Küberturvalisuse seaduse muutmise seaduse eelnõu seletuskiri

1. Sissejuhatus

Seaduseelnõuga muudetakse küberturvalisuse seadust. Muudatusega täpsustatakse seaduses kasutatavaid mõisteid, võrgu- ja infosüsteemide turvameetmete rakendamise ulatust ning muudetakse riiklikku ja haldusjärelevalvet puudutavaid sätteid.

Riigikogu võttis 10.12.2025 vastu küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi (NIS2) ülevõtmine). Nimetatud seaduse eelnõu (739 SE) (edaspidi *eelnõu (739 SE)*) menetlemisel jäi kaasatud Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (edaspidi *ITL*) eriarvamusele eelnõu küberturvalisuse 2. direktiivile vastavuse osas. Eelnõu (739 SE) menetlemisega oli kiire, sest NIS 2 direktiiv pidanuks olema Eesti õigusesse täies mahus üle võetud 2024. aasta 18. oktoobriks. Eesti vastu oli Euroopa Komisjoni poolt algatatud rikkumismenetlus.

Arvestades eelpool toodud pidas riigikaitsekomisjon oma 01.12.2025 istungil vajalikuks teha Justiits- ja Digiministeeriumile ning ITL-ile ettepanek läbi rääkida eelnõu (739 SE) väljatöötamise ja menetlemisel tekkinud ning lahendamata jäänud erimeelsused 2026. aasta märtsiks ning teha riigikaitsekomisjonile ülevaade erimeelsuste lahendamise tulemusest. Riigikaitsekomisjoni antud ülesande täitmiseks moodustati töörühm (edaspidi *KüTS töörühm*), kuhu kuulusid Justiits- ja Digiministeeriumi, Riigi Infosüsteemi Ameti, ITL-i ning advokaadibüroo WIDEN esindajad. Advokaadibüroo WIDEN esindajad olid kaasatud erapooletu osapoolena.

Riigikaitsekomisjon kutsus osapooled oma 13.04.2026 istugile, et saada ülevaade läbirääkimiste tulemustest, osapoolte seisukohtadest ja võimalikest kokkulepetest. Ühtlasi soovis komisjon teada, kas osapooled peavad vajalikuks küberturvalisuse seaduse muutmist. Istungi tulemusel soovis riigikaitsekomisjon saada Justiits- ja Digiministeeriumilt kokkulepitu osas seaduseelnõu kavandit ja seletuskirja läbi räägitud võimalike muudatuste ning muude leitud lahenduste kohta.

KüTS töörühma töötulemusi ning riigikaitsekomisjoni poolt 13.04.2026 istungil tehtud ettepanekuid arvesse võttes koostas Justiits- ja Digiministeeriumi riikliku küberturvalisuse talitus KüTS töörühma raporti põhjal eelnõu ning seletuskirja. Eelnõu ja seletuskirja teksti täpsustas riigikaitsekomisjoni nõunik-sekretariaadijuhataja Aivar Engel. Riigikaitsekomisjon otsustas konsensuslikult oma 04.05.2026 istungil eelnõu algatamise. Riigikaitsekomisjoni poolne eelnõu ettekandja on komisjoni liige Priit Sibul.

2. Seaduse eesmärk

Seaduse eelnõu eesmärk on esiteks ühtlustada küberturvalisuse 2. direktiivi[1] ja küberturvalisuse seaduse (edaspidi *KüTS*) termineid. Teiseks, luua seaduse subjektidele selgem arusaam Riigi

[1] Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, 14. detsember 2022, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv)

