaalutlusruum osas, kas määrata üks või mitu riiklikku küberturvalisuse sertifitseerimise asutust või vastastikusel kokkuleppel teise liikmesriigiga ühe või mitu riiklikku küberturvalisuse sertifitseerimise asutust, mis asub nimetatud teises liikmesriigis ja mis vastutab järelevalveülesannete eest määravas liikmesriigis.[12] Eelnõu koostamise käigus ei ole peetud teiste liikmesriikidega läbirääkimisi, et taolist kokkulepet sõlmida.

[12] Küberturvalisuse määruse art 58 lg 1.

Küberturvalisuse määruses on selgitatud, et riiklik küberturvalisuse sertifitseerimise asutus peaks ennekõike:

1. jälgima tema riigi territooriumil asuvate IKT-toodete, -teenuste või -protsesside tootjate ja pakkujate kohustusi seoses ELi vastavusdeklaratsiooniga ning tagama nimetatud kohustuste täitmise;
2. abistama riiklikke akrediteerimisasutusi vastavushindamisasutuste tegevuse seire ja järelevalve osas, pakkudes neile oskusteavet ja asjakohast teavet;
3. volitama vastavushindamisasutusi täitma nende ülesandeid, kui nad vastavad Euroopa küberturvalisuse sertifitseerimise kavas sätestatud täiendavatele nõuetele;
4. jälgima asjakohast arengut küberturvalisuse sertifitseerimise valdkonnas;
5. käsitlema füüsiliste või juriidiliste isikute esitatud kaebusi seoses nende või vastavushindamisasutuste poolt väljaantud kõrge usaldusväärsuse tasemega Euroopa küberturvalisuse sertifikaatidega, uurima asjakohasel määral kaebuse sisu ja teavitama kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest;
6. tegema koostööd teiste riiklike küberturvalisuse sertifitseerimise asutuste ja muude avaliku sektori asutustega, sealhulgas jagades teavet IKT-toodete, -teenuste ja -protsesside võimaliku mittevastavuse kohta küberturvalisuse määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele. Komisjon peaks hõlbustama seda teabevahetust, tehes kättesaadavaks üldise elektroonilise teabe tugisüsteemi, nagu turujärelevalve info- ja teavitussüsteem (ICSMS) ja kiire teabevahetuse süsteem toiduks mittekasutatavate toodete kohta (RAPEX), mida turujärelevalveasutused juba kasutavad vastavalt määrusele (EÜ) nr 765/2008.[13]

Küberturvalisuse määruse kohaselt on riikliku küberturvalisuse sertifitseerimise asutuse ehk TTJA ülesanded järgmised (lihtsustatult):

a) teha koostöös teiste asjaomaste turujärelevalveasutustega järelevalvet Euroopa küberturvalisuse sertifitseerimise kavade täitmise üle;
b) jälgida oma liikmesriigi territooriumil asuvate ja vastavuse enesehindamist tegevate tootjate või pakkujate kohustuste täitmist ning tagada nende kohustuste täitmine;
c) toetada ja aidata aktiivselt riiklikke akrediteerimisasutusi;
d) kontrollida avaliku sektori asutuste tegevust, kui nad annavad välja kõrgetasemelisi sertifikaate;
e) kui Euroopa Liidu sertifitseerimise kavast tuleb vastavushindamisasutusele lisatingimusi, anda neile luba, lube piirata või ära võtta;
f) käsitleda kaebusi seoses Euroopa küberturvalisuse sertifikaatidega, mille on väljastanud selleks pädevad asutused või mis seonduvad ELi vastavusdeklaratsioonidega ning uurida asjakohasel määral kaebuste sisu ja teavitada kaebuse esitajat uurimises käigust ja tulemusest;
g) esitada iga-aastane kokkuvõtlik aruanne oma tegevuste kohta ENISA-le ja Euroopa küberturvalisuse sertifitseerimise rühmale;
h) teha koostööd teiste riiklike küberturvalisuse sertifitseerimise asutustega, sealhulgas jagada teavet IKT-toodete, -teenuste ja -protsesside võimaliku mittevastavuse kohta käesoleva määruse või konkreetsete Euroopa küberturvalisuse sertifitseerimise kavade nõuetele;

[13] Küberturvalisuse määrus, pp 102.

i) jälgida küberturvalisuse sertifitseerimise valdkonna asjakohast arengut.[14]

Liikmesriigid peavad tagama, et riikliku küberturvalisuse sertifitseerimise asutuste tegevus on Euroopa küberturvalisuse sertifikaatide väljaandmisega rangelt lahus järelevalvetegevustest ning et nimetatud tegevusi viiakse ellu üksteisest sõltumatult.[15] Sertifitseerimise kavad võivad ette näha nõude, et kõrgetasemelisi sertifikaate tohib väljastada vaid avalik asutus. See avalik asutus võib olla riiklik küberturvalisuse sertifitseerimise asutus ise või muu avalik asutus, kes on akrediteeritud vastavushindamisasutusena. Seega võib põhimõtteliselt olla riiklik küberturvalisuse sertifitseerimise asutus nii järelevalvaja kui ka sertifitseerija rollis, kuid need ülesanded peavad olema üksteisest rangelt eraldatud, sealhulgas ei tohi neid ülesandeid teostada samad inimesed. Tagada tuleb riikliku küberturvalisuse sertifitseerimise asutuse rolli ja vastavushindamisasutuse rolli vahelise huvide konflikti puudumine ning see dokumenteerida.[16]

Arvestades eeltoodut, määratakse eelnõuga riikliku sertifitseerimise asutuseks TTJA, kes peaks ühendust EL tasandiga ja teostaks järelevalvet. Kui tegu on kõrge taseme sertifikaadiga, võib sertifikaati välja anda ainult riiklik sertifitseerimise asutus või muu avalik asutus, kes on vastavushindamisasutusena akrediteeritud. Ka sertifitseerimise kavast võib tuleneda, et teatud sertifikaati võib välja anda üksnes avalik asutus. Sertifitseerimist teostava asutusena ehk vastavushindamisasutusena tegutsemine eeldab akrediteerimist ja tegevusluba. Akrediteeringut oleks vaja nii riikliku sertifitseerimisasutuse organil kui ka muul avalikul asutusel, mis sertifitseerimisega tegeleks.

RIA on KüTS §-i 5 järgi Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 artikli 8 lõikes 1 nimetatud pädev asutus ja lõikes 3 nimetatud ühtne kontaktpunkt ning artikli 9 lõikes 1 nimetatud küberturbe intsidentide lahendamise üksuse ülesannete täitja. Eelnõu koostamisel on lähtutud eeldusest, mille kohaselt võiks sertifikaate väljastav avalik asutus olla RIA, kellel on ametitest kõige suurem kompetents küberturvalisuse valdkonnas. Sellega oleks järelevalvaja roll (TTJA) ning sertifitseerija roll (RIA) omavahel eraldatud ja sõltumatud.

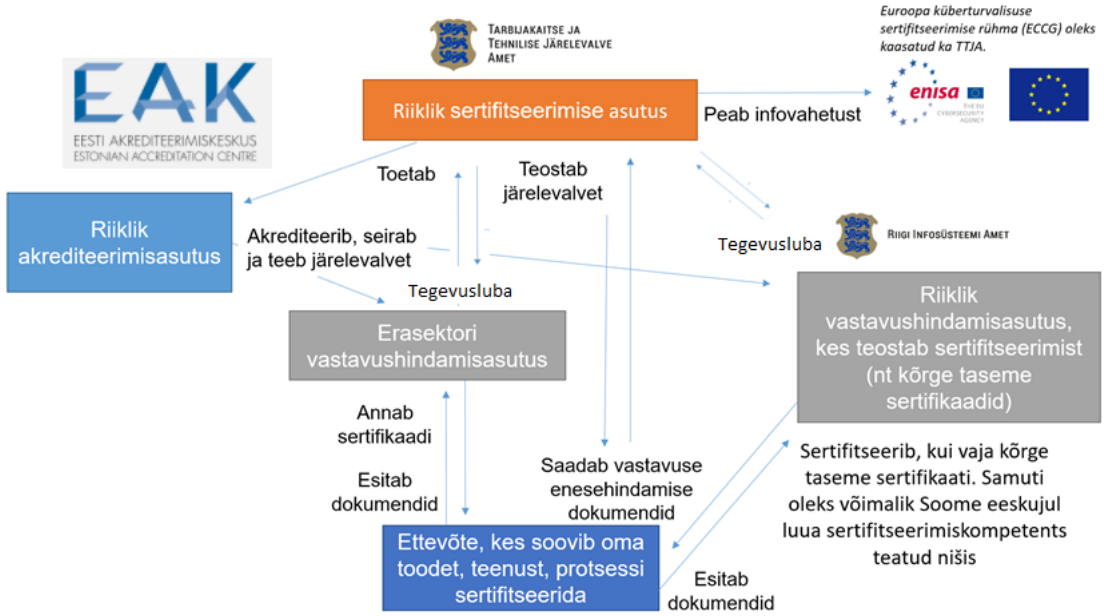
Samas eeldab RIA tegutsemine vastavushindamisasutusena tema eelnevat akrediteerimist. Seaduse tasandil ei ole võimalik määratleda, et RIA on küberturvalisuse määruse kohane vastavushindamisasutus, sest vastavushindamisasutuseks saamine eeldab akrediteerimisprotsessi läbimist ning akrediteerimine on edukas, kui asutus vastab küberturvalisuse määruse nõuetele.[17] Eelnõu koostamisel lähtutakse eeldusest, et RIA läbib vastava akrediteerimise.

Lisaks on ka võimalus, et vastavushindamisasutuse rolli saab mõni erasektori ettevõte – kuid siin tuleb arvestada võimalusega, et Euroopa küberturvalisuse sertifitseerimise kavas nähakse ette, et nimetatud kavast tuleneva Euroopa küberturvalisuse sertifikaadi võib välja anda üksnes avaliku sektori asutus. Lisaks sellele on ka võimalik olukord, kus akrediteerimisasutus ei ole üldse Eestis – määrusest ei tulene, et vastavushindamisasutused tuleb akrediteerida ilmtingimata Eestis. Sertifitseerimise temaatikaga on seotud ka riiklikud akrediteerimisasutused (vt järgneva paragrahvi selgitusi).

[14] Küberturvalisuse määruse art 58 lg 7.
[15] Küberturvalisuse määruse art 58 lg 4.
[16] Küberturvalisuse määruse lisa 1 (vastavushindamisasutuste suhtes kehtivad nõuded) p 6.
[17] Küberturvalisuse määruse art 60 ja lisa 1.

Vastavushindamisasutus peab lisaks akrediteeringu läbimisele saama ka tegevusloa (vt ka järgneva paragrahvi selgitusi).

Arvestades eeltoodut, toimuks eelnõu järgselt Eestis küberturvalisuse valdkonnas toimuv sertifitseerimise korraldus järgnevalt:



KütS §-ga 13[2] sisustatakse vastavushindamisasutusena tegutsemise ja talle tegevusloa andmise korraldus.

Paragrahvi sisu: vastavushindamisasutusena tegutsemisele ja vastavushindamisasutusele tegevusloa andmisel kohaldatakse toote nõuetele vastavuse seaduse (edaspidi *TNVS*) § 22–33 ja § 35 lõiget 1, arvestades küberturvalisuse määruse nr 2019/881 artiklites 60 ja 61 ning artikli 61 alusel vastu võetud Euroopa Komisjoni rakendusaktis ja sama määruse lisas toodud erisusi. Viidatud TNVS-i sätted juba reguleerivad menetlusnorme, millest lähtuvalt TTJA haldab (st väljastab ja vajadusel tunnistab kehtetuks) vastavushindamisasutusele antavat tegevusluba. Kuna vastavushindamisasutusena tegutsemise ning talle tegevusloa menetlust reguleerivad normid on juba loodud ning TTJA-l tuleb lähtuda küberturvalisuse valdkonna vastavushindamisasutuste korral tegevusluba andes samadest nõuetest, siis puudub vajadus KüTS-s eraldi seda temaatikat reguleerida. Tegevusluba väljastades TTJA kontrollib, kas vastavushindamisasutus vastab küberturvalisuse määruses ja TNVS-is viidatud nõuetele. Küberturvalisuse määruse artiklis 60 ning selle määruse lisas on sätestatud peamised nõuded vastavushindamisasutusele, millega peab vastavushindamisasutus arvestama ning järgima. Enamik küberturvalisuse määruse lisas olevatest nõuetest on samad või võrreldavad TNVS § 28 lõike 1 punktides olevate nõuetega.

Küberturvalisuse määruse artikli 60 lõikes 3 on sätestatud, et kui *„Euroopa küberturvalisuse sertifitseerimise kavades on vastavalt [küberturvalisuse määruse] artikli 54 lõike 1 punktile f sätestatud konkreetsed või täiendavad nõuded, annab riiklik küberturvalisuse sertifitseerimise asutus nende kavade kohaste ülesannete täitmiseks loa üksnes sellistele vastavushindamisasutustele, kes vastavad nimetatud nõuetele“*. Kavandatav § 13[2] lõige 1 annab aimu, et mainitud küberturvalisuse määruse säte kohaldub ka tegevusloa väljastamisel ehk

tegemist on tegevusloa ühe eeltingimusega. Kui varasemalt väljastatud tegevusloa väljastamisel ei kontrollitud Euroopa küberturvalisuse sertifitseerimise kavades olevaid nõudeid, siis tuleb vastavushindamisasutusel uuendada enda tegevusluba.

Riiklikud küberturvalisuse sertifitseerimise asutused teatavad vastu võetud Euroopa küberturvalisuse sertifitseerimise kava puhul Euroopa Komisjonile, millised akrediteeritud ja asjakohasel juhul küberturvalisuse määruse artikli 60 lõike 3 kohaselt loa saanud vastavushindamisasutused võivad anda välja sama määruse artiklis 52 osutatud usaldusväärsuse tasemega sertifikaate.[18] Euroopa Komisjonile teavitamisel lähtutakse küberturvalisuse määruse artiklis 61 lõike 5 alusel vastu võetud Euroopa Komisjoni rakendusaktist, milles määratakse kindlaks teavitamise asjaolud, vormingud ja menetlused. Sel põhjusel ei kohaldata TNVS § 34 sätestatud Euroopa Komisjoni ja teiste liikmesriikide teavitamise protseduuri,

Kui TNVS-is vastavushindamisasutustega seotud nõuded on erinevad küberturvalisuse määruses (sh määruse artiklite alusel kehtestatud Euroopa Komisjoni rakendusaktis) olevatest nõuetest, siis kohaldatakse küberturvalisuse määruse nõudeid.

Vastavushindamisasutuse akrediteerib Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 765/2008, millega sätestatakse akrediteerimise ja turujärelevalve nõuded seoses toodete turustamisega ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93 (ELT L 218, 13.8.2008, lk 30–47), II peatüki nõuetele vastav akrediteerimisasutus.

Küberturvalisuse määruse artikli 2 (mõisted) punktides 15-18 olevate mõistete puhul on viidatud Euroopa Parlamendi ja nõukogu määruses (EL) nr 765/2008 olevatele mõistetele. Üks neist mõistetest on ka riiklik akrediteerimisasutus. Küberturvalisuse määrus riikliku akrediteerimisasutuse määramise osas kaalutlusruumi ei anna[19] – see on seotud määrusega (EÜ) nr 765/2008, konkreetsemalt selle artikli 2 punktiga 11, mille kohaselt akrediteerimisasutuseks saab olla ainult üks akrediteerimist teostav asutus liikmesriigis, kes on selleks riigi poolt volitatud.

Eestis on riiklikuks akrediteerimisasutuseks mittetulundusühing Standardimis- ja Akrediteerimiskeskuse, kes on volitatud seda ülesannet täitma TNVS § 37 lg 2 alusel antud Vabariigi Valitsuse korraldusega[20], struktuuriüksus Eesti Akrediteerimiskeskus (edaspidi *EAK*). Muude Euroopa Liidu liikmesriikide puhul on määratud riiklikuks akrediteerimisasutuseks asutus, mis vastab samuti määruse nr 765/2008 nõuetele.

EAK-l puudub hetkel kompetents ja võimekus küberturvalisuse valdkonnas vastavushindamisasutusi akrediteerida, mistõttu potentsiaalsetel akrediteerimisest huvitatutel peab olema võimalus pöörduda mõne muu riigi akrediteerimisasutuse poole, kes küberturvalisuse valdkonnas akrediteerimisteenust pakub. Riiklik akrediteerimisasutus lähtub uute tehnilisi valdkondade välja arendamisel muuhulgas turunõudlusest ja teenuse isetasuvusest. Tänase EAK võimekuse juures EAK ei ole võimeline oma tegevust küberturvalisuse valdkonda laiendama. Seetõttu on oluline KüTS-s määratleda, et riikliku akrediteerimisasutuse ülesannet võib täita ka muu riigi vastav asutus.

[18] Küberturvalisuse määruse art 61 lg .1

[19] Küberturvalisuse määruse art 60 lg 1.