Infosüsteemi Ameti järelevalve ulatusest võrgu- ja infosüsteemide osas. Kolmandaks seotakse küberturvalisuse 2. direktiivi rakendusmäärusega kehtestatavad turvanõuded selgemalt teenustega, mida rakendusmäärus puudutab.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõus on toodud muudatusettepanekud, mis leidsid toetust KüTS töörühma poolt. ITLi esitatud muude ettepanekute osas jõuti KüTS töörühmas ühisele arusaamale, et seaduse tasemel ei ole neid teemasid vaja reguleerida. Ühine arusaam hõlmab muu hulgas Vabariigi Valitsuse määruse tasandil turvameetmete rakendamisel teenuse, mille osutamise asutus või ettevõtja on KüTS subjekt, põhise lähenemise ette nägemist ja küberturvalisuse 2. direktiivi rakendusaktide rakendamist teenuste põhiselt. Muud nimetamata ettepanekud reguleeritakse kokkuleppe kohaselt samuti kas määrustega või koostatakse vastav juhendmaterjal. Ühtlasi leppis KüTS töörühm alguses kokku, et arutelu alla ei võeta teemasid, mida ei ole käsitletud ITL poolt riigikaitsekomisjoni saadetud kirjas[2] ning ei tehta kirjast mittelähtuvaid muudatusettepanekuid.

KüTS § 2 punkti 19 muudetakse ja sõnastatakse uuesti küberintsidendi termin. Eelnõu (739 SE) menetlemise ajal esitas ITL Riigikogu riigikaitsekomisjonile oma arvamuse, mille kohaselt eelnõus sisalduv küberintsidendi termin ei vasta küberturvalisuse 2. direktiivi artikkel 6 punktis 6 sätestatule.

Eelnõu (739 SE) kohaselt oli küberintsident võrgu- ja infosüsteemis toimuv sündmus, mis ohustab või kahjustab võrgu- ja infosüsteemi turvalisust. ITL oli seisukohal, et tegemist on direktiivi olulise laiendamisega, mida ei tohi minimaalse ülevõtmise korral mingil juhul teha.

ITL jäi seisukohale, et teavitamise kohustused peavad olema selgelt arusaadavad ning Eestis ei peaks mõistet laiendama. Seda enam, et mitmed teenuse osutajad peavad lähtuma teavitamisel küberturvalisuse 2. direktiivi rakendusmäärusest 2024/2690, mille aluseks on direktiivis sisalduv küberintsidendi definitsioon. See tähendab, et Euroopa Komisjon on täpsustanud intsidentidest teavitamist küberturvalisuse 2. direktiivi rakendusaktis lähtudes direktiivi mõistest ning praktika hakkab kujunema vastavalt sellele.

Nõue, et ettevõtted ja asutused peavad esitama intsidenditeateid ka sündmuse kohta, mis ohustab võrgu- või infosüsteemi turvalisust, tekitab seaduse subjektidest ettevõtetele ja asutustele olulise vastavusriski, kuna oht on hinnanguline ja subjektiivne. See suurendab oluliselt ja ebamõistlikult regulatiivset koormust nii seaduse subjektidele kui ka järelevalve teostajale. Samal ajal on küberturvalisuse 2. direktiivi kohaselt küberohtude kohta info jagamine oluline pigem riikide vastavate asutuste vahel ning subjektidele on see võimalus antud vabatahtlikuna.

ITL sõnul ei olnud eelnõu koostamisel arvestatud, milline koormus tekib teenuseosutajatele ja järelevalvele igast ohust teavitamisel. Näiteks võib lugeda selliseks ohuks igat petukirja ja -kõne, mille hulk igakuiselt ulatub küberruumis teatavasti miljonitesse. Küberturvalisuse 2. direktiivi koostamisel mõisteti ilmselt, et ohu hõlmamine intsidendi mõistesse tekitab liigset subjektiivsust ning põhjendamatut vastavusriski ettevõtetele ja asutustele, kuna oht küberturvalisusele eksisteerib pidevalt. ITL tõi välja, et kui praktikas hakkaksid kõik igast ohust järelevalvet teavitama, siis ei saaks subjektid ise ega ka Riigi Infosüsteemi Amet millegi muuga tegeleda.

---

[2] ITLi 05.11.2025 kiri nr 6.1-2/13-1, kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/arvamused/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine

ITL leidis, et kuigi ohu kriteerium sisaldub ka kehtiva KüTS-i küberintsidendi mõistes, tuleb antud sättest kustutada ja Eesti õigus Euroopa Liidu õigusega vastavusse viia. ITL osundas, et intsidendiohust tuleb küberturvalisuse 2. direktiivi kohaselt teavitada ainult vabatahtlikult (vt direktiivi artiklid 23 ja 30) ning nii peaks olema ka Eesti seaduse kohaselt.