[20] Vabariigi Valitsuse 09.07.2020 korraldus nr 253 „Volitus Sihtasutuse Eesti Akrediteerimiskeskus lõpetamise otsustamiseks ja Eesti riikliku akrediteerimisasutuse nimetamine“, RT III, 11.07.2020, 3.

Eelnõu koostamise käigus ei uuritud teistelt riikidelt nende valmisolekut ja võimekust vastavushindamise läbi viimiseks, siis tulevikus võib analüüsida, milliste riikidega sel teemal koostööd teha. Seda saab teha ennekõike siis, kui hakkab selguma, milliseid Euroopa Liidu üleseid sertifitseerimiskavu koostatakse ning vastu võetakse. Samuti võib osutuda teenuse suure turunõudluse korral EAK-l otstarbekaks teenus endal välja töötada.

Küberturvalisuse määrusega seotud akrediteerimine toimub TNVS 4. peatüki kohaselt, arvestades küberturvalisuse määruse artikli 60 lõikes 4 ning sama määruse lisas olevaid nõudeid. Riikliku akrediteerimisasutuse regulatsioon tuleneb TNVS 4. peatükist ning selle § 36 järgi akrediteerimist korraldatakse ja tehakse määruse (EÜ) nr 765/2008 II peatükis sätestatu kohaselt.

Kui vastavushindamisasutused vastavad küberturvalisuse määruses sätestatud nõuetele, peaks riiklik akrediteerimisasutus need akrediteerima. Akrediteerida saab maksimaalselt viieks aastaks ja akrediteerimise kehtivust võib pikendada samadel tingimustel seni, kuni vastavushindamisasutus vastab jätkuvalt nõuetele. Riiklik akrediteerimisasutus peaks vastavushindamisasutuse akrediteerimist piirama, selle peatama või kehtetuks tunnistama, kui akrediteerimise andmise tingimused ei olnud täidetud või ei ole enam täidetud või kui vastavushindamisasutus rikub küberturvalisuse määrust.

Küberturvalisuse määruse art 60 lõikes 4 on märgitud, et sama artikli lõikes 1 osutatud vastavushindamisasutuste akrediteerimine kehtib maksimaalselt viis aastat ja selle kehtivust võib pikendada samadel tingimustel, kui vastavushindamisasutus vastab jätkuvalt samas artiklis sätestatud nõuetele. Sama artikli lõike 1 sõnastust arvestades peab vastavushindamisasutus jätkuvalt vastama ka küberturvalisuse määruse lisas olevatele nõuetele. Riiklik akrediteerimisasutus võtab mõistliku aja jooksul kõik asjakohased meetmed, et piirata, peatada või tunnistada lõike 1 kohane vastavushindamisasutuse akrediteerimine kehtetuks, kui akrediteerimise tingimused ei ole täidetud või ei ole enam täidetud või kui vastavushindamisasutus rikub küberturvalisuse määrust.

Mainitud artikli lõike 4 teises lauses nimetatud toimingute teostamine toimub TNVS 4. peatüki kohaselt, arvestades küberturvalisuse määruse artikli 60 lõikes 4 ning sama määruse lisas olevaid nõudeid. Nendeks nõueteks on näiteks, et vastavushindamisasutuse akrediteering kehtib viis aastat. Selles lauses olev „mõistlik aeg“ sõltub konkreetsest olukorrast ning on paljuski seotud asjaoluga, millal akrediteerimise tingimus(t)e mittetäitmisest teada saadakse ning kui kaua läheb aega, et mingi asjakohase meetmeni jõutakse (nt antakse tähtaeg tingimuste uuesti kooskõlla viimiseks või nö viimase meetmena võtta vastavushindamisasutuselt akrediteering ära).

Eelnõu § 1 punktiga 12 muudetakse KüTS § 14 lõike 3 sõnastust. Muudatus on seotud eelnõu § 1 punktiga 10, millega tunnistatakse KüTS § 9 kehtetuks. Kehtiv KüTS § 14 lõige 3 viitab KüTS § 9 lõikele 3, kuid kuna KüTS § 9 tunnistatakse kehtetuks, siis tuleb vastava lõike sõnastust muuta.

Kaitseministeeriumi valitsemisalas rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide nimekiri ning neile süsteemidele kehtestatavad nõuded saavad olema kavandatava KüTS § 7 lõike 5 alusel antud määruses, mille põhilised raamid on sama lõike alusel antud Vabariigi Valitsuse määruses (vt kavandit nimega „Võrgu- ja infosüsteemide küberturvalisuse nõuded“).

Kaitseministri määruse alusel kehtestatud määruses olevate süsteemide ning nende suhtes kehtestatavate nõuete üle teostab riiklikku ja haldusjärelevalvet Kaitseministeerium. Muude Kaitseministeeriumi valitsemisalas olevate süsteemide osas, mis ei ole kaitseministri määruses olevas nimekirjas, teostab riiklikku ja haldusjärelevalvet RIA.

Eelnõu § 1 punktiga 13 lisatakse olemasolevale KüTS §-le 14 lõige 4, milles sätestatakse TTJA pädevus teostada riiklikku ja haldusjärelevalvet küberturvalisuse määruse artikli 58 lõikes 7 sätestatud ulatuses.

Eespool on lisanduva KüTS §-ga 13^1 selgituste juures märgitud vastavad ülesanded. Nende ülesannete ulatuses ongi TTJA-l võimalik teostada riiklikku ja haldusjärelevalvet. Riiklikku järelevalvet teostatakse korrakaitseseaduse (KorS) alusel ning haldusjärelevalvet teostatakse Vabariigi Valitsuse seaduse (VVS) 4. peatüki 6. jaos sätestatud korras.

Riikliku järelevalve teostamisel on TTJA-l võimalik kasutada KorS-s sätestatud riikliku järelevalve üldmeetmeid (vt KorS §-e 23-29) ning KüTS § 15 lõike 1 järgi on tal ka võimalik kasutada riiklikus järelevalvemenetluses samas lõikes nimetatud KorS-i riikliku järelevalve erimeetmeid. TTJA-le kohaldub KüTS § 15 lg 1, kuna eelnõuga lisanduva § 15 lg 4 tõttu on ta samuti korrakaitseorgan KorS § 6 lg 1 tähenduses. TTJA-le ei kohaldu KüTS § 15 lg 2, kuna TTJA ei teosta järelevalvet KüTS §-de 7 ja 8 ning nende alusel kehtestatud õigusaktide nõuete täitmise üle riiklikku järelevalvet – seda teostab RIA.

Eelnõu § 1 punktiga 14 täiendatakse KüTS §-i 16 lõikega 1^1, milles antakse TTJA-le pädevus rakendada riiklikus järelevalvemenetluses küberturvalisuse määruse artikli 58 lõikes 8 sätestatud meetmeid. Meetmete rakendamise eesmärgiks on tagada küberturvalisuse määruses sätestatud nõuete järgimine. Nendeks meetmeteks on:

a) vastavushindamisasutustele, Euroopa küberturvalisuse sertifikaadi omanikele ja ELi vastavusdeklaratsiooni väljaandjatele teabe esitamise korralduse esitamine, mis on vajalik TTJA kui küberturvalisuse sertifitseerimise asutuse ülesannete täitmiseks;
b) vastavushindamisasutuste, Euroopa küberturvalisuse sertifikaadi omanike ja ELi vastavusdeklaratsiooni väljaandjate auditeerimine;
c) vastavalt Eesti õigusele asjakohaste meetmete võtmine tagamaks, et vastavushindamisasutused, Euroopa küberturvalisuse sertifikaadi omanikud ja ELi vastavusdeklaratsiooni väljaandjad järgivad küberturvalisuse määruse ja Euroopa küberturvalisuse sertifitseerimise kava nõudeid;
d) juurdepääsu saamine kõigile vastavushindamisasutuste ja Euroopa küberturvalisuse sertifikaadi omanike ruumidele, et toimetada uurimisi kooskõlas Euroopa Liidu või Eesti menetlusõigusega;
e) Eesti õiguse kohaselt Euroopa küberturvalisuse sertifikaatide kehtetuks tunnistamine, mille on välja andnud riiklik küberturvalisuse sertifitseerimise asutus või vastavushindamisasutus, kui need sertifikaadid ei vasta küberturvalisuse määrusele või Euroopa küberturvalisuse sertifitseerimise kavale;
f) Eesti õiguse kohaselt küberturvalisuse määruses sätestatud nõuete rikkumise eest karistuste määramine ning küberturvalisuse määruses sätestatud kohustuste rikkumise viivitamatu lõpetamise nõudmine.[21]

[21] Küberturvalisuse määruse artikkel 58 lg 8.

Kuna järelevalvatavad subjektid võivad olla nii riiklikud asutused kui ka erasektori ettevõtted, siis nende üle teostatavale järelevalvele kohalduv õigus sõltub järelevalve subjektist.

Eelnõu järgi ei ole riigiasutuse (nt RIA kui vastavushindamisasutuse) üle järelevalve teostamisel võimalik kasutada küberturvalisuse määruse art 58 lõikes 8 olevaid meetmeid, kuid võrdväärsed järelevalvemeetmed tulenevad VVS §-st 75^2. Siiski esitatakse selguse huvides siinses seletuskirjas selgitusi ka haldusjärelevalve kohta – et oleks selge, kas ning mil määral on võimalik vastavaid meetmeid kasutada VVS-i alusel toimuvas haldusjärelevalves.

Punktis a mainitud korralduse all on mõeldud järelepärimist (toiming) kui ka ettekirjutust kui haldusakti haldusmenetluse seaduse (edaspidi *HMS*) tähenduses; olenevalt järelevalve subjektist võib see toimuda nii riiklikus kui ka haldusjärelevalve menetluses. Punktis b mainitud auditeerimine võib toimuda nii riiklikus kui ka haldusjärelevalve menetluses. Punktis c mainitud meetmete võtmine võib tähendada ettekirjutuste tegemist ning asjakohasel juhul ka sunniraha määramist (vt riikliku järelevalve puhul ka KorS §-e 26-29 ning asjakohasel juhul ka kasutatavaid riikliku järelevalve erimeetmeid; haldusjärelevalve osas vt VVS § 75^1 lõikeid 3 ja 4; sunniraha osas vt lisanduva KüTS § 17^1 selgitusi). Punktis d märgitud juurdepääsu saamine toimub riiklikus järelevalves KorS §-de 49-51 kohaselt ning haldusjärelevalve puhul VVS § 75^2 lg 1 punktide 3-5 kohaselt. Punktis e märgitud Euroopa küberturvalisuse sertifikaadi kehtetuks tunnistamine toimub haldusakti tegemise kaudu. Punktis f mainitud karistuste osas vt lisanduva KüTS § 18^1 selgitusi; küberturvalisuse määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist saab teha nii teavitusega või soovitusega (vt nt KorS § § 26 lg 1; tegemist pole haldusaktiga) kui ka ettekirjutusega (vt ka siinses tekstilõigus märgitud punkti c selgitusi).

Eelnõu § 1 punktiga 15 täiendatakse seadust §-dega 17^1 (sätestab sunniraha määra) ja 17^2 (sätestab kaebuse läbivaatamise tähtaja).

KüTS § 17^1 määratleb sunniraha määra ettekirjutuse korral. Asendustäitmise ja sunniraha seaduse § 10 lõike 2 järgi sätestab sunniraha igakordse rakendamise ülemmäära seadus. Eelnõuga määratakse sunniraha 100 000 eurot.

Küberturvalisuse määruse art 58 lg 8 punkti c arvestades peab TTJA-l olema volitus „*võtta asjakohaseid meetmeid vastavalt liikmesriigi õigusele tagamaks, et vastavushindamisasutused, Euroopa küberturvalisuse sertifikaadi omanikud ja ELi vastavusdeklaratsiooni väljaandjad järgivad käesoleva määruse ja Euroopa küberturvalisuse sertifitseerimise kava nõudeid*“. Vastavate nõuete tagamiseks saabki TTJA teha ettekirjutuse (korralduse) ning vajadusel teha ettekirjutuses ka sunniraha määramise hoiatuse või määrata sunniraha, kui ettekirjutust ei täideta.

Sunniraha suuruse ülemmäära (100 000 eurot) määratlemisel arvestati TTJA antud tagasisidet, mille kohaselt oleks eelnevalt mainitud ülemmäär piisav, mis vajadusel motiveeriks vastavushindamisasutust, Euroopa küberturvalisuse sertifikaadi omanikku ja ELi vastavusdeklaratsiooni väljaandjat lähtuma küberturvalisuse määruse ja tulevikus konkreetse valdkonna osas vastu võetava Euroopa küberturvalisuse sertifitseerimise kava nõuete kohaselt.

Käesoleval hetkel on RIA-l ning Kaitseministeeriumil võimalik sunniraha määrata ettekirjutuse täitmata jätmise korral kuni 9600 eurot.[22] Eelnõu tulemusena sunniraha ülemmäär suureneb 100 000 euroni, mis omakorda motiveerib nimetatud valitsusasutuste järelevalve subjekte lähtuma KüTS-i ning selle alusel antud õigusaktide nõuete kohaselt. Sunniraha kui meetme rakendamist toetab kaudselt ka Euroopa Parlamendi ja Nõukogu direktiiv nr 2016/1148, mis on üle võetud KüTS-i.[23]

Sunniraha ülemmäär võimaldab TTJA-l efektiivselt sekkuda küberturvalisuse sertifitseerimisega seotud nõuete rikkumisel. Sama on ka eelnõu järgselt RIA ning Kaitseministeeriumi puhul, kui nad kontrollivad küberturvalisuse nõuete täitmist. Näiteks, kui eesmärk on ettekirjutusega nõuda küberturvalisuse määruses sätestatud kohustuste rikkumise viivitamatut lõpetamist ning selle nõude täitmise tagamiseks tehakse samas ettekirjutuses ka sunniraha määramise hoiatus – kui ettekirjutust kohaselt ei täideta, siis kohaldatakse sunniraha.

Sunniraha kasutamine ettekirjutuse osana (sunniraha hoiatusena) sõltub järelevalvatavast isikust. Järelevalveasutusel on võimalik riiklikus järelevalves eelnõuga märgitud sunniraha ülemmäära kasutada; haldusjärelevalvemenetluse korral on sunniraha võimalik kasutada ainult teise haldusekandja suhtes, kuid mitte riigiasutuste (näiteks, kui TTJA teostab järelevalvet RIA) suhtes (vt VVS § 75^1 lõiget 4).

Järelevalveasutus peab sunniraha määramisel hindama, millises määras sunniraha rakendamine on Eesti kontekstis proportsionaalne.

KüTS § 17^2 määratleb kaebuse läbivaatamise tähtaja. Paragrahv koosneb kahest lõikest – esimene lõige määratleb üldise kaebuse läbivaatamise tähtaja ning teine lõige määratleb olukorrad, mil kaebuse lahendamise tähtaega võidakse pikendada.

Küberturvalisuse määruse artikli 63 ja eelnõu järgi käsitleb TTJA füüsiliste või juriidiliste isikute kaebusi seoses Euroopa küberturvalisuse sertifikaatidega, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused või kooskõlas küberturvalisuse määruse artikli 56 lõikega 6 vastavushindamisasutused, või seoses küberturvalisuse määruse artikli 53 kohaselt välja antud ELi vastavusdeklaratsioonidega, ning uurib asjakohasel määral nende kaebuste sisu ja teavitab kaebuse esitajat mõistliku aja jooksul uurimise käigust ja tulemusest.

Küberturvalisuse määruses ei ole ette nähtud tähtaeg, mis aja jooksul tuleb esitatud kaebus läbi vaadata (teostada järelevalvet) – seda tuleb teha mõistliku aja jooksul. Õigusselguse huvides määratletakse, et TTJA peab esitatud kaebuse lahendama hiljemalt 90. päeval kaebuse saamisest arvates (**lõige 1**).

90 kalendripäevane tähtaeg on piisav aeg, mis võimaldaks TTJA-l uurida esitatud kaebusega seotud asjaolusid. Tähtaja pikkus on seotud menetlustoimingutega: esmajärjekorras on vajadus küsida Euroopa küberturvalisuse sertifikaadi väljastanud asutuselt või isikult selgitusi esitatud kaebuse sisu kohta, sh vajadusel esitada ka mitu järelepärimist, kui esmaste vastuste põhjal ei ole võimalik kaebust lahendada; kõigi järelepärimiste korral tuleb anda järelepärimise adressaadile ka piisav aeg vastuste koostamiseks ja edastamiseks TTJA-le; olenevalt kaebuse sisust, võib tekkida ka vajadus küsida ka muu riigi riiklikult küberturvalisuse sertifitseerimise

[22] Eelnõuga muudetakse KüTS § 14 lõike 3 sõnastust, mille tulemusena ei ole Kaitseväel järelevalve teostamise õigust.
[23] Euroopa Parlamendi ja Nõukogu 6. juuli 2016. a määrus nr 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus; vt viidatud määruse artikleid 15 ja 17.

asutuselt seisukohti või arvamust, millele tuleb samuti anda piisav vastamistähtaeg (vt ka lõike 2 selgitust). Lühemat tähtaega ei ole mõistlik määrata (nt 30 päeva), kuna kui menetlus kestab, siis tuleks perioodiliselt (nt iga 30 päeva möödumisel) esitada kaebuse esitajale teavitus menetluse tähtaja pikendamise kohta, mis omakorda suurendaks TTJA halduskoormust. Kui esitatud kaebus on puudustega, siis lähtutakse HMS §-st 15, sh on võimalik TTJA-l esimesel võimalusel määrata tähtaeg kaebuses esinenud puuduste kõrvaldamiseks.

Lõikes 2 määratletakse lõikes 1 oleva tähtaja pikendamise võimalus. Kui kaebuse lahendamiseks on vaja teha koostööd teise riigi riikliku küberturvalisuse sertifitseerimise asutusega, on TTJA-l õigus pikendada kaebuse läbivaatamise tähtaega aja võrra, mis on vajalik asutuse arvamuse ärakuulamiseks. Kaebuse läbivaatamise tähtaja pikendamisest teavitatakse kaebuse esitajat kirjalikult.

Kaebuse lahendamisel võib tekkida vajadus kaasata või teha koostööd teise liikmesriigi riiklikku küberturvalisuse sertifitseerimise asutusega. Kuna selle asutuse kaasamine, tema enda seisukohtade kujundamine võib võtta aega, siis võib menetlusele kuluv aeg olla pikem kui on käesoleva paragrahvi lõikes 1 ette nähtud 90 päeva. Seetõttu nähakse võimalus pikendada kaebuse läbi vaatamise tähtaega.

Eelnõu § 1 punktiga 16 lisatakse seadusesse § 18^1, millega sätestatakse väärteokaristused.

Liikmesriigile on küberturvalisuse määruse 3. jaotises (küberturvalisuse sertifitseerimise raamistik) antud kohustus kehtestada küberturvalisuse sertifitseerimise raamistiku ja Euroopa küberturvalisuse sertifitseerimise kavade rikkumise korral kohaldatavad karistusnormid ning võtta kõik vajalikud meetmed nende rakendamise tagamiseks. Kehtestatud karistused peavad olema tõhusad, proportsionaalsed ja hoiatavad. Määrus ei anna ette karistuse rahatrahvi miinimum või maksimumpiiri. Rahatrahvi suurus on seega liikmesriigi enda otsustada. Samuti võib teha eri karistusnormid eri kohustuste rikkumise puhuks.[24]

Eelnõu järgi on nii füüsilisele kui juriidilisele isikule võimalik määrata rahatrahvi väärteomenetluse korras küberturvalisuse määruses sätestatud nõuete mittetäitmise eest. Eelnõu kohaselt on KüTS-i alusel väärteomenetluses võimalik rahatrahvi määrata:

- küberturvalisuse määruse artikli 53 lõikes 2 sätestatud tingimustele mittevastava vastavusdeklaratsiooni väljastamise eest; või
- küberturvalisuse määruse artikli 55 lõikes 1 nimetatud teabe korral sama artikli lõikes 2 sätestatud nõuete rikkumise.

Küberturvalisuse määruse artikli 53 lõike 2 sisu: *„IKT-toodete, -teenuste või -protsesside tootja või pakkuja võib anda välja ELi vastavusdeklaratsiooni, milles kinnitatakse, et [Euroopa küberturvalisuse sertifitseerimise] kavas esitatud nõuded on täidetud. ELi vastavusdeklaratsiooni väljaandmisega võtab IKT-toodete, -teenuste või -protsesside tootja või pakkuja vastutuse IKT-toote, -teenuse või -protsessi vastavuse eest kõnealuses kavas sätestatud nõuetele“.*

Seletuskirja koostamise seisuga on ENISA valmistanud ette pilveandmetöötlusteenustega seotud EL-i küberturvalisuse sertifitseerimise kava ning ettevalmistamisel on eraldi EL-i

[24] Küberturvalisuse määruse art 65.

küberturvalisuse sertifitseerimise kava ka 5G mobiilsidevõrgu standardi funktsiooniga võrkudega jaoks.[25]

Küberturvalisuse määruse artikli 55 lõige 1 sisustab, mida *„[s]ertifitseeritud või ELi vastavusdeklaratsiooni saanud IKT-toodete, -teenuste ja -protsesside tootja või pakkuja teeb avalikkusele kättesaadavaks“*. Selleks teabeks on:

a) suunised ja soovitused, mis aitavad lõppkasutajal IKT-tooteid või -teenuseid turvaliselt konfigureerida, paigaldada, kasutusele võtta ning neid käitada ja hooldada;
b) ajavahemik, mille jooksul pakutakse lõppkasutajatele turvalisuse alast tuge, eelkõige võimaldades saada küberturvalisuse alaseid uuendusi;
c) tootja või pakkuja kontaktandmed ja aktsepteeritavad viisid lõppkasutajatelt ja küberturvalisusega tegelevatelt teadlastelt turvanõrkuste kohta teabe saamiseks;
d) viited internetis asuvatele andmebaasidele, kus on loetletud IKT-toote, -teenuse või -protsessiga seotud avalikult teada antud turvanõrkused ja asjakohased küberturvalisuse alased nõuanded.

Sama artikli lõike 2 kohaselt peab see teave *„olema kättesaadav elektroonilisel kujul ning see peab olema kättesaadav ja seda tuleb ajakohastada vajaduse korral vähemalt kuni vastava Euroopa küberturvalisuse sertifikaadi või ELi vastavusdeklaratsiooni kehtivuse lõppemiseni“*.

TTJA peab igal juhul hindama, kas väärteomenetluse läbiviimine ning trahvi määramine on konkreetse rikkumise olemust ja iseloomu arvestades on vajalik ja proportsionaalne. Tegemist on kaalutlusõigusega ehk TTJA kui järelevalveasutus peab tegema kaks erinevat kaalutlusotsust. Esiteks, tuleb otsustada kas konkreetse rikkumise korral on väärteomenetluse alustamine vajalik ning proportsionaalne või on teiste järelevalvemeetmete rakendamine tõhusam. Siin tuleb väärteomenetluse algatamise otsustamisel lähtuda väärteomenetluse seadustiku (VTMS) §-st 3^1, mis sätestab väärteomenetluse kohustuslikkuse põhimõtte. Teiseks, juhul kui järelevalveasutus otsustab alustada väärteomenetlust, tuleb erinevaid tegureid arvesse võttes otsustada määratava trahvi suurus.

Paragrahvis on seatud rahalise karistuse ülempiir, milleks on füüsilise isiku puhul 200 trahviühikut ja juriidilise isiku puhul 20 000 eurot. Ülemmäärade seadmisel on võetud eeskuju KüTS §-st 18, mis omakorda lähtus hädaolukorra seaduse 8. peatükis sätestatud väärteokoosseisude rahatrahvide ülemmäärast. Nagu ka KüTS-is kehtestatud küberturvalisuse tagamise ja kehtestatud nõuded on suunatud kindlatele isikutele, siis ka küberturvalisuse sertifitseerimise nõuded puudutavad vaid IKT-toodete, -teenuste ja -protsesside tootjaid. Seetõttu on vaja kehtestada piisavalt kõrged trahvimäärad, mis suudaksid tagada sertifitseerimisnõuete meetmete eesmärgi realiseerumist.[26] Näiteks Slovakkias ulatuvad samad karistusmäärad 300 000 euroni.

Ka NIS direktiivi ülevõtmisel, mille Eesti võttis üle KüTS-iga, on liikmesriigid kehtestanud erinevates suurustes trahvimäärasid. Iirimaal on väärteo eest trahvimäär 4000 kuni 5000 eurot,

[25] Leitavad vastavalt: https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes/ ning https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.
[26] Seletuskiri küberturvalisuse seaduse eelnõu juurde, 597 SE, lk 33.

seejuures kuriteo eest on karistusraam füüsilisele isikule maksimaalselt 50 000 ning juriidilisele isikule 500 000 eurot.[27] Poolas on karistusmäärad vastavalt kuni 50 000 või 230 000 eurot.[28]

Tulevikus on võimalik hinnata, kas KüTS §-s 18 ning eelnõuga lisanduva § 18[1] väärteokoosseisude rahatrahvide suurusi tuleks suurendada. Seda on võimalik teha uue küberturvalisuse direktiivi üle võtmise käigus (nn NIS 2 direktiiv; hetkel ettepaneku staatuses).[29] NIS 2 direktiivi ettepanekus on rahatrahvide suurused märgatavalt tõusnud – direktiivi ettepaneku kohaselt tuleb teatud isikutele määrata NIS 2 direktiivi nõuete rikkumise korral määrata haldustrahv, mille maksimummäär on *„vähemalt 10 000 000 eurot või kuni 2 % (olenevalt sellest, kumb summa on suurem) selle ettevõtja ülemaailmsest aastasest kogukäibest, kellele oluline üksus eelneval majandusaastal kuulub"* (vt ettepaneku artikkel 31 lõiget 4). Seetõttu on sobilikum teostada KüTS-s olevate süüteokoosseisude eest ette nähtavate väärteokaristuste määrade üle vaatamine, kas KüTS-i revisjoni või NIS 2 direktiivi üle võtmise käigus. Nimetatud muudatuste tegemine oleks ka seotud Eesti õigusesse haldustrahvi instituudi loomisega.

Kuivõrd eelnõu järgi määratakse küberturvalisuse määruse nõuete rikkumisega ette nähtud „karistusi" väärteomenetluse raames, tuleb lähtuda väärteomenetluse üldreeglitest. VTMS § 3 lg 1 selgitab, et väärteomenetlusõigus kehtib füüsilise ja juriidilise isiku suhtes. Ainult kirjalikku hoiatamismenetlust (VTMS § 54[1]) kohaldatakse ka riigi, kohaliku omavalitsuse ja avalik-õigusliku juriidilise isiku suhtes – kuid siinsete rikkumiste olukorras pole võimalik kirjalikku hoiatamismenetlust kasutada. Seega eelnõuga ettenähtud väärteotrahve ei ole võimalik kohaldada riigiasutuse (nt RIA) suhtes.

Eelnõu § 1 punktiga 17 täiendatakse KüTS §-i 19 lõikega 1[1], millega sätestatakse, et paragrahvis 18[1] sätestatud väärteo kohtuvälise menetlejaks on TTJA. Selle sättega antakse riikliku küberturvalisuse sertifitseerimise asutusele pädevus määrata rahalisi karistusi vastavate küberturvalisuse määruse nõuete rikkumise eest.

Eelnõu § 1 punktiga 18 jäetakse KüTS § 21 punktist 1 välja sõnad „käesoleva paragrahvi lõike 1 punktis 10 sätestatud ülesande täitmiseks kasutatavate". Nimetatud paragrahviga soovitakse teha muudatus Eesti Rahvusringhäälingu seadusesse, mis jõustub KüTS § 29 lõike 3 tõttu 1. jaanuaril 2022. a.

Eelnõu § 1 punkti 3 juures on selgitatud, miks tehakse muudatusi KüTS § 3 lõikes 1 sätestatud teenuse osutajate sõnastustes. Nimetatud muudatuse tõttu tuleb ka teenuse osutaja tegevust reguleeriva eriseaduse, kus on viited KüTS §-de 7 ja 8 kohaldumisele, sõnastus viia kooskõlla kavandatava KüTS § 3 lõikega 1. Kuna nimetatud muudatus ei ole veel jõustunud ning Eesti Rahvusringhäälingu kui teenuse osutaja kohta käivas eriseaduses tehakse muudatus KüTS-is oleva paragrahviga, tulebki muuta KüTS-s oleva paragrahvi sõnastust, et valdkondlik seadus oleks ülejäänud eelnõuga kooskõlas.

Muudetav õigusnorm on rohkem teavitusliku kui regulatiivse sisuga. Kuivõrd Eesti Rahvusringhääling on teenuse osutaja KüTS § 3 lõike 1 punkti 10 alusel, siis kohaldatakse

[27] Bird&Bird&, jaanuar 2020. Developments on NIS Directive in EU Member States, lk 28 https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf
[28] Ibid, lk 37.
[29] Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv 2016/1148 – leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52020PC0823.

küberturvalisuse nõudeid KüTS-i teenuse osutaja kohustusi reguleerivate sätete alusel. Õiguslikku mõju ei omaks ka alternatiivselt Eesti Rahvusringhäälingu seaduses § 5 lõike 2^1 ning § 34 lõike 4^1 kehtestamata jätmine.

Eelnõu § 1 punktiga 19 jäetakse KüTS § 28 punktis 1 välja sõnad „üldarstiabi osutamisel kasutatava". Nimetatud punktiga soovitakse teha muudatus tervishoiuteenuste korraldamise seadusesse, mis jõustub KüTS § 29 lõike 3 tõttu 1. jaanuaril 2022. a.

Eelnõu § 1 punkti 3 juures on selgitatud, miks tehakse muudatusi KüTS § 3 lõikes 1 sätestatud teenuse osutajate sõnastustes. Tolle muudatuse tõttu tuleb ka teenuse osutaja tegevust reguleeriva eriseaduse, kus on viited KüTS §-de 7 ja 8 kohaldumisele, sõnastus viia kooskõlla kavandatava KüTS § 3 lõikega 1. Kuna nimetatud muudatus ei ole veel jõustunud ning perearsti ehk teenuse osutaja kohta käivas eriseaduses tehakse muudatus KüTS-is oleva paragrahviga, tulebki muuta KüTS-s oleva paragrahvi sõnastust, et valdkondlik seadus oleks ülejäänud eelnõuga kooskõlas.

Muudetav õigusnorm on rohkem teavitusliku kui regulatiivse sisuga. Kuivõrd perearst on teenuse osutaja KüTS § 3 lõike 1 punkti 7 alusel, siis kohaldatakse küberturvalisuse nõudeid KüTS-i teenuse osutaja kohustusi reguleerivate sätete alusel. Õiguslikku mõju ei omaks ka alternatiivselt tervishoiuteenuste korraldamise seaduses § 10 muudatuste ning § 60 lõike 2 muudatuste kehtestamata jätmine.

Eelnõu §-ga 2 muudetakse avaliku teabe seadust.

Eelnõu § 2 punktiga 1 tunnistatakse kehtetuks AvTS § 43^9 lg 1 punkt 4 ehk ISKE määruse volitusnorm.

Eesti infoturbealases õigusruumis on probleemiks üksnes andmekogudele fokusseeritud infoturbeparadigma, mis vajab lahendamist. Kehtiv regulatsioon on üles ehitatud andmekogude põhisele infoturbe tagamise süsteemile. ISKE-t rakendatakse andmekogudes sisalduvate andmete töötlemiseks kasutatavatele infosüsteemidele ja seega keskendub ISKE kitsalt andmekogudes sisalduvate andmete kaitsmisele. See lähenemine on loonud olukorra, kus turvameetmete rakendamisel on rakendaja perspektiiv sageli ebaproportsionaalselt kitsas, jättes turvameetmed rakendamata paljude oluliste infosüsteemide osas, mis ei kujuta AvTS-i tähenduses andmekogu.

Asutused on praktikas sageli jätnud ISKE rakendamata, kui võrgu- ja infosüsteemi defineerimiseks oli võimalik leida mistahes muu definitsioon, kui „andmekogu" AvTS-i tähenduses. KüTS-i jõustumine küll leevendas olukorda, tuues Eesti õigusesse oluliselt laiema „võrgu- ja infosüsteemi (süsteemi)" termini koos sellega kaasneva riskianalüüsi nõudega, kuid KüTS süsteemide osas eriregulatsiooni kehtestamine AvTS-i määrusesse ei ole täna võimalik. Õigusselguse ja infosüsteemide turvalisuse tagamise huvides on siiski erisused andmekogude ning teiste süsteemide osas selgelt välja tuua ja korrektselt reguleerida. Andmekogude pidamiseks kehtestatud turvameetmete süsteemilt üleminek avalike ülesannete täitmiseks loodud äriprotsesside põhisele infoturbe haldussüsteemile tuleb sätestada ka õigusaktides.

Kehtetuks tunnistatava punkti alusel on antud Vabariigi Valitsuse määrus „Infosüsteemide turvameetmete süsteem". See volitusnorm on AvTS-s andmekogudel põhinev, kuid reaalsuses rakendatakse sama määrust kõigile riigi ja kohaliku omavalitsuse süsteemidele. ISKE-t pole 2017. aastast saadik täiendatud, mistõttu on tekkinud vajadus infoturbe halduse süsteemi järele, mis pole ainult andmekogude, vaid võrgu- ja infosüsteemide (mille hulgas on ka andmekogud)

põhiseks. Seetõttu on mõistlik muuta KüTS-s olev norm, mis praegu viitab AvTS-i andmekogude põhisele volitusnormile, ise volitusnormiks KüTS §-s 7 (vt eelnõu § 1 punkti 8). Sellisel viisil on võimalik tulevikus Vabariigi Valitsuse määrust „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ sisustada nii andmekogude kui ka võrgu- ja infosüsteemide kaitse seisukohalt. Kuna eelnõuga luuakse KüTS-s võimalus kehtestada E-ITS, siis tuleb ISKE määruse volitusnorm tunnistada kehtetuks. Üleminekuperioodi jooksul (kuni 31. detsembrini 2022. a – vt eelnõu § 10 lõiget 2 ja selle selgitusi) kehtivad ISKE ja E-ITS-i nõuded samaaegselt, et oleks võimalik lihtsamini võimalik üle minna ISKE-lt E-ITS-le.