Justiits- ja Digiministeerium jäi eelnõu (739 SE) menetlemisel seisukohale, et küberintsidendi termin oli samasisuline ka sellel ajal kehtinud KüTS versioonis ning minimaalne üle võtmine ei puuduta olemasolevaid sätteid vaid direktiiviga lisanduvat. Küberintsidendi mõistet ei muudetud, kuid rohkete lisandunud terminite tõttu sõnastati ümber kogu § 2 mistõttu esitati ka olemasolev termin eelnõus uuesti. Seega ei olnud termini sisuline muutmine kooskõlas ülevõtmise eesmärgiga, milleks oli ka olemasolevate sätete muutmata jätmine, kui direktiivist ei tulenenud teisiti ja seetõttu ei toetanud termini sisulist muutmist. KüTSi töörühma menetluse käigus selgitas Justiits- ja Digiministeerium, et KüTSi küberintsidendi mõistes oleva tekstiosa "võrgu- ja infosüsteemi turvalisust" viitab sama seaduse § 2 punktis 38 sätestatud samanimelisele terminile. KüTS töörühma arutelude käigus tõdeti, et kõik KüTSi subjektid ei pruugi küberintsidendi puhul selle terminiga seost ära tunda.

Advokaadibüroo WIDEN tõi osapoolte seisukohti ära kuulates välja järgmise.
Esiteks - hetkel sisaldab KüTS § 2 punktis 19 toodud termin „küberintsident“ ülevõtmiskohustuse kontekstis kahte küberturvalisuse 2. direktiivi alusterminit: intsident ning napilt toimumata jäänud küberintsident (*near miss*) – selguse ja õigusloome jätkusuutlikkuse huvides on mõistlik need kaks terminit eraldada.
Teiseks – kehtiva versiooni sõnastus, mille järgi küberintsident KüTS § 2 punkti 19 järgi sisaldab ka sündmust, mis ohustab võrgu- ja infosüsteemi turvalisust, on direktiivi teksti ja eesmärgiga võrreldes laiendav – muuhulgas on võimalik KüTS-i tõlgendada selliselt, et on olemas teavituskohustus ka napilt toimumata jäänud küberintsidentide osas, olgugi, et küberturvalisuse 2. direktiivist see kohustus ei tulene.

Küberintsidendi praegune sõnastus hõlmab vaid võrgu- ja infosüsteemis aset leidnud sündmust, mis ei ole (muuhulgas ülevõtmiskohustuse kontekstis) piisav, kuivõrd küberintsident, millel on vahetu kahjulik mõju võrgu- ja infosüsteemile võib leida aset ka väljaspool subjekti enda võrgu- ja infosüsteemi.

Võrdlus Läti ja Leedu õiguskorraga näitas, et teised Balti riigid on otsustanud lähtuda küberturvalisuse 2. direktiivi ülevõtmisel kolmest direktiivi alusterminist „intsident“, „napilt toimumata jäänud küberintsident“ ning „küberoht“. Neis riikides ei ole subjektidel kohustust teavitada kohustuslikus korras napilt toimumata jäänud küberintsidentidest ega küberohtudest - teavitamiskohustus on rangelt vaid intsidentide osas. Küll aga on Läti ja Leedu laiendanud teavituskohustust direktiiviga võrredes selliselt, et teatud juhtudel on subjektidel kohustus teavitada regulaatorit ka taolistest intsidentidest, mis ei ole olulised.

KüTS töörühmas jõuti arutelude tulemusel kokkuleppele teha ettepanek KüTS termini „küberintsident“ muutmiseks viisil, mis vastab küberturvalisuse 2. direktiivi artikkel 6 punktile 6. Ühtlasi ohu välja jätmisega seoses võetakse kasutusele termin „napilt toimumata jäänud küberintsident“ mille sisu vastab küberturvalisuse 2. direktiivi artikkel 6 punktis 5 sätestatud „napilt ära hoitud intsidendile“ (**KüTS § 2 punkti 22[1]**).

KüTS § 8[1] lõike 1 punktide 1 ja 2 muutmisega nähakse ette napilt toimumata jäänud intsidendist vabatahtlik teavitamine.