Eelnõu § 2 punktiga 2 muudetakse AvTS § 43^9 lõike 3 teise lause sõnastust. Uus sõnastus on: „Käesoleva seaduse § 43^3 lõikes 4 nimetatud andmekogu pidamisele on kohustuslikud käesoleva paragrahvi lõike 1 punktides 1, 2 ja 6 nimetatud kindlustavad süsteemid.“.

Punktiga kaotatakse viide kehtetuks tunnistatud süsteemile (vt eelnõu § 2 punkti 1) ehk AvTS § 43^9 lg 1 punktile 4. Kuna nimetatud kindlustava süsteemi ehk ISKE määruse volitusnorm tunnistatakse kehtetuks, siis tuleb teha ka muudatus AvTS § 43^9 lõike 3 teises lauses.

Eelnõu § 2 punktiga 3 muudetakse AvTS § 53^1 lõike 1 sõnastust. Uus sõnastus on: Riigi Infosüsteemi Amet teostab riiklikku ja haldusjärelevalvet infosüsteemide andmevahetuskihiga liitumise üle“.

Muudatuse tulemusena ei ole nimetatud lõikes edaspidiselt lauseosa „infosüsteemide turvameetmete süsteemi rakendamise ning“, mille sisu on seotud ISKE-ga. Muudatus on vajalik, kuna ISKE kui kindlustava süsteemi pidamist reguleeriva määruse volitusnorm tunnistatakse kehtetuks (vt eelnõu § 2 punkti 1).

Eelnõu §-des 3-8 muudetakse seadusi, kus turvanõuete rakendamise kohustuses varasemalt viidati HOS-le ning mis KüTS-i kehtestamisega seotud rakendussätetega muudeti viideteks KüTS-le. Sätetest jäetakse välja sõnad „teenuse osutamiseks kasutatava“ või selle ekvivalent.

Eelnõu § 1 punkti 3 juures on selgitatud, miks tehakse muudatusi KüTS § 3 lõikes 1 sätestatud teenuse osutajate sõnastustes. Tolle muudatuse tõttu tuleb ka teenuse osutaja tegevust reguleeriva eriseaduse, kus on viited KüTS §-de 7 ja 8 kohaldumisele, sõnastus viia kooskõlla kavandatava KüTS § 3 lõikega 1. Muudatusega viiakse teenuse osutaja kohta käiva valdkondliku seaduse sõnastus ülejäänud eelnõuga kooskõlla.

Muudetavad õigusnormid on rohkem teavitusliku kui regulatiivse sisuga. Kuivõrd KüTS § 3 lõige 1 sätestab, kes on teenuse osutajad selle seaduse tähenduses, siis kohaldatakse ka muudetavates rakendussätetes viidatud seaduse kaudu defineeritud isikutele küberturvalisuse nõudeid just KüTS-i teenuse osutaja kohustusi reguleerivate sätete alusel.

Õiguslikku mõju ei omaks ka alternatiivselt elektroonilise side seaduse § 100^3 lõike 3, § 100^4 lõike 2, § 100^5 lõike 2 § 133 lõike 5 teise poole, hädaolukorra seaduse § 41 lõike 1, lennundusseaduse § 59^1, § 60^1 lõike 5, raudteeseaduse § 8, § 143 lõike 1 punkti 6 ning lõike 8, sadamaseaduse § 13 lõike 4, § 42 lõike 5 ning tervishoiuteenuste korraldamise seaduse § 17 lõike 1^2, § 22 lõike 4^2 ning § 60 lõike 2 kehtetuks tunnistamine.

KüTS-i kohaldamisala on määratletud KüTS-i §-s 3. Muudes seadustes sätestatud viited KüTS nõuete kohaldamisele ei saa kehtida osas, kus need kitsendaks KüTS-s sätestatud kohaldamisala.

Eelnõu §-ga 9 tehakse täiendus VVS-s, mille § 63 lõikes 1 asendatakse sõna „haldamine“ sõnadega „haldamine; avaliku sektori digiarengu ning üleriigilise küberturvalisuse tagamise juhtimine, korraldamine ja järelevalve“.

Eelnõu tulemusena uuendatakse VVS-i sõnastust, et oleks selgelt reguleeritud, et Majandus- ja Kommunikatsiooniministeeriumi valitsemisalaga on seotud avaliku sektori digiarengu ja üleriigilise küberturvalisuse tagamisega seotud teemad. Muudatus on seotud ka eelnõu § 1 punktiga 8, mille tulemusena lisandub KüTS-i § 7 lõige 5 ehk volitusnorm Vabariigi Valitsuse määruse (vt eelnõule lisatud kavandit) kehtestamiseks. Tolles määruses on sätestatud edasivolitus, et E-ITS-i kehtestab üleriigilise küberturvalisuse tagamise korraldamise eest vastutav minister enda määrusega. Selleks ministriks on ettevõtlus- ja infotehnoloogiaminister.

Eelnõu § 10 sätestab seaduse jõustumise kuupäeva, milleks on 1. jaanuar 2022. a.

Erandina jõustub seaduse § 2, mille jõustumise kuupäevaks on 1. jaanuar 2023. a. Jõustumistähtaja pikendamine on seotud ISKE rakendajatele ülemineku võimaldamiseks auditite läbiviimsel. Kuni 2022. aasta lõpuni on ISKE auditeerimiskohuslastel võimalus viia läbi turvameetmete rakendamise auditeerimine ISKE reeglite järgi. Selleks, et tagada küberturvalisuse nõuete järgimise püsiv kontroll, on eelnõu § 1 punkti 8 alusel kavandatava Vabariigi Valitsuse määruse alusel E-ITS reeglite järgi auditeerimiskohustus varasematel ISKE kohuslastel hiljemalt viimase läbiviidud ISKE auditi aegumisel ning eelnõu § 2 hilisem jõustumine võimaldab seega tellida 2022. aastal audit ISKE reeglite järgi, kui peaks olema vajadus E-ITS-i esmakordse auditi tähtaega pikendada.

1. jaanuar 2022. a kuni 1 jaanuar 2023. a on seetõttu kohaldatavad nii ISKE kui ka E-ITS nõuded, aga kuivõrd E-ITS tingimuste järgimisel on sisuliselt tagatud ka ISKE nõuete järgimine, siis ei ole käesoleva eelnõu jõustumisskeem ISKE nõuete järgijate suhtes täiendavalt koormav.

Seaduse ning selle alusel kavandatavate määruste järgi oleks teenuse osutajale sätestatud kohustuste täitmine nõutav alates 1. jaanuarist 2022. a. Olgu siinkohal mainitud, et E-ITS-i kehtestamine alates 1. jaanuarist 2022. aastal tähendab küll kohustust alustada E-ITS tingimuste järgimist (nt infoturbeprotsessi läbiviimist), kuid ei tähenda, et teenuse osutaja peab juba samal päeval olema rakendanud E-ITS tingimuste järgimisest tulenevad turvameetmed.

3.2. Muude riikide regulatsioonid

3.2.1. Kavandatav muudatus: E-ITS-i kehtestamine

ISKE uuendamine on juba aastaid peatunud, kui alusstandardiks olnud Saksa versiooni uuendused lõpetati. Seetõttu tekkiski vajadus E-ITS luua ja kehtestada. Ka Saksamaa on välja andnud uue infoturbe haldamise süsteemi (ISMS) nimetusega IT-Grundschutz, mis on võrreldav standardiga ISO/IEC 27001.[30] Eelnõu koostades ei analüüsitud muude riikide regulatsioone.

3.2.2. Kavandatav muudatus: küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramine ja sellega seotud ülesannete korraldus

[30] Lisainfo: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html;jsessionid=1D6D810F4B804204B0D9ED9AB4864E6B.internet082.

Eelnõu koostamise hetkel ei ole EL-i liikmesriigid enda riikides lõpule viinud riikliku koordineerimiskeskuse määratlemisega seotud toiminguid, sh ka õigusloomeliselt. Hetkel on teada, et mõni riik on otsustanud selle keskuse ülesanded anda ministeeriumile, mõnes riigis kavatsetakse see anda mitmele asutusele (tehakse koostöölepe vms, kuid Euroopa Komisjonile antakse üles ühe asutuse nimi). Seetõttu ei ole ka hetkel võimalik tuua selget ülevaadet teiste riikide regulatsioonidest. Seda enam, et Euroopa Komisjon on alles koostamas suuniseid, mis peaksid hõlbustama riikliku koordineerimiskeskuse määramist, kuid nende koostamisega alustati 2021. a suvel ning konkreetsem selgus suuniste sõnastuste osas saabub alles 2021. a sügisel.

3.2.3. Kavandatav muudatus: küberturvalisuse sertifitseerimise korralduse reguleerimine

Eelnõu koostamisel on lähtutud paljuski **Soome** eeskujust. Soome valitsus on küberturvalisuse määruses sätestatud riikliku küberturvalisuse sertifitseerimise asutuse loomise kohustuse täitmiseks teinud parlamendile elektroonilise side seaduse muutmise ettepaneku, mille kohaselt pannakse riikliku küberturvalisuse sertifitseerimise asutuse kohustused Soome Transpordi- ja Sideametile. Seda seetõttu, et ameti all tegutsevas Soome küberturvalisuse keskuses juba tegutsetakse küberturvalisuse alal.[31] Samuti on Soome küberturvalisuse keskus (SKK) Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/1148 artikli 8 lõikes 3 mõttes võrgu- ja infosüsteemide turbe vallas Soome riiklik ühtne kontaktpunkt. Selles osas on SKK analoogne Eesti RIA-ga. Soome hinnangul ei oma küberturvalisuse määrusest tulenev riikliku küberturvalisuse sertifitseerimise asutuse määramine olulist mõju riigi rahandusele, majandusele, kodumajapidamistele ega ka ettevõttetele, kuna sertifitseerimine on esialgu vabatahtlik. Samas mõjutavad Soome tehnoloogiaettevõtete konkurentsivõimet Euroopa sertifitseerimissüsteemi nõuded ja asjaolu, kui hästi vastavad Soome ettevõtete tooted Euroopa sertifitseerimissüsteemi nõuetele.

Küpros planeerib riikliku sertifitseerimise asutuse rolli anda Digitaalse Turvalisuse Ametile (*Digital Security Authority, Αρχή Ψηφιακής Ασφάλειας*).[32]

Slovakkia seaduseelnõu kohaselt saab riiklikuks sertifitseerimise asutuseks Riiklik Turvalisuse Amet (*Národný bezpečnostný urad, National Security Authority*). Slovakkia seaduseelnõus on karistuste puhul eristatud küberturvalisuse määruse paragrahvid:

- Artiklis 53 sätestatud vastavushindamise deklaratsiooni väljastamise eest vastuolus määrusega, karistatakse ettevõtjat rahatrahviga 300 kuni 100 000 eurot.
- Kui vastavusdeklaratsiooni väljastanud ettevõtja jätab vastavusdeklaratsiooni elektroonilises vormis avaldamata või ei uuenda määruse artiklis 51(1) punktides a-d nimetatud teavet, karistatakse rahatrahviga 300 kuni 100 000 eurot.
- Vastavushindamisasutust, Euroopa küberturvalisuse sertifikaadi omanikku ja ELi vastavusdeklaratsiooni väljaandjat selle eest, kui a) ei anta riiklikule küberturvalisuse sertifitseerimise asutusele artikkel 58(8)(a) kohast teavet; b) takistab riiklikul küberturvalisuse sertifitseerimise asutusel auditi vormis uurimist vastavalt artiklile 58(8)(b), karistatakse 300 kuni 100 000 euroga.

[31] HE 98/2020 vp, lk 118.
[32] Kättesaadav: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2019-eu-ia-0109.

- Vastavushindamisasutust, Euroopa küberturvalisuse sertifikaadi omanikku ja ELi vastavusdeklaratsiooni väljaandjat karistatakse 300 kuni 100 000 euroga, kui ta ei võimalda riiklikule sertifitseerimise asutusele ligipääsu oma ruumidele vastavalt määruse artiklile 58(8)(d).[33]

4. Eelnõu terminoloogia

Eelnõu § 1 punktiga 2 lisandub KüTS-i §-i 2 termin „turvameetmed“, mille sisu on: rakendatavad organisatsioonilised, füüsilised ja infotehnilised toimingud või vahendid andmete ja süsteemide turvalisuse saavutamiseks ja säilitamiseks.

Eelnõus kasutatakse ka termineid, mida kasutatakse küberturvalisuse määruses. Eesti kontekstis siiski võetakse eelnõuga kasutusele uus termin „riiklik küberturvalisuse sertifitseerimise asutus,“ mille definitsiooni saab tuletada küberturvalisuse määruse artikilist 58 (kuigi küberturvalisuse määruses endas seda ei defineerita). Riiklik küberturvalisuse sertifitseerimise asutus kujutab endast asutust, mis teeb koostööd EL tasandiga infovahetuseks ja teostab küberturvalisuse määruses sätestatud kohustuste üle järelevalvet.

Eelnõus kasutatakse ka termineid, mida kasutatakse küberturvalisuse TTT määruses. Näiteks on selles sätestatud, mis asutus on „küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus“ ning mis on selle valdkonnaga seotud „riiklik koordineerimiskeskus“.[34] Viimase mõistega seonduvalt määratakse eelnõus, et riikliku koordineerimiskeskuse ülesandeid täidab „küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksus“ ehk „TTT koordineerimisüksus“ – sellega on soov rõhutada, et tegemist pole lihtsalt riikliku koordineerimisüksusega, vaid see toimetab tööstuse, tehnoloogia ja teadusuuringute valdkonnas.

Järgnevad terminid ei ole uued terminid (nad on juba liidu või Eesti õiguses juba kasutusel või defineeritud), kuid eelnõust ja seletuskirjast parema arusaamise jaoks, on need selgitava infona lisatud seletuskirja:

- riiklik akrediteerimisasutus – ainus akrediteerimist teostav asutus liikmesriigis, kes on selleks riigi poolt volitatud[35] ehk asutus, mis akrediteerib vastavushindamisasutusi;
- vastavushindamisasutus – avalik asutus või eraettevõte, mis teostab vastavushindamist, sealhulgas kalibreerimist, katsetamist, sertifitseerimist ja kontrolli;
- akrediteerimine – riikliku akrediteerimisasutuse läbiviidav vastavushindamisasutuse atesteerimine, mis tõendab tema vastavust kindlaksmääratud vastavushindamisülesande täitmiseks harmoneeritud standardi põhjal kehtestatud nõuetele ja vajaduse korral mis tahes lisanõuetele, sealhulgas asjaomaste valdkondlike normide alusel kehtestatud nõuetele.[36]

5. Eelnõu vastavus Euroopa Liidu õigusele

E-ITS-i kehtestamise eesmärk ei ole seotud EL-i õigusega. Euroopas on standardimine korraldatud vastavalt Euroopa Parlamendi ja nõukogu määrusele (EL) nr 1025/2012. Selle määruse kohaselt on riiklik standard - standard, mille on vastu võtnud riigi

[33] Kättesaadav: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2020/400
[34] Euroopa Parlamendi ja nõukogu määruse (EL) nr 2021/887 artiklid 1, 6 ja 12.
[35] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008 artikkel 2 lõige 11. Vastavushindamisasutuse temaatikat reguleerib ka toote nõuetele vastavuse seadus.
[36] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 765/2008 artikkel 2 lõige 10.

standardiorganisatsioon (Eesti Standardimis- ja Akrediteerimiskeskus). Taoliste standardite puhul kohaldub TNVS § 40. Samas pole E-ITS standard nimetatud EL-i määruse ning TNVS-i tähenduses. E-ITS on pigem ühtsete nõuete kogum, mitte standardiorganisatsiooni poolt kinnitatud dokument. Eestis on ka täna juba standardiorganisatsiooni väliseid standardeid, mis on analoogselt kehtestatud määrusega.[37]

Küberturvalisuse TTT määruse artikli 6 lõike 1 kohaselt peab iga EL-i liikmesriik määrama 29. detsembriks 2021. a ühe sama artikli lõikes 5 sätestatud kriteeriume täitva asutuse sama määruse kohaldamisel riiklikuks koordineerimiskeskuseks.[38] Viidatud lõike 5 sisu: *„Riiklik koordineerimiskeskus on avaliku sektori asutus või liikmesriigi enamusosalusega asutus, kes täidab liikmesriigi õiguse alusel avaliku halduse ülesandeid, sealhulgas delegeerimise kaudu, ja kellel on suutlikkus toetada pädevuskeskust ja võrgustikku nende käesoleva määruse artiklis 3 sätestatud missiooni elluviimisel. Asutusel peavad olema teaduse ja tehnoloogia alased eksperditeadmised küberturvalisuse valdkonnas või juurdepääs sellistele teadmistele. Asutus peab suutma pidada tulemuslikku dialoogi ja koordineerida oma tegevust tööstuse, avaliku sektori, akadeemilise ja teaduskogukonnaga ning kodanikega, sealhulgas direktiivi (EL) 2016/1148 kohaselt määratud asutustega.“* Eelnõu ning selle lisaks oleva ministri määruse kavandiga määratakse RIA riiklikuks koordineerimiskeskuses nimetatud küberturvalisuse TTT määruse tähenduses. RIA vastab eelnevalt nimetatud lõike 5 tingimustele. Samuti on RIA KüTS §-i 5 järgi direktiivi nr 2016/1148 artikli 8 lõikes 1 nimetatud pädev asutus ja lõikes 3 nimetatud ühtne kontaktpunkt ning artikli 9 lõikes 1 nimetatud küberturbe intsidentide lahendamise üksuse ülesannete täitja. Seega on võimalik RIA vastavaks asutuseks määrata – seda ülesannet täidetakse TTT koordineerimisüksusena.

Eelnõu on vastavuses Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881 (küberturvalisuse määrus) ning selle otseseks eesmärgiks on küberturvalisuse määrusega liikmesriikidele sätestatud kohustuste täitmine. Eelnõu regulatsioon jääb küberturvalisuse määrusega liikmesriikidele antud riikliku küberturvalisuse sertifitseerimise asutuse määratlemise ja küberturvalisuse määruses sätestatud nõuete rikkumise eest karistusmäärade kehtestamise pädevuse piiridesse.

Seega on seaduseelnõu kooskõlas Euroopa Liidu õigusega.

6. Seaduse mõjud

6.1. Kavandatav muudatus: E-ITS-i kehtestamine

6.1.1. Sotsiaalne, sh demograafiline mõju

6.1.1.1. Mõju ettevõtjale

Eelnõu ei tekita ettevõtjale sotsiaalset mõju. Teenuse osutajate vajadus tööturul sobiva kvalifikatsiooniga küberturbe ekspertide järele küberturvalisuse tagamiseks jääb püsima.

[37] Vt nt haridus- ja teadusministri 28.11.2008. a määrust nr 69 „Kutsestandardite koostamise, muutmise ja vormistamise kord“, 19.06.2015. a määrust nr 27 „Täienduskoolituse standard“, 21.03.2007. a määrust nr 27 „Huviharidusstandard“ ning rahandusministri 13.12.2011. a määrust nr 57 „Siseaudiitori kutsetegevuse standardite kehtestamine“.

[38] Vt ka: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre.

Küberintsidendist teavitamise nõude täpsustamine ei tekita samuti ettevõtjale sotsiaalset mõju. Sarnane nõue on ka isikuandmete kaitse valdkonnas, mistõttu tegemist ei ole oma olemuselt uue nõudega.[39]

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.1.2. Mõju kodanikele

Eelnõu ei tekita kodanikele sotsiaalselt mõju. Eesmärk E-ITS kehtestamise kaudu tugevdada küberturvalisuse taset parandab küll elutähtsate teenuste toimepidevust, kuid eelnõu koostamise hetkel ei ole Eestis elutähtsate teenuste toimepidevus ohustatud, et eelnõu tekitaks sotsiaalsest perspektiivist kodanikule erisust kehtiva seadusega võrreldes.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.2. Mõju riigi julgeolekule ja välissuhetele

6.1.2.1. Mõju ettevõtjatele

KüTS-i mõistes teenuse osutajad pakuvad riigi toimimiseks vajalikke teenuseid. E-ITS-i kehtestamise eesmärk on täpsustatud ja selgema infoturbe haldamissüsteemi rakendamisega aidata edendada teenuse osutaja ning tema teenuste vastupanuvõimet küberintsidentidele ning sellest tulenevalt on eelnõul positiivne mõju riigi julgeolekule. Sama eesmärk ja mõju on ka küberintsidendist teavitamise nõude täiendamisel.

Eelnõu ei mõjuta otseselt ettevõtjate välissuhteid, kuivõrd teenuse osutajatel on ka edaspidi võimalik E-ITS-i rakendamise asemel rakendada küberturbe tagamisel ka rahvusvahelisi ISO standardeid. Kaudselt on eelnõul positiivne mõju välissuhete edendamisele tugevama küberturvalisuse kuvandi tõttu.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

6.1.2.2. Mõju avalikule sektorile

Eelnõul on positiivne mõju riigi julgeolekule ka avaliku sektori kaudu. Selgema avaliku sektori määratluse ning E-ITS-i kehtestamisega kehtiva ISKE asemel on avalikus sektoris ka suurem selgus, et kes ja mida tegema peab. Samuti vähendab E-ITS-i organisatsioonipõhine lähenemine küberturbe tagamisel ka avaliku sektori haavatavust küberintsidentidele ning nende mõjude levimist avalike sektori jaoks olulisemate süsteemideni. Seda aitab saavutada ka küberintsidendist teavitamise nõude täiendamine.

Välissuhete vaatepunktist aitab avaliku sektori küberturvalisuse nõuete uuendamine ka säilitada ning arendada Eesti riigi kui küberturvalisuse eestvedaja kuvandit.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

6.1.2.3. Mõju järelvalveasutusele (RIA-le)

Eelnõu aitab RIA-l läbi täpsemate küberturvalisuse tagamise nõuete tugineda küberintsidentide ennetamisel, tuvastamisel ja lahendamisel ühtsematele eeldustele teenuse osutajate ja avaliku

[39] Vt Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679, mis käsitleb füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (edaspidi *GDPR*) artikli 28 lõike 3 punkti f ning artikli 33 lõiget 2.

sektori turvameetmete suhtes. Samuti aitab eelnõu läbi reguleeritud auditeerimistingimuste tagada selgema ja kiiremini analüüsitava ülevaate küberturbe tasemest Eestis. Sellest tulenevalt on eelnõul positiivne mõju RIA riigikaitse ja julgeolekuga seotud valmisolekule küberintsidentide ennetamiseks, tõrjumiseks ja lahendamiseks.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

6.1.3. Mõju majandusele

6.1.3.1. Mõju ettevõtjatele

E-ITS kehtestamisest tulenevad muutused kujundavad formaalselt ümber teenuse osutajate kohustusi, kuid ei muuda neid sisuliselt võrreldes varasemate kohustustega küberturvalisuse tagamisel. Kehtiva KüTS-i § 7 lõike 1 alusel peavad teenuse osutajad juba praegu rakendama turvameetmeid ning lõike 2 alusel koostama süsteemide riskianalüüse. Neid kohustusi sisustab KüTS § 7 lõike 4 alusel kehtestatud määrus.

Muudatusega ei lähtuks teenuse osutajad nende tegevuste läbiviimisel enam KüTS § 7 lõike 4 alusel kehtestatud määrusest, vaid KüTS § 7 lõike 5 alusel kehtestatud määrusest. E-ITS on kindlasti mahukam dokument kui KüTS § 7 lõike 4 alusel kehtestatud määrus, kuid selle põhjuseks on nõuete põhjalikum kirjeldus, mitte nõuete oluline laiendamine. Sarnaselt praegu KüTS § 7 lõike 4 alusel kehtestatud määruses sisustatud nõuetega, põhinevad ka E-ITS-i nõuded organisatsiooni riskianalüüsile ja selle põhjal rakendatud turvameetmetele. Seega eeldusel, et teenuse osutaja on varasemalt teinud pingutusi küberturvalisuse tagamiseks KüTS § 7 lõike 4 alusel kehtestatud määruse nõuete järgimisega, ei tulene teenuse osutajale E-ITS tingimuste järgimise kohustusest suurt majanduslikku mõju.

E-ITS kehtestamisega kaasneks ettevõtjatele kohustus läbi viia E-ITS-i vastavusaudit iga kolme aasta järel. Sellega asendatakse KüTS § 7 lõike 2 punktide 5 ja 6 alusel kehtiv kohustus viia läbi ning dokumenteerida turvameetmete rakendamise piisavuse kontroll. Kehtivate nõuete kohaselt on turvameetmete rakendamise piisavuse kontrolli üks meetoditest auditi läbiviimine pädeva sõltumatu isiku poolt, kuid seda võib asendada ka nn enesehindamisega. E-ITS-i kehtestamise järgselt kaoks võimalus asendada audit enesekontrolliga ning E-ITS sätestab konkreetse raamistiku auditite läbiviimiseks eesmärgiga tagada selgem ja läbipaistvam küberturvalisuse nõuete järgimine. Teenuse osutajatele, kes varasemalt teostasid turvameetmete rakendamise piisavuse kontrolli nn enesehindamise kaudu, võib muudatus avaldada majanduslikku mõju, kuid seda maksimaalselt ulatuses, mis oleks nn enesehindamise läbiviimise ja auditi läbiviimise kulude vahe. Majanduslik mõju võib olla teenuse osutaja positsiooni soodustav, kui E-ITS-i auditeerimine kujuneb odavamaks teenuseks kui KüTS § 7 lõike 2 punkti 5 alusel auditi või enesehindamise läbiviimine.

Küberintsidendist teavitamise nõude täiendamisel puudub oluline majanduslik mõju ettevõtjatele, kuna sarnane nõue on kehtiv ka isikuandmete kaitse valdkonnas (vt seletuskirja punkti 6.1.1.1.).

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.3.2. Mõju avalikule sektorile

E-ITS kehtestamisega asendatakse AvTS-i alusel kehtestatud ISKE järgimise kohustus. Eeldusel, et avaliku sektori rakendaja on järginud ISKE nõudeid, puudub ISKE ja E-ITS nõuete

võrdluses E-ITS-i kehtestamisest tulenev majanduslik mõju avalikule sektorile nii turvameetmete rakendamisel kui ka vastavusauditite läbiviimisel. Majanduslik mõju avalikule sektorile, mis tuleneb täpsemalt raamistatud organisatsioonipõhisest lähenemisest küberturbe tagamisel (sh kaardistustegevused ja riskianalüüsid) on minimaalne ning praktikas rakendatav läbi E-ITS-i üleminekujuhendite kasutamise.

Avaliku sektori täpsema määratluse kaudu laieneb E-ITS-i järgimiseks kohustatud isikute, asutuste või muude üksuste hulk – seda ennekõike muude avalik-õiguslike juriidiliste isikute ning Riigikogus esindatud erakondade näol. Sarnaselt kehtiva seaduse alusel avalikule sektorile kehtestatud kohustustele, on ka siinjuhul majanduslik mõju avalikule sektorile kahesuunaline. Ühelt poolt tuleb avaliku sektori sellel osal, mis ei ole piisavalt võrgu- ja infosüsteemide turvalisuse tähelepanu pööranud, rakendada nõuetekohaseid meetmeid nende turvalisuse tagamiseks. Teisalt aitab võrgu- ja infosüsteemide turvalisuse tagamine vähendada küberintsidentidest kaasnevat majanduslikku kahju.

Küberintsidendist teavitamise nõude täiendamisel puudub oluline majanduslik mõju avalikule sektorile, kuna sarnane nõue on kehtiv ka isikuandmete kaitse valdkonnas (vt GDPR artikli 28 lõike 3 punkti f ning artikli 33 lõiget 2 ja isikuandmete kaitse seaduse § 44 lõiget 2).

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.3.3. Mõju kodanikele

E-ITS kehtestamise eesmärk on selgema raamistiku kaudu edendada võrgu- infosüsteemide turvalisust. Sellel on vahetu mõju majanduskeskkonna toimimisele, kuivõrd Eesti konkurentsieelis digilahenduste kasutuselevõtus ja arendamises on tugevalt seotud nende digitaalsete lahenduste ja sealse andmetöötluse toimepidevuse, tervikluse ning konfidentsiaalsuse tagamisega. Samuti mõjutab eelnõu kodanikke rohkem digitaalseid teenuseid usaldama, tagades seega ka nende toimimise jätkusuutlikkuse suureneva kasutamise kaudu.

Kodanike halduskoormust eelnõu ei mõjuta.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.4. Mõju elu- ja looduskeskkonnale

Eelnõu ei avalda otsest mõju elu- ja looduskeskkonnale. Kaudselt võib eelnõu positiivset mõju elu- ja looduskeskkonnale aga avaldada läbi vastupanuvõimekuse suurendamise küberrünnakute suhtes, mis saaksid põhjustada elukeskkonnale või looduskeskkonnale kahjulikke tagajärgi (nt veepuhastusprotsessi sekkumine ja kasutatavate kemikaalide koguste muutmine). Nende võimalike kahjulike tagajärgede tekkimise võimalust vähendab küberrünnakust ning selle põhjustatud küberintsidendist teada saamine, mistõttu on küberintsidendist teavitamise nõude täiendamisel positiivne mõju.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.5. Mõju regionaalarengule

Seaduseelnõu ei oma olulist mõju regionaalarengule.

6.1.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

6.1.6.1. Mõju avalikule sektorile

Eelnõu ei mõjuta avaliku sektori töökorraldust, kuivõrd kehtiva seaduse alusel on avalik sektor kohustatud kõikidele võrgu- ja infosüsteemide küberturbe tagamisel järgima ISKE nõudeid. E-ITS-i kehtestamine ei too kaasa muudatusi, mille rakendamine vajaks asutuse töökorralduse või selles osas töökoormuse olulist suurendamist.

Eelnõu võib kaudselt mõjutada avaliku sektori teenuste kvaliteeti, kuivõrd teenuste kaardistamise ja riskipõhine lähenemine aitab kaasa asutusel tehnoloogilisi mahajäämusi või paremaid arendussuundi tuvastada.

Mõju avaliku sektori kuludele võib eelnõu kehtestamisel esineda neil juriidilistel isikutel ja asutustel, kes varasemalt ei ole olnud ISKE kohuslased ning ühtlasi pole teinud pingutusi kasutatavate võrgu- ja infosüsteemide turvalisuse tagamiseks. Sellisel juhul suurendab E-ITS kehtestamine kulutuste tegemise vajadust pädeva personali palkamiseks, asjakohaste turvameetmete rakendamiseks ning auditite läbiviimiseks ja vähendab kulutuste tegemise vajadust küberintsidentidest tuleneva kahju või muude tagajärgede likvideerimiseks.

Sellegipoolest oleks ka siis mõjude ulatus väike, kuivõrd kohustusi avalikule sektorile tehniliste ja korralduslike turvameetmete rakendamiseks tuleneb ka mujalt. Ennekõike peab sõltumata KüTS-s sätestatud kohustustest avalik sektor rakendama isikuandmete turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid GDPR artikkel 32 lõike 1alusel ning samuti lähtuma selle kohustuse täitmisel riskide analüüsist GDPR artikkel 32 lõike 2 alusel.

Küberintsidendist teavitamise nõude täiendamisel puudub oluline mõju avalikule sektorile, kuna sarnane nõue on kehtiv ka isikuandmete kaitse valdkonnas (vt GDPR artikkel 28 lõike 3 punkti f ning artikli 33 lõiget 2 ja isikuandmete kaitse seaduse § 44 lõiget 2).

VVS-i muudatusel puudub oluline mõju Majandus- ja Kommunikatsiooniministeeriumile ning selle valitsemisalale, kuna muudatusega seonduvalt ei toimu ministeeriumile ega selle valitsemisalale uute ülesannete lisandumist ning sellega seonduv muudatus ministeeriumi põhimääruses on juba teostatud. Alates 2021. a 1. maist on ministeeriumis loodud riikliku küberturvalisuse osakond.[40]

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.6.2. Mõju järelvalveasutusele (RIA-le)

E-ITS-i kehtestamise eesmärgi raames ei mõjuta eelnõu RIA töökorraldust. Varasem KüTS § 7 lõike 4 alusel kehtestatud nõuete ja ISKE nõuete järgimise kontroll asendub E-ITS nõuete järgimise kontrolliga.

RIA töökoormust võib eelnõu suurendada suurema hulga auditite järeldusotsuste ülevaatamise vajaduse tõttu, kuid samuti ka vähendada tänu küberturbe korralduste kui ka auditite põhjalikumale standardiseeritusele.

Küberintsidendist teavitamise nõude täiendamisel ning VVS-i täiendamisel puudub oluline mõju RIA-le.

[40] Vabariigi Valitsuse 23.10.2002 määrus nr 323 „Majandus- ja Kommunikatsiooniministeeriumi põhimäärus“, vt § 11 lõiget 2 ja § 17 punkti 14^1.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.1.7. Muu otsene või kaudne mõju

Seaduseelnõu ei muud otsest või kaudset olulist mõju.