Intsidendist, sh napilt toimumata jäänud intsidendi osas jäi Riigi Infosüsteemi Amet arvamusele, et KüTS-i subjektid peaksid kohustuslikus korras teavitama ametit mitte ainult

olulisest küberintsidendist nagu nõuab küberturvalisuse 2. direktiiv, vaid lisaks sellele peaks teavituskohustus kehtima ka „olulistele napilt toimumata jäänud küberintsidentidele“. Riigi Infosüsteemi Ameti hinnangul tingib Eesti riskiprofiil (nt agressiivne idanaaber) kõrgendatud küberturbevajaduse võrreldes Euroopa Liidu miinimumstandardiga – on loomulik, et kriitilistes valdkondades näeb riik enda seaduse subjektidele ette kõrgemad ootused kui muud Euroopa Liidu liikmesriigid. Täiendav teavituskohustus on vajalik ja kohane meede ning ei põhjustaks subjektidele olulist lisakoormust, kusjuures olulisuse kriteeriumid on samad, mis küberintsidendi puhul.

ITL-i hinnangul ei ole võrreldes direktiivis sätestatuga napilt toimumata jäänud küberintsidendi juures täiendava teavituskohustuse ette nägemine Eestis vajalik, ega mõistlik. ITL seisukohast tuleks lähtuda olemasolevast küberturvalisuse 2. direktiivi raamistikust ning mitte direktiivi „kuldplaatida“ (*goldplating*). Kohustus teavitada olulisest küberintsidendist on piisav ning täienduste tegemine üksnes muudaks riigisisese õiguse rakendamise keeruliseks ja tekitaks asjatut segadust. ITL seisukohast on probleem lahendatav teadlikkuse tõstmisega subjektide hulgas, et subjektid oleksid paremini võimelised rakendama turvameetmeid ning vajadusel ära tundma teavituskohustuse alla kuuluvaid küberintsidente.

Justiits- ja Digiministeerium leidis, et kui küberintsidendi termin muudetakse sarnaseks küberturvalisuse 2. direktiivis sätestatuga ja terminist eraldatakse napilt toimumata jäänud küberintsidendi osa (st oht), siis uue termini sisustamisel peaks lähtuma samuti direktiivist ja ei peaks tekitama kohustust teavitada “olulistest napilt toimumata jäänud küberintsidentidest”. Küll tuleb selgemalt ette näha vabatahtliku teavitamise võimalus. Napilt toimumata jäänud küberintsidendi termin sisaldab endas subjektiivsust „mis oleks võinud kahjustada“, mistõttu on KüTSi subjektil raske hinnata, kas ja milline oleks olnud mõju kui intsident oleks aset leidnud. Subjektiivsus tooks kaasa täiendava hindamiskohustuse KüTSi subjektile. Teisalt oleks subjektiivsus küsitav ka riikliku või haldusjärelevalve vaatenurgast, sest kuidas tõestada, et intsidendi toimumisel oleks olnud oluline mõju.

Arvestades eeltoodut on eelnõus jäädud napilt toimumata jäänud küberintsidendi vabatahtliku teavitamise juurde.

KüTS §-i 2 punkti 26 muudetakse. KüTSi terminist „sihipärane turvaaudit“ jäetakse välja sõna „sihipärane“. Samuti lisatakse termini „turvaaudit“ seletusse sõna „üksus“, et termin siduda panemini KüTS subjektidega võrgu- ja infosüsteemidega.

ITL tõi oma kirjas riigikaitsekomisjonile välja, et KüTS-is tuleb defineerida üheselt ja selgelt järelevalve meetmeid puudutavad terminid nagu eelkontroll, pisteline kontroll, korrapärane ja sihipärane turvaaudit (üliolulisel üksusel), sihipärane turvaaudit (olulisel üksusel), erakorraline (*ad hoc*) audit ja turvalisuse kontroll. Nende mõistete selgitusse tuleks lisada, millal, mis ulatuses (mahus) ja mis meetmetega neid teostatakse.

Järelevalve mõistete sisustamine ja ühene arusaam on vajalik nii järelevalveasutusele kui ka neile, kelle üle järelevalvet teostatakse. Subjektidel peab olema võimalik eelnõust aru saada, millised õigused on Riigi Infosüsteemi Ametil ja millised subjektil.