6.2. Kavandatav muudatus: küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramine ja sellega seotud ülesannete korraldus

Küberturvalisuse TTT määruse ettevalmistamisel hinnati eraldi ka vastava EL-i määruse mõjusid EL-i üleselt.[41] Järgnevalt esitatakse eelnõuga vastu võetavate sätete mõjud Eestis.

6.2.1. Sotsiaalne, sh demograafiline mõju

6.2.1.1. Mõju ettevõtjale

Eelnõu sotsiaalne mõju ettevõtjatele võib olla positiivne. Riikliku koordineerimiskeskuse määramine võimaldab ettevõtjatel läbi koordineerimiskeskuse hallatava kogukonna rääkida kaasa Euroopa Liidu tasandil küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute prioriteetide otsustamisel, osaleda korraldatavates arendusprojektides ja panustada ettevõtjate kompetentsivõrkude loomisesse.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.2.1.2. Mõju kodanikele

Eelnõul on vähesel määral positiivne sotsiaalne mõju ka kodanikele. Määratava riikliku koordineerimiskeskuse põhiülesannete hulka kuuluvad mh küberturvalisuse teemadel tehtud arengute kajastamine avalikkuses ning küberturvalisuse haridusprogrammide toetamine. Nende ülesannete edukal täitmisel võib suureneda Eestis küberturvalisusega seotud oskuste omandamine ning tööhõive.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.2.2. Mõju riigi julgeolekule ja välissuhetele

Eelnõul on pigem positiivne mõju riigi julgeolekule, kuivõrd riikliku koordineerimiskeskuse määramise eesmärk on ka kindlustada Eesti julgeolekuliste huvide esindamine EL tasandil küberturvalisuse valdkonnas uute suundade ja arenduste otsustamisel.

Eelnõul on positiivne mõju riigi välissuhetele kuivõrd eelnõu eesmärk on tagada Eesti osalus küberturvalisuse TTT määruse alusel loodavates rahvusvahelistes võrgustikes.

Ulatus keskmine, sagedus keskmine, ebasoovitavate mõjude risk väike.

6.2.3. Mõju majandusele

Eelnõuga reguleeritakse küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramist ja sellega seotud ülesannete korraldust. Nimetatud muudatused ei oma olulist mõju riigieelarvele ega Eesti majandusele. Kaudselt võib majandusele avalduda positiivne mõju koordineerimiskeskuse abil küberturvalisuse

[41] Leitavad siit: https://eur-lex.europa.eu/legal-content/ET/ALL/?qid=1610959968587&uri=CELEX%3A52018SC0403.

valdkonnas EL arendusprojektides osalemine ning rahastuse saamine, kuid sel juhul ei ole tegemist eelnõu mõjuga, vaid juba koordineerimiskesksuseks määratud asutuse tegevuste tulemuslikkusega.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.2.4. Mõju elu- ja looduskeskkonnale

Eelnõu muudatusel puuduvad olulised mõjud elu- ja looduskeskkonnale.

6.2.5. Mõju regionaalarengule

Seaduseelnõu ei oma olulist mõju regionaalarengule.

6.2.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

Eelnõu mõjutab ennekõike riiklikuks koordineerimiskeskuseks määratud asutuse töökorraldust, milleks kavandatava ministri määruse alusel on RIA.

Küberturvalisuse TTT määruse artiklis 6 lõikes 5 on sätestatud, mis nõuetele peab riiklik koordineerimiskeskus vastama ning artiklis 7 on sätestatud tema ülesanded.

Riiklikule koordineerimiskeskusele küberturvalisuse TTT määrusest tulenevate kohustuste täitmisega kaasneb RIA-le vajadus lisaks olemasolevale personalile värvata täiendavat personali (ca 6-7 inimest). Värvatava personali tõttu ei mõjuta ülesande lisandumine RIA muude ülesannete teostamist. Ülesande täitmise jaoks võidakse luua uus struktuuriüksus, mis asub küberturvalisuse teenistuse koosseisus.

Ülesande lisandumine võib tähendada vähesel määral koolitusvajadust lisanduva ülesande täitjatele, kuid koolituse vajadus ei ole suur, kuna täiendava personali värbamisel on võimalik võtta tööle valdkonnas pädevaid inimesi.

Lisaks RIA-le on eelnõul teatav mõju Majandus- ja Kommunikatsiooniministeeriumile, konkreetsemalt ministeeriumi riikliku küberturvalisuse osakonnale, kuid see mõju avaldub kavandatava KüTS § 5^1 lõike 3 alusel kehtestava määrusega (vt lisatud määruse kavandit).

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.2.7. Muu otsene või kaudne mõju

Seaduseelnõu ei muud otsest või kaudset olulist mõju.

6.3. Kavandatav muudatus: küberturvalisuse sertifitseerimise korralduse reguleerimine

Eelnõuga sisustatakse teatavad sätted, mis on võimalik küberturvalisuse määruse alusel. Küberturvalisuse määruse ettevalmistamisel hinnati eraldi ka EL-i ülese sertifitseerimise raamistiku loomise mõjusid EL-i üleselt.[42] Järgnevalt esitatakse eelnõuga vastu võetavate sätete mõjud Eestis.

6.3.1. Sotsiaalne, sh demograafiline mõju

[42] Leitavad siit: https://eur-lex.europa.eu/procedure/ET/2017_225.

Seaduseelnõu ei oma olulist sotsiaalset ega demograafilist mõju. Kui eelnõu vastu võtmise järgselt mõni ettevõtja soovib enda IKT-tooted, -teenused ja -protsessid Eestis sertifitseerida vastu võetud valdkondliku EL küberturvalisuse sertifitseerimise kava nõuete vastu, siis selle mõju on positiivne inimestele. Seeläbi saavad inimesed suurema kindluse, et IKT-toode, -teenus või protsess, mida nad enda tegemistes kasutavad (tarbijana) või mida kasutatakse ettevõtja juures, mille kliendiks ta on, vastab sertifitseerimise hetkel EL-i küberturvalisuse sertifitseerimise kava nõuetele. Kuigi siinne sertifitseerimine on eraldiseisev isikuandmete kaitse üldmääruses sätestatud sertifitseerimisest isikuandmete kaitse töötlemise valdkonnas, aitab ka siinse eelnõuga seotud sertifitseerimise teostamine isikuandmete kaitse tagamist.[43] Seetõttu on mõju inimestele positiivne, sh ei suurene tema halduskoormus.

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.3.2. Mõju riigi julgeolekule ja välissuhetele

Eelnõul on pigem positiivne mõju riigi julgeolekule ja välissuhetele, kuna sellega võimaldatakse ettevõtjatel suurendada enda IKT-toote, -teenuse või -protsessi küberturvalisust, kui see on sertifitseeritud EL-i küberturvalisuse sertifitseerimise kava nõuete vastu. Seeläbi on selle toote kasutajal (nt riigiasutusel) ka suurem kindlus, et vastava toote küberturvalisuse taset on kontrollitud. Sertifitseeritud toote kasutamine pigem suurendab toote kasutaja võrgu- ja infosüsteemide turvalisust.

Eelnõu edendab EL-i liikmesriikides olevate riiklike küberturvalisuse sertifitseerimise asutuste ning ENISA-ga koostööd. Koostöö võib suureneda ka kolmandate riikidega, kui EL-i üleselt tulevikus luuakse võimalus EL-i küberturvalisuse sertifitseerimise kava nõuetele vastava sertifikaadi tunnustamiseks ka kolmandates riikides.[44]

Ulatus väike, sagedus väike, ebasoovitavate mõjude risk väike.

6.3.3. Mõju majandusele

Eelnõuga reguleeritakse riikliku küberturvalisuse sertifitseerimise asutuse määramine, küberturvalisuse määruses sätestatud nõuete rikkumise eest karistuste määramine ning karistuste määramise pädevuse kehtestamine. Nimetatud muudatused ei oma olulist mõju riigieelarvele ega Eesti majandusele. Kuigi eelnõu puudutab otseselt IKT-valdkonna ettevõtjaid ja nende tegevust, ei ole eelnõul teadaolevalt ettevõtetele olulist mõju, kuna sertifitseerimine on hetkeseisuga vabatahtlik ning tulevikus toimuvaid muudatusi (nt mõne küberturvalisuse sertifitseerimiskava õigusaktiga Euroopa Liidus kohustuslikuks tegemine) on raske prognoosida. Eelnõu ei mõjuta uute ettevõtete pääsu EL-i ühtsele digitaalvaldkonna turule. Hetkel on ka keeruline prognoosida (sh ka suurusjärguna), millisel määral on ettevõtjatel huvi sertifitseerida enda IKT-tooted, -teenused ja -protsessid Eestis. Seega ei oma eelnõu olulist mõju majandusele. Küll aga tuleb nentida, et, sarnaselt Soome hinnangule, võib Eesti IKT-ettevõtete konkurentsivõimet mõjutada Euroopa sertifitseerimissüsteemi nõuded ja see, kas/mis ulatuses Eesti ettevõtjad nendele nõuetele vastavad. Eeldatavasti suurendab ning edendab EL-i küberturvalisuse sertifitseerimise kava nõuete suhtes sertifitseerimine ka innovatsiooni, sh võivad sertifitseeritud IKT-tooted, -teenused või -protsessid edendada ettevõtjate eksporditegevusi.

[43] Euroopa Parlamendi ja nõukogu (EL) määrus nr 2016/679; vt ka küberturvalisuse määruse pp 15 ja 74.
[44] Vt küberturvalisuse määruse pp 105.

Kui erasektoris olev vastavushindamisasutus läbib riikliku akrediteerimisasutuse juures akrediteerimise, siis kaasnevad sellega täiendavad kulud (taotluse läbivaatamise tasu, akrediteerimise tasu, ning aastatasu akrediteeringu ja tunnistuse kehtivana hoidmise eest). Siin vt TNVS §-e 38^1-38^4, sama seaduse § 38^4 lõike 4 alusel antud määrust ning kinnitatud hinnakirja[45]. Nende kohaselt on võimalikud kulutused (kui akrediteeringut soovitakse MTÜ-lt Eesti Standardimis- ja Akrediteerimiskeskus):

- esmase akrediteerimise taotluse läbivaatamise tasu 300 eurot;
- akrediteerimisulatuse laiendamise taotluse läbivaatamise eest 200 eurot;
- akrediteerimise tasu: tasu suurus sõltub hindamisele kulunud ajast, hindamise keerukusest ja hindajate (edaspidi *assessor*) tasu suurusest ning hindamisega kaasnenud otsestest kuludest, konkreetsemalt:
    - assessori töötasu suurus sõltub temaga saavutatud tasu kokkuleppest; Eesti akrediteerimisasutus tutvustab akrediteerimist taotlevale või akrediteeritud asutusele eelnevalt akrediteerimise eeldatavat maksumust ja võimaldab esitada seisukoha kaasatava assessori tasu kohta;
    - hindamise eest vastutava hindaja (edaspidi *peaassessor*) tunnitasu suurus on kuni 20-kordne töölepingu seaduse § 29 lõike 5 kohaselt kehtestatud tunnitasu alammäär; Eesti akrediteerimisasutus kehtestab igal aastal peaassessori tunnitasu konkreetse määra; aastatel 2021-2022 on peaassessori tunnitasu suurus 50 eurot;
    - akrediteerimise otsesed kulud on assessori lähetuskulud, tõlkekulud (kui hindamine ei toimu eesti keeles) ja muud akrediteerimisega seonduvad kulud;
- krediteeritud asutus maksab akrediteeringu kehtivana hoidmise eest aastatasu. Aastatasu suurus sõltub Eesti akrediteerimisasutuse jätkusuutlikuks toimimiseks vajalikest kuludest, mis jaotatakse akrediteeritud asutuste ja erialaselt pädevate mõõtjate vahel proportsionaalselt akrediteeringu ulatust ja keerukust arvestades. Tasude suurused on määratletud hinnakategooriate järgi (1-10). Alates 1. jaanuarist 2021. a kehtiva hinnakirja[46] kohaselt on aastatasu suurus järgnev (esimene arv on aastate 2021 ja 2022 kohta, teine arv on alates aastast 2023; summad on eurodes):
    - Hinnakategooria 1 – 1050 – 1260;
    - Hinnakategooria 2 – 1330 – 1595;
    - Hinnakategooria 3 – 1680 – 2015;
    - Hinnakategooria 4 – 2030 – 2435
    - Hinnakategooria 5 – 2450 – 2940;
    - Hinnakategooria 6 – 2870 – 3445;
    - Hinnakategooria 7 – 3360 – 4030;
    - Hinnakategooria 8 – 3920 – 4705;
    - Hinnakategooria 9 – 4620 – 5545;
    - Hinnakategooria 10 – 5320 – 6385.

Kui akrediteeringut soovitakse läbida mõne muu EL-i liikmesriigis olevas riiklikus akrediteerimisasutuses, võivad akrediteerimise protsessiga ja akrediteeringu hoidmisega seotud kulututuste suurused erineda. Siin tuleb täpsemalt tutvuda vastava riikliku

[45] Alates 1. jaanuarist 2021.a. kehtib MTÜ Eesti Standardimis- ja Akrediteerimiskeskuse struktuuriüksuse Eesti Akrediteerimiskeskus (EAK) teenuste hinnakiri – leitav: http://www.eak.ee/?pageId=59.
[46] Hinnakirja osas vt eelmist altviidet.

akrediteerimisasutuse hinnakirjadega. Akrediteeringu saamiseks tekivad vastavushindamisasutusel teatav halduskoormus, et akrediteeringut saada – ennekõike peab vastavushindamisasutus viima enda tegevuse küberturvalisuse määruses olevate vastavushindamisasutuse nõuetele vastavaks ning läbima riiklikus akrediteerimisasutuse läbi viidava akrediteeringu.

Lisaks eeltoodule on vastavushindamisasutusel ka teatavad kulud ja halduskoormus seoses kasutusloa saamisega. Nimetatud tegevus omab keskmist mõju. Vt siin ka lisanduva KüTS § 13^2 lõike 1 selgitusi.

EL küberturvalisuse sertifitseerimise raamistiku üheks eesmärgiks on aidata vältida üksteisele vastukäivate või kattuvate riiklike küberturvalisuse sertifitseerimise kavade paljusust. Seeläbi peaks vähendatama digitaalsel ühtsel turul tegutsevate ettevõtjate kulusid ja halduskoormust. Küberturvalisuse määruse ettepanekus[47] on toodud näitena kaugloendurid (*smart meter*). Kui kaugloenduri tootjad sooviksid mitmes liikmesriigis enda tooteid müüa, siis nad peavad arvestama ning lähtuma mitme riigi sertifitseerimise kavast (nõuetest). Igas liikmesriigis võivad sertifitseerimise summad olla erinevad; samuti tõstab see tootjate halduskoormust, kuna tekib vajadus läbida igas liikmesriigis sertifitseerimine (kui ei toimu teise liikmesriigi sertifikaadi tunnustamist). Eeltoodu näitab, et mitmes liikmesriigis sama toote sertifitseerimine viib EL-i üleste nõuete ja turu killustumiseni, kuna selle kõige tulemusena võib tekkida igas EL-i liikmesriigis eri nõuded samadele toodetele. Selle olukorra vältimiseks sätestatakse küberturvalisuse määruses võimalus koostada Euroopa küberturvalisuse sertifitseerimise kavu, mille järgi väljastatud sertifikaadid kehtivad EL-i üleselt. Selle tulemusena vähenevad digitaalsel ühtsel turul tegutsevate ettevõtete kulud ja halduskoormus.

Seletuskirja koostamise seisuga on ENISA valmistanud ette pilveandmetöötlusteenustega seotud küberturvalisuse sertifitseerimise kava ning ettevalmistamisel on eraldi küberturvalisuse sertifitseerimise kava ka 5G mobiilsidevõrgu standardi funktsiooniga võrkudega jaoks.[48] Nimetatud teemadel tulevad esimesed Euroopa küberturvalisuse sertifitseerimise kavad.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

6.3.4. Mõju elu- ja looduskeskkonnale

Seaduseelnõu ei oma olulist mõju elu- ja looduskeskkonnale.

6.3.5. Mõju regionaalarengule

Seaduseelnõu ei oma olulist mõju regionaalarengule.

6.3.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

Seaduseelnõu ei oma olulist mõju kohaliku omavalitsuse korraldusele ning muudele asutustele, mis pole allpool nimetatud. Eelnõu võib suurendada muudatustega enim eelnõuga seotud asutuste suhtlust, koostööd ja valdkondliku järelevalve teostamist.

[47] Leitav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52017PC0477, PDF- versioonis vt lk 92.

[48] Leitavad vastavalt: https://www.enisa.europa.eu/topics/standards/Public-Consultations/public-consultations-cybersecurity-schemes/ ning https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification.

TTJA hakkab teostama küberturvalisuse määruse artikli 58 lõikes 7 sätestatud ülesandeid, millest osa on seotud riikliku akrediteerimisasutusega (Eestis MTÜ Eesti Standardimis- ja Akrediteerimiskeskus) või vastavushindamisasutusega (eelnõu kohaselt RIA, kes eeldatavasti läbib vastava akrediteerimise). Samuti teostab TTJA juba praegu TNVS-i alusel tegevuslubade väljastamisega. TTJA-le on juba eraldatud vastav kompetents, kes küberturvalisuse valdkonnaga tegeleb, kuid tulevikus võib tekkida vajadus suurendada vastava kompetentsi suurust. Eelnõuga lisandub KüTS-i ka uued väärteokoosseisud, millede puhul TTJA-le olulist mõju ei avaldu, kuna ka praegu on TTJA kohtuväline menetleja.

RIA kui vastavushindamisasutus viib akrediteeringu läbimiseks oma tegevuse kooskõlla küberturvalisuse määruse artikliga 60 ning sama määruse lisas olevate nõuetega. Seetõttu tuleb akrediteerimisega seotud protsessis üle vaadata olemasolevad töökorraldused.

Küberturvalisuse määruse rakendamine mõjutab ka MTÜ Eesti Standardimis- ja Akrediteerimiskeskuse tegevust, kuigi see pole otseselt seotud käesoleva eelnõu kaalutluskohtadega, kuna MTÜ roll riikliku akrediteerimisasutusena tuleneb otse küberturvalisuse määrusest. Küberturvalisuse määrus ei ütle, et keelatud oleks akrediteerimiseks suunamine muu liikmesriigi akrediteerimisasutuse poole, kui Eesti riiklikul akrediteerimiskeskus parasjagu kompetentsi ei oma. Ehk MTÜ-l on ka võimalik akrediteerimistaotluse saamisel suunata vastavushindamisasutuse kandidaat teise liikmesriigi riikliku akrediteerimisasutuse poole. Küberturvalisuse sertifitseerimise vastavushindamise asutuste akrediteerimisvõimekuse loomine nõuab olulist ressurssi ning seda ei pruugi olla mõistlik rakendada olukorras, kus on keeruline öelda, kas siseriiklikult üldse vastavushindamisasutuseks saamise osas nõudlust on. Tavaliselt küsitakse akrediteerimise eest tasu, kuid 1-2 vastavushindamisasutusega ei pruugi olla võimalik akrediteerimise süsteemi vaid küsitavatest tasudest ülal hoida. Kuniks selle teenuse vastu on nõudlus tekkinud, on võimalik akrediteeringu taotleja suunata teise liikmesriigi riikliku akrediteerimisasutuse poole. Lisaks on ka võimalus, et küberturvalisuse valdkonnas sertifitseerimise valdkonnas võib lisaks eelmainitud MTÜ-le kasutada ka muu liikmesriigi riikliku akrediteerimisasutuse teenuseid.

Lisandunud ülesanded võivad tähendada eelmainitud asutuste teenistujate koolitamist akrediteerimise ja sertifitseerimise teemadel. Eeldatavasti hakkavad vastavaid koolitusi ja töötube pakkuma EL-is olevad valdkondlikud asutused ning eeldatavasti saavad oma kogemusi jagada ka Eestis olevad asutused, kes tegelevad muudes valdkondades eelnõu teemadega.

Ulatus keskmine, sagedus väike, ebasoovitavate mõjude risk väike.

6.3.7. Muu otsene või kaudne mõju

Seaduseelnõu ei muud otsest või kaudset olulist mõju.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

7.1. Kavandatav muudatus: E-ITS-i kehtestamine

7.1.1. Küberturvalisuse tagamiseks vajalike kulutuste ja E-ITS kehtestamisest tulenevate kulutuste eristamine

Kuigi eelnõu eesmärk on kehtestada uued infoturbe halduse nõuded, siis selle kehtestamisest tuleneva majandusliku mõju analüüsil tuleb eristada E-ITS spetsiifikast tulenevaid kulutusi

küberturbe tagamiseks tehtavatest kulutustest üleüldiselt. Teenuse osutajad ning enamik isikutest, kellele kohaldatakse teenuse osutajale sätestatud nõudeid, on pidanud küberturvalisuse tagamiseks tegema vastavaid investeeringuid juba kehtiva õiguse (KüTS § 7) alusel.

Mis eristab E-ITS-i varasemalt kehtinud nõuetest, on ennekõike terviklik ja struktureeritud lähenemine küberturbe tagamisele organisatsioonis ning see, et nende nõuete täitmist on lihtsam kontrollida. E-ITS aga ei kujuta endast kannapööret küberturbe rakendamise põhimõtetes ega parimas praktikas.

On tõenäoline, et E-ITS-i rakendaja hakkab tegema varasemast rohkem investeeringuid küberturvalisusesse, et jõuda vastavusse kehtestatavatele nõuetele ning sealhulgas viia läbi edukas audit. See aga ei tähenda, et majanduslik mõju E-ITS-i rakendajale tulenes E-ITS-i kehtestamisest – pigem viitab selline olukord, et E-ITS rakendaja ei ole varem KüTS-i alusel kehtestatud nõudeid piisavalt põhjalikult järginud.

Seega isegi kui teenuse osutajad ning need, kellele kohaldatakse teenuse osutajale sätestatud nõudeid, peavad tegema olulisi investeeringuid E-ITS nõuetele vastamiseks, siis väitmaks, et eelnõu majanduslik mõju on rakendajale suure ulatusega, ei pea rakendaja põhistama, kuidas konkreetsed kulutused on vajalikud E-ITS nõuete täitmiseks, vaid just põhistama, kuidas konkreetsed kulutused ei olnud vajalikud kehtiva seaduse nõuete täitmiseks. Küberturvalisuse tagamiseks on vaja teha olulisi pingutusi ja investeeringuid esitatud eelnõust sõltumata.

7.1.2. Küberturvalisuse tagamiseks tehtavate kulutuste majanduslik mõju

Küberturvalisusega seotud kulutused võib jaotada kaheks liigiks – kulutused, mida tehakse küberturvalisuse tagamiseks organisatsioonis (pädeva personali palkamine, teenuste ja süsteemide kaardistamine, riskianalüüs, meetmete rakendamine) ning kulutused, mida tehakse küberintsidendi tagajärgede likvideerimiseks (lunavara nõuded, andmebaaside taastamine, riistvara välja vahetamine, info- ja võrgusüsteemide uuesti arendamine, teenuse osutamata jätmisega tekkinud kahju kandmine (sh esitatud kahjunõuded ja leppetrahvid) jne).

Alati on võimalik, et küberturvalisuse tagamisele olulisi kulutusi teinud organisatsioon ei suuda vältida kahjulikke küberintsidente ega nendega kaasnevaid kulutusi ning et küberturvalisuse tagamisele kulutusi mitte teinud organisatsioon ei lange küberintsidendi ohvriks ega kanna ka sellest tulenevaid kulutusi, kuid üldreeglina tähendab küberturvalisuse tagamiseks tehtavate kulutuste suurendamine küberintsidendi juhtumise tõenäosuse vähenemist.

Kui eelnõu tulemusel on seetõttu oodatav E-ITS rakendajatel ühel või teisel põhjusel (nt varasemalt nõuete ebapiisav täitmine või küberturvalisusega seotud kohustuste puudumine) küberturvalisusele tehtavate kulutuste suurenemist, ei saa seda vaadelda vaid kulutuste kandmise vaatenurgast, vaid tuleb arvestada ka teist liiki kulutuste vältimist. Küberintsidendid on ebaregulaarsed sündmused, mille põhjustajaks on enamasti pahatahtlikud kolmandad isikud, seega ei ole ka otseselt ennustatav suhe, kui palju konkreetne teenuse osutaja küberturvalisuse meetmete rakendamisest majanduslikult võidab või kaotab.

7.1.3. Riigi ja kohaliku omavalitsuse tegevused, eeldatavad tulud ja kulud

Eelnõu rakendamisel kaasneb nii riigi kui ka kohaliku omavalitsuse tasandil ajakulu senise ISKE dokumentatsiooni vastavusse viimisel E-ITSiga. E-ITS-i juurutamise etapis tuleb

arvestada, et infoturbe rolli täitvatel inimestel kulub põhitöö kõrvalt täiendavalt aega E-ITSi nõuetega vastavusse viimiseks (aktiivses juurutamise etapis mõned tunnid nädalas).

Eelnõust tulenevalt täiendavate kulutuste tegemise vajadust ei teki, kuivõrd üleminek ISKE-lt E-ITS-i rakendamisele asendab vastavad auditeerimiskulud ning nõuab peamiselt ajalist panust dokumentatsiooni koostamisele.[49]

Küberturvalisuse tagamiseks tehtavate kulutustega tuleb arvestada ka kehtiva seaduse alusel ning kui seni ei ole avalik sektor sellele piisavalt tähelepanu pööranud, siis tuleb avaliku sektori asutusel või muul üksusel selle eest seista oma majandusaasta eelarvestamisel, sh võimaluse korral riigieelarve läbirääkimistel. Asjaolu, et käesolev eelnõu ei too otseselt kaasa kulutuste kasvu kehtiva seadusega võrreldes, ei tähenda, et oleks juriidilisel isikul või asutusel oleks õigustatud küberturvalisuse tagamiseks vajalike kulutuste jätkuv alahindamine.

7.1.4. Küberintsidendist teavitamise nõude täiendamise ja VVS-i täiendamisega seotud tegevused, eeldatavad tulud ja kulud

Küberintsidendist teavitamise nõude täiendamise tõttu peab teenuse osutaja (nii avalikus kui erasektoris – vt kavandatava KüTS § 3 lõigete 1 ja 4 sõnastusi) kommunikeerima isikutele, kellele on usaldatud võrgu- ja infosüsteemi haldamine või majutamine, et nad peavad teenuse osutajat teatavatest küberintsidentidest teavitama. Selleks võidakse uuendada varasemaid kokkuleppeid või lepinguid. Sellega seotud kulutused ei ole märkimisväärsed, kuna GDPR artikli 28 lõike 3 punkti f ning artikli 33 lõike 2 ja isikuandmete kaitse seaduse § 44 lõikes 2 on sarnased nõuded, mis on kehtinud aastaid.

VVS-i muudatusel puuduvad täiendavad tegevused ning kulud Majandus- ja Kommunikatsiooniministeeriumile ning selle valitsemisalale, kuna muudatusega seonduvalt ei toimu ministeeriumile ega selle valitsemisalale uute ülesannete lisandumist ning sellega seonduv muudatus ministeeriumi põhimääruses on juba teostatud. Alates 2021. a 1. maist on ministeeriumis loodud riikliku küberturvalisuse osakond.[50]

7.2. Kavandatav muudatus: küberturvalisuse valdkonnas tööstuse, tehnoloogia ja teadusuuringute riikliku koordineerimiskeskuse määramine ja sellega seotud ülesannete korraldus

Eelnõu mõjutab ennekõike riiklikuks koordineerimiskeskuseks määratud asutuse töökorraldust, milleks kavandatava ministri määruse alusel on RIA.

Riiklik koordineerimiskeskus võib igal ajal taotleda selle tunnustamist, et tal on vajalik suutlikkus hallata vahendeid, et viia ellu käesolevas määruses sätestatud missiooni ja eesmärke kooskõlas määrustega (EL) 2021/695 ja (EL) 2021/694. Kolme kuu jooksul kõnealuse taotluse esitamisest hindab komisjon, kas riiklikul koordineerimiskeskusel on vajalik suutlikkus olemas ja teeb otsuse. Nimetatud otsuse all on mõeldud Euroopa Komisjoni antavat positiivset arvamust, millega tunnustatakse asjaomase riikliku koordineerimiskeskuse vajalikku suutlikkust käesoleva lõike kohaldamisel.[51]

[49] Siin on abiks vastavad abimaterjalid, mis on leitavad E-ITS-i portaalist: https://eits.ria.ee/.
[50] Vabariigi Valitsuse 23.10.2002 määrus nr 323 „Majandus- ja Kommunikatsiooniministeeriumi põhimäärus“, vt § 11 lõiget 2 ja § 17 punkti 14[1].
[51] Küberturvalisuse TTT määrus, artikkel 6 lõige 6.

Küberturvalisuse TTT määruse artikli 7 lõikes 1 on sätestatud RIA ülesanded. Sama artikli lõikes 3 on märgitud, et määruse artikli 6 lõikes 6 osutatud otsuse alusel võivad riiklikud koordineerimiskeskused saada artiklis 7 sätestatud ülesannete täitmiseks EL-ilt toetust kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046 (finantsmäärus)[52] artikli 195 esimese lõigu punktiga d.[53] Olemasoleva teabe põhjal plaanib Euroopa Komisjon aastate 2021-2023 peale riiklikele koordinatsioonikeskustele toetuseks eraldada 50 miljonit eurot, mis jaguneb 27 liikmesriigi peale võrdselt (ehk ca 2 miljonit eurot). Komisjon on soovitanud liikmesriikidel sama summa lisada.

Finantsiline panus on oluline ka seetõttu, et lisaks riiklikele koordineerimiskeskustele loodi küberturvalisuse TTT määrusega ka küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus (edaspidi *pädevuskeskus*), mille ühismeetmeid rahastavad EL ja liikmesriigid vabatahtlike osalustega.[54] Pädevuskeskuses osalemisel on vajalik ka panustada, kuna see on seotud pädevuskeskuses olevate ühismeetmetega.[55]

Liikmesriigid osalevad vabatahtlikult ühismeetmetes oma vabatahtliku rahalise ja/või mitterahalise osalusega. Kui liikmesriik ühismeetmes osaleb, katab selle liikmesriigi rahaline osalus halduskulud proportsionaalselt tema osalusega kõnealuses ühismeetmes. Osalus ühismeetmete halduskulude katmises on rahaline. Osalus ühismeetmete tegevuskulude katmises võib kooskõlas programmidega „Euroopa horisont“ ja „Digitaalne Euroopa“ olla rahaline või mitterahaline. Liikmesriigi osalus võib olla toetuse vormis, mida see liikmesriik annab ühismeetme raames kõnealuses liikmesriigis asuvatele toetusesaajatele. Liikmesriikide mitterahaline osalus koosneb riiklike koordineerimiskeskuste ja muude avaliku sektori asutuste rahastamiskõlblikest kuludest küberturvalisuse TTT määruse alusel rahastatud projektides osalemisel, millest arvatakse maha liidu toetus nende kulude katmiseks. Programmist „Euroopa horisont“ rahastatavate projektide puhul arvutatakse rahastamiskõlblikud kulud vastavalt määruse (EL) 2021/695 artiklile 36. Programmist „Digitaalne Euroopa“ rahastatavate projektide puhul arvutatakse rahastamiskõlblikud kulud vastavalt finantsmäärusele. Programmi „Euroopa horisont“ kohasteks ühismeetmeteks kavandatud liikmesriikide vabatahtliku koguosaluse summa, sealhulgas rahaline osalus halduskuludeks, määratakse kindlaks, et võtta seda arvesse programmi „Euroopa horisont“ strateegilise planeerimise protsessis, mis viiakse pädevuskeskuse nõukogu kaasabil läbi määruse (EL) 2021/695 artikli 6 lõike 6 alusel. Olenemata määruse (EL) 2021/694 artiklist 15, võivad liikmesriigid programmi „Digitaalne Euroopa“ kohaste meetmete puhul osaleda nimetatud programmist kaasrahastatavate

[52] Euroopa Parlamendi ja nõukogu 18. juuli 2018. aasta määrus (EL, Euratom) 2018/1046, mis käsitleb liidu üldeelarve suhtes kohaldatavaid finantsreegleid ja millega muudetakse määrusi (EL) nr 1296/2013, (EL) nr 1301/2013, (EL) nr 1303/2013, (EL) nr 1304/2013, (EL) nr 1309/2013, (EL) nr 1316/2013, (EL) nr 223/2014 ja (EL) nr 283/2014 ja otsust nr 541/2014/EL ning tunnistatakse kehtetuks määrus (EL, Euratom) nr 966/2012 (ELT L 193, 30.7.2018, lk 1).

[53] Euroopa Parlamendi ja nõukogu määruse (EL, Euratom) 2018/1046 artikkel 195 esimese lõigu punkt d: Toetusi võib anda ilma konkursikutseta ainult järgmistel juhtudel: d) asutustele, kes on artiklis 58 osutatud alusaktis kindlaks määratud toetusesaajatena, või asutustele, kelle on oma vastutusel määranud liikmesriigid, kui kõnealused liikmesriigid on alusaktiga kindlaks määratud toetusesaajatena.

[54] Küberturvalisuse TTT määrus, artikkel 21 lõige 1.