KüTS töörühma töö tulemusena otsustati defineerida ainsa katusterminina „turvaaudit“ senise „sihipärase turvaaudit“ asemel. Definitsiooni sisu jääb samaks, sest senine definitsioon ei iseloomustanud sihipärasust. Turvaauditi sihipärasust jääb senisel kujul iseloomustama **KüTS-i lisatavad § 16 lõike 1^1 punkt 2^1 ja § 17 lõike 1^1 punkt 2^1**. Lisaks selgitab Riigi Infosüsteemi Amet sihipärase turvaauditi tähendust enda juhendmaterjalis ja kokkuleppe kohaselt tehakse see kõigile kättesaadavaks ameti veebilehel.

Samuti saavutati kokkulepe, et terminite sihipärane turvaaudit, vajaduspõhine turvaaudit, korrapärane turvaaudit, pisteline kontroll, turvalisuse kontroll tähendusi ei ole vajalik KüTS-is esitada, kui Riigi Infosüsteemi Amet korraldab nende selgitamise oma juhendmaterjalis ja teeb ajakohased lahtikirjutused kõigile avalikult kättesaadavaks oma veebilehel. Kokkuleppest tulenevalt tunnistatakse kehtetuks **KüTS § 2 punkt 32**.

Riigi Infosüsteemi Ameti poolt terminite defineerimise kohustuse võtmise tulemusel jäetakse seadusest välja „pisteline järelevalve". Tegemist oli katusmõistega küberturvalisuse 2. direktiivis kasutatavatele mõistetele „pisteline kontroll'' ja „*ad hoc*" turvaaudit. KüTS-i jäävad sarnaselt direktiivile „pisteline kontroll" ja „vajaduspõhine turvaaudit" (*ad hoc* audit) defineerimata kujul. Kokkuleppe tulemusel muudetakse **KüTS § 16 lõike 1[1] punkti 1** ja **KüTS § 17 lõike 1[1] punkti 1** ning **KüTS § 16 lõiget 1[1] ja § 17 lõiget 1[1]** täiendatakse **uue punktiga 1[1]**.

Riigi Infosüsteemi Amet toetas üldjoontes lähenemist, mille kohaselt erinevaid turvaauditeid ei defineerita seaduse tasandil, kuid jäi teistest osapooltest eriarvamusele katustermini „turvaaudit" seaduses avamise osas.

Riigi Infosüsteemi Ameti hinnangul ühtib „turvaauditi" definitsioon kavandatud kujul sisuliselt järelevalve tegevustega. Tegemist on täpselt samade tegevustega, mida amet juba üle 10 aasta igapäevaselt teeb. Riigi Infosüsteemi Ameti seisukohalt toob defineerimine kaasa olukorra, kus sama tegevuste komplekti hakatakse edaspidi nimetama kahte erinevat moodi ning nendele kehtivad erinevad nõuded. Kuna turvaauditit küberturvalisuse 2. direktiivi mõistes tehtaks järelevalve tegevuste raames, siis tekiks olukord, kus üheks järelevalve toiminguks on järelevalve tegemine, mis loogiliselt ei ühildu.

Lisaks sellele leidis Riigi Infosüsteemi Amet, et osasid turvaauditeid saab teha vaid üliolulistе üksuste suhtes ning see omakorda muudab keeruliseks järelevalvemenetluste tegemise oluliste üksuste suhtes, sest subjektid ei pruugi osata eristada järelevalve tegevusi. Riigi Infosüsteemi Ameti hinnangul tekib õigusselgusetus asjaolus, millal tegevused on käsitatavad järelevalvena ning millal turvaauditina. Riigi Infosüsteemi Ameti sõnul puuduvad neil oskused ja teave auditite tegemiseks, kuid samal ajal on auditeerimise teenus turul kättesaadav. Eeltoodust tulenevalt tegi Riigi Infosüsteemi Amet ettepaneku täiendada definitsiooni järgmiselt: „mida teeb sõltumatu välisaudiitor Riigi Infosüsteemi Ameti tellimusel".