[55] Küberturvalisuse TTT määrus, artikkel 2, punkt 5: ühismeede – iga-aastases tööprogrammis sisalduv meede, mis saab rahalist toetust programmidest „Euroopa horisont“ ja „Digitaalne Euroopa“ või muudest EL-i programmidest, samuti rahalist või mitterahalist toetust ühelt või mitmelt liikmesriigilt, ning mida rakendatakse projektide kaudu, mis hõlmavad nimetatud liikmesriikides asuvaid ja neilt rahalist või mitterahalist toetust saavaid toetusesaajaid.

pädevuskeskuse kulude katmises summa ulatuses, mis on väiksem kui küberturvalisuse TTT määruse artikli 21 lõike 3 punktis a sätestatud summad.[56]

Kui mõni liikmesriik ei täida seoses ühismeetmetega oma rahalise või mitterahalise osalusega seotud kohustusi, siis võivad sellel olla ka teatavad tagajärjed ehk liikmesriigi hääleõigus pädevuskeskuse nõukogus võidakse tühistada või rakendatakse muid meetmeid, kuni kõnealune liikmesriik on oma kohustused täitnud; samuti on võimalik, et Euroopa Komisjon lõpetab ühismeetmetele EL-i rahalise toetuse andmise, seda proportsionaalselt vähendada või selle andmise peatada.[57]

Osalevad liikmesriigid teatavad pädevuskeskuse nõukogule iga aasta 31. jaanuariks küberturvalisuse TTT määruse lõikes 7 osutatud osaluse suuruse, mis on eelneval eelarveaastal EL-iga läbi viidava ühismeetme puhul makstud.[58]

RIA-le lisanduvate ülesannete tõttu kaasneb RIA-le vajadus lisaks olemasolevale personalile värvata täiendavat personali (ca 6-7 inimest). Värvatavate inimeste palgafond ja lisanduva ülesandega seotud administratiivsed kulud on osalised võimalik katta eelnevalt mainitud EL-i antavate finantsidega, kuid lisaks sellele peavad lisanduma ka täiendavad ressurssid (sh ühismeetmete läbi viimisel). Seetõttu omab eelnõu mõju Majandus- ja Kommunikatsiooniministeeriumi valitsemisala eelarvele. Vastavad ressursid planeeritakse riigieelarve protsessis.

7.3. Kavandatav muudatus: küberturvalisuse sertifitseerimise korralduse reguleerimine

Seaduseelnõu ei oma tegevusi kohaliku omavalitsuse tegevusele ning muudele asutustele, mis pole allpool nimetatud. Sama on ka eeldatavate kulude ja tuludega.

Mõjud TTJA-le

Liikmesriigid peavad tagama, et riiklikel küberturvalisuse sertifitseerimise asutustel on piisavad ressursid oma volituste rakendamiseks ning oma ülesannete tulemuslikuks ja tõhusaks täitmiseks.[59]

Seaduseelnõu võib tulevikus omada mõju Majandus- ja Kommunikatsiooniministeeriumi valitsemisala eelarvele. Eelnõuga sätestatakse TTJA riikliku küberturvalisuse sertifitseerimise asutusena. Et TTJA saaks nõuetekohaselt oma ülesandeid täita, on vaja luua asutuses vastav küberturvalisuse sertifitseerimise kompetents. TTJA-le on juba eraldatud ühe ametikohaga seotud ressursid, mistõttu selles osas ei teki täiendavaid kulusid. Tuleviku perspektiive arvestades võib tulevikus tekkida vajadus suurendada TTJA küberturvalisuse sertifitseerimise ülesandega seotud personali arvu. Sel juhul planeeritakse vastavad ressursid riigieelarve protsessis. Võimalike infosüsteemide või muude IT kulude osas võib lisanduda täiendavad kulud, kuid hetkel ei ole võimalik neid prognoosida. Nimetatud kulutusi ja nende katmise allikaid analüüsitakse siis, kui on selge, kas ning millist laadi uus IKT-lahendus on vaja luua või tekib vajadus uuendada olemasolevaid lahendusi.

[56] Küberturvalisuse TTT määrus, artikkel 21 lõige 7.
[57] Küberturvalisuse TTT määrus, artikkel 21 lõiked 10 ja 11.
[58] Küberturvalisuse TTT määrus, artikkel 21 lõige 12.
[59] Küberturvalisuse määruse art 58 lõige 5.

Mõjud RIA-le

Eelnõu ja seletuskirja kohaselt ei ole võimalik seaduse tasandil konkreetselt määratleda RIA-t kui küberturvalisuse määruse kohase vastavushindamisasutusena. Seda seetõttu, et vastavushindamisasutuseks saamine eeldab akrediteerimist. Eelnõu ja seletuskirja koostamisel on lähtutud eeldusest, et RIA läbib vastava akrediteerimise ja saab vastavushindamisasutuseks.

Akrediteerimisprotsessi läbimise ja akrediteeringu hoidmise kulutused on kirjeldatud seletuskirja punktis 6.3.3. (erasektoris oleva vastavushindamisasutuse kulud), mis on üle kantavad ka RIA-le. Samuti on vaja saada TTJA-lt tegevusluba (vt sama seletuskirja punkti).

Hetkel on keeruline prognoosida, millisel määral võib tekkida vajadus välja anda kõrgetasemelisi sertifikaate või kui suures mahus võidakse sertifitseerimise kavas ette näha, et sertifikaati võib väljastada üksnes avalik asutus. Samuti ei ole ka hetkel ette teada, kas mõni ettevõtja soovib sertifikaati saada ehk eelduslikult ei pruugi olla selleks nõudlust.

Kuna sertifitseerimise kompetentsi loomine eeldab vastavate tehniliste teadmiste ja kogemustega töötajate olemasolu ning muud ressurssi vastavushindamistoimingute nõuetekohaseks teostamiseks, võib RIA vajada akrediteeringu läbimise korral täiendavat ressurssi, mis nähakse ette riigieelarve protsessis kindlaksmääratud vahenditest. Akrediteeringu läbimiseks peavad RIA teenistujatel olema heal tasemel tehniline ja kutsealane väljaõpe (mis hõlmab kõiki vastavushindamistegevusi), piisavad teadmised nende poolt tehtavate vastavushindamistoimingute nõuetest, piisav pädevus nimetatud hindamistoimingute läbiviimiseks, sobilikud teadmised ja arusaam kehtivatest nõuetest ning katsestandarditest ja oskus koostada sertifikaate, protokolle ning aruandeid (mis tõendavad vastavushindamistoimingute läbiviimist).[60] Kompetentsi loomine eeldab seega rahastust, mille abil kompetents luua. Vastavushindamisasutus saab sertifitseerimise eest ettevõtjatelt tasu küsida, kuid see eeldab, et kompetents on juba loodud ning akrediteering olemas ning õiguslik regulatsioon võimaldab tasu võtta.

Vajaliku riigieelarvelise rahastuse saamiseks, et kompetents luua, võib olla mõistlik lisada sertifitseerimisvõimekuse olemasolu tagamine ülesandena näiteks RIA põhimäärusesse. Üks võimalus nende kulude täiendavaks katmiseks on ka sertifitseerimise eest tasu võtmine. Vastavad võimalikud ressursid planeeritakse riigieelarve protsessis. RIA kulud vastavushindamisasutusena ei ole aga otseselt seotud käesoleva eelnõuga, vaid tulenevad otse küberturvalisuse määrusest (vt ka seletuskirja p 6.3. ning seal olevat altviidet EL-i ülese sertifitseerimise raamistiku loomise mõjudest EL-i üleselt, sh sellega seotud kulude teemal).

Mõjud MTÜ-le Eesti Standardimis- ja Akrediteerimiskeskus

MTÜ varasemalt antud tagasisides on märgitud, et EAK-l puudub paraku igasugune kompetents ja võimekus küberturvalisuse valdkonnas vastavushindamisasutusi akrediteerida, mistõttu potentsiaalsetel akrediteerimisest huvitatutel peab olema võimalus pöörduda mõne muu riigi akrediteerimisasutuse poole, kes küberturvalisuse valdkonnas akrediteerimisteenust pakub. Riiklik akrediteerimisasutus otsustab ise, milliseid tehnilisi valdkondi ta akrediteerib ja milliseid mitte ning see sõltub erinevatest asjaoludest. MTÜ tagasiside kohaselt pole MTÜ võimeline oma tegevust küberturvalisuse valdkonda laiendama. Eelnõus ei ole eraldi sätestatud, mis asutust on võimalik aktsepteerida riikliku akrediteerimisasutusena, kuna vastav nõue

[60] Küberturvalisuse määruse lisa 1.

tuleneb otse küberturvalisuse määrusest ehk riikliku akrediteerimisasutuse ülesannet võib täita MTÜ ise või suunata akrediteeringu taotleja muu riigi vastav asutuse poole (kes vastab Euroopa Parlamendi ja nõukogu määruse (EL) nr 765/2008 II peatüki nõuetele). Kui tekib soov suurendada MTÜ võimekust ka küberturvalisuse valdkonnas, siis tuleb pädevuse tõstmise jaoks planeerida vastavaid ressursse, mis tuleks ette näha riigieelarve protsessis kindlaksmääratud vahenditest.

Eeldatavad tulud

Võimalik eeldatav tulu riigieelarvele võib ilmneda lisanduva väärteokoosseisu tõttu. Siiski, kuna hetkel on keeruline prognoosida, millisel määral on ettevõtjatel huvi sertifitseerida enda IKT tooted, teenused ja protsessid Eestis, siis ei ole ka võimalik prognoosida, kas ning kuivõrd määratakse rikkumiste korral väärteokaristusi.

8. Rakendusaktid

Eelnõuga tekivad KüTS-i järgmised volitusnormid ning nende alusel kehtestatavad Vabariigi Valitsuse ning ministrite määrused:

- KüTS § 7 lg 5:Vabariigi Valitsuse määrus „Võrgu- ja infosüsteemide küberturvalisuse nõuded“;
- KüTS § 7 lg 5 ning sama lõike alusel antud Vabariigi Valitsuse määruse § § 4 lõige 3: ettevõtlus- ja infotehnoloogiaministri määrus „Eesti Infoturbestandardi kehtestamine“;
- KüTS § 5^1 lõige 3: ettevõtlus- ja infotehnoloogiaministri määrus „Eesti küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute koordineerimisüksuse määramine ja ülesannete täitmise kord“;
- KüTS § 7 lg 5 ning sama lõike alusel antud Vabariigi Valitsuse määruse § § 13 lõige 1: kaitseministri määrus „Rahvusvaheliseks sõjaliseks koostööks vajalike süsteemide loetelu ja nende turvanõuded“.

E-ITS-iga seotud muudatuste tegemiseks tehakse muudatusi järgmistes Vabariigi Valitsuse ning ministrite määrustes:

- Vabariigi Valitsuse 22. detsembri 2011. a määrus nr 181 „Arhiivieeskiri“, RT I, 19.06.2020, 27;
- Vabariigi Valitsuse 3. oktoobri 2013. a määrus nr 145 „Eesti teabevärava eesti.ee haldamise, teabe kättesaadavaks tegemise, arendamise ning kasutamise nõuded ja kord“, RT I, 25.03.2021, 5;
- Vabariigi Valitsuse 15. märtsi 2012. a määrus nr 26 „Infoturbe juhtimise süsteem“, RT I, 19.03.2012, 4;
- Vabariigi Valitsuse 28. veebruari 2008. a määrus nr 58 „Riigi infosüsteemi haldussüsteem“, RT I, 06.08.2019, 18;
- Vabariigi Valitsuse 31. juuli 2014. a määrus nr 121 „Struktuuritoetuse registri pidamise põhimäärus“, RT I, 28.08.2018, 9;
- Vabariigi Valitsuse 14. veebruari 2013. a määruse nr 27 „Testide andmekogu asutamine ja põhimäärus“, RT I, 28.07.2020, 15;
- majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määrus nr 28 „Riigi Infosüsteemi Ameti põhimäärus”, RT I, 09.06.2021, 17;

- majandus- ja taristuministri 15. aprilli 2015. a määrus nr 31 „Avalike teenuste pakkumise arendamiseks toetuse andmise tingimused ja kord“, RT I, 09.06.2021, 9;
- majandus- ja taristuministri 12. märtsi 2015. a määrus nr 21 „Nutika teenuste taristu arendamise toetamise tingimused ja investeeringute kava koostamise kord“, RT I, 09.06.2021, 10;
- rahandusministri 19. juuni 2012. a määrus nr 26 „Hasartmängukorraldaja elektroonilises arvestus- ja kontrollisüsteemis registreeritavate andmete loetelu ja sisestamise kord ning elektroonilise arvestus- ja kontrollisüsteemi Maksu- ja Tolliameti infosüsteemiga ühendamise kord“, RT I, 29.04.2015, 6;
- rahandusministri 7. aprilli 2004. a määrus nr 70 „Ühendusevälise riigi füüsilisele isikule võõrandatava kauba ekspordina käsitamise kord“, RT I, 19.05.2016, 23;
- Tervise- ja tööministri 6. märtsi 2019. a määrus nr 15 „Vee terviseohutuse infosüsteemi põhimäärus“, RT I, 12.03.2019, 20.

Eeltoodud uued määrused ning olemasolevate määruste muudatused jõustuvad 1. jaanuaril 2022. a. Mõningates eelnõudes on teatavate muudatuste jõustumise tähtajaks 1. jaanuar 2023. a – sel juhul on muudatus seotud AvTS-i muudatustega. Määruste kavandid on lisatud eelnõule.

Volitusnormide vajalikkust, selle eesmärki, sisu ja ulatust on põhjendatud vastava volitusnormi juures.

Eelnõu tulemusena muutub kehtetuks KüTS § 7 lõike 4 volitusnorm ning selle alusel antud ettevõtlus- ja infotehnoloogiaministri 5. juuli 2018. a määrus nr 40 „Võrgu- ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus“ (RT I, 10.07.2018, 6).[61] Volitusnorm ja seeläbi ka vastav määrus tunnistatakse kehtetuks, kuna sama sisuga määrus asub KüTS § 7 lg 5 alusel vastu võetavas Vabariigi Valitsuse määruses ning E-ITS-is endas.

AvTS-i muutmisega tunnistatakse kehtetuks AvTS § 43^9 lg 1 punkt 4 ehk volitusnorm Vabariigi Valitsuse 20.12.2007. a määruse nr 252 „Infosüsteemi turvameetmete süsteem“ kehtestamiseks, et asendada tänaseks aegunud ISKE uue E-ITS-iga. Uuendatud volitusnorm võimaldaks kehtestada ISKE asemel avalike ülesannete täitmiseks loodud äriprotsessidel (*business process*) põhineva turvameetmete süsteemi E-ITS.

9. Seaduse jõustumine

Seadus jõustub 1. jaanuaril 2022. a. Seaduse § 2 (avaliku teabe seaduse muudatused) jõustuvad 1. jaanuaril 2023. a. Vt ka eelnõu § 10 selgitusi.

10. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Küberturvalisuse seaduse muutmiseks on eelnõude infosüsteemis kaks toimikut (nr-d 21-0125 ja 21-0684; vastutajateks Majandus- ja Kommunikatsiooniministeerium), millede sisu viiakse kokku käesolevasse eelnõusse ning ühe toimiku (nr 21-0125) alla.

E-ITS-ga seotud eelnõu (toimik nr 21-0125) esitati eelnõude infosüsteemi kaudu kooskõlastamiseks Kaitseministeeriumile, Siseministeeriumile, Välisministeeriumile ja Justiitsministeeriumile ning arvamuse andmiseks Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule ning Eesti Infoturbe Assotsiatsioonile. Tagasiside saabus

[61] https://www.riigiteataja.ee/akt/110072018006?dbNotReadOnly=true.

Justiitsministeeriumilt, Kaitseministeeriumilt, Siseministeeriumilt, Välisministeeriumilt, Eesti Linnade ja Valdade Liidult ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidult.

Küberturvalisuse sertifitseerimise reguleerimisega seonduvalt on eelnõu koostamisse varasemalt kaasatud Tarbijakaitse ja Tehnilise Järelevalve Amet, Riigi Infosüsteemi Amet ning MTÜ-ks Eesti Standardimis- ja Akrediteerimiskeskus ühinenud juriidilised isikud (MTÜ Standardikeskus ja SA Eesti Akrediteerimiskeskus). Eelnõu saadetakse eelnõude infosüsteemi (toimik nr 21-0684) kaudu kooskõlastamiseks Justiitsministeeriumile, Rahandusministeeriumile ja Riigikantseleile ning arvamuse avaldamiseks Eesti Standardimis- ja Akrediteerimiskeskusele, Eesti Infoturbe Assotsiatsioonile ja Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule. Tagasiside saabus Justiitsministeeriumilt, Rahandusministeeriumilt, Eesti Standardimis- ja Akrediteerimiskeskuselt ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidult.

Mõlema teema kohta saabunud tagasiside on lisatud seletuskirja lisaks olevasse kooskõlastustabelisse.

Käesolev eelnõu on edastatud eelnõude infosüsteemi kaudu kooskõlastamiseks ja arvamuse avaldamiseks ministeeriumitele, Riigikantseleile, Eesti Linnade ja Valdade Liidule, Eesti Standardimis- ja Akrediteerimiskeskusele ning Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule. Eelnõu asub eelnõude infosüsteemi toimikus nr 21-0125.

Algatab Vabariigi Valitsus

…2021. a