Justiits- ja Digiministeeriumi hinnangul „turvaaudit", kui termin, vastab KüTS kehtiva versiooni § 2 punkt 26 sätestatud terminile sihipärane turvaaudit. Tegu on nö katusterminiga, mis ei sätesta ühegi isiku õigusi ja kohustusi. Turvaauditit ei kasutata seaduses iseseisvalt, vaid kasutatakse alamterminite koosseisus - vajaduspõhine turvaauditit, sihipärane turvaaudit ja regulaarne turvaauditi. Seejuures on mõlemad alamterminid järelevalve sätetes (KüTS § 16 ja 17). Mõlemad on seega auditi osa riiklikust või haldusjärelevalvest, mille teostajaks saab olla vastavalt korrakaitseseadusele või Vabariigi Valitsuse seadusele vaid Riigi Infosüsteemi Amet. Katusterminit ei ole võimalik kitsendada ilma Riigi Infosüsteemi Ameti õigusi piiramata. Küberturvalisuse 2. direktiivi artikli 32 lõike 2 punkt b ja artikli 33 lõike 2 punkt b sätestavad, et turvaauditi tegemise õigus tuleb tagada järelevalveülesandena pädevale asutusele ehk antud juhul on tegemist järelevalve meetmega, mitte sõltumatu välise hindaja hinnanguga kas KüTSi subjekti infoturbe halduse süsteem ja selle raames rakendatud meetmed vastavad subjekti vajadustele. Meetmete rakendamise ulatuse hindamine välise audiitori poolt ei ole järelevalve. Samuti ei ole „sõltumatu välisaudiitor" pädev asutus järelevalveülesannete täitmiseks, ei Eesti ega Euroopa Liidu õiguse kohaselt.

Justiits- ja Digiministeerium ei nõustunud Riigi Infosüsteemi Ameti poolse teadmise puudumisega, kuivõrd amet on ise välja toonud, et turvaauditi termin vastab järelevalves juba täna tehtavatele tegevustele. Samuti on Riigi Infosüsteemi Amet osaline võrgu- ja infosüsteemide küberturvalisuse nõuete, sealhulgas Eesti infoturbestandardi väljatöötamises ning tema ülesanne on muuhulgas nõustada KüTSi subjekte küberturvalisuse valdkonna õigusaktide täitmisel.[3] Niisamuti ei ole piiratud Riigi Infosüsteemi Ametil järelevalvemenetlustes kasutada toimingutes väliste ekspertide abi, kuid menetlusotsuste tegemine on vaid ameti pädevuses.

Arvestades ITL soovi, et seaduses oleks järelevalve meetmeid käsilevad terminid selgelt defineeritud, sealhulgas peaks olema selge, millal, mis ulatuses (mahus) ja mis meetmetega seda teostatakse ning KüTSis sätestatud Riigi Infosüsteemi Ameti ülesannet teostada riiklikku ja haldusjärelevalvet, toetab Justiits- ja Digiministeerium termini „turvaaudit“ defineerimist eelnõus esitatud kujul. Definitsiooni toetab ka ITL.

KüTS § 12 lõiget 4[1] täiendataks viitega napilt toimumata jäänud küberintsidendile. Muudatuse kohaselt Riigi Infosüsteemi Amet lisab Euroopa Liidu Küberturvalisuse Ametile esitatavasse koondaruandesse ka napilt toimumata jäänud küberintsidentide koondandmed. Andmed esitatakse anonüümsel kujul. Koondaruande jaoks vajaliku teabe saab Riigi Infosüsteemi Amet küberintsidentide registrist.

Napilt toimumata jäänud küberintsidendist teavitamine on KüTSi subjektile vabatahtlik (vt ka KüTS § 2 punktide 19 ja 22[1] muudatuste seletust). Teavitused kantakse Riigi Infosüsteemi Ameti poolt peetavasse küberintsidentide registrisse. Sellest tulenevalt tehakse muudatus ka küberintsidentide registri eesmärki (**KüTS § 13 lõige 1**) ning registrisse kantavat teavet (**KüTS § 13 lõige 2**) puudutavates sätetes.

Küberintsidendi termini muutmisega on seotud ka **KüTS § 13 lõike 5 punktis 1** tehtav muudatus. KüTS kehtiv versioon sätestab, et küberintsidendi kohta kantud andmeid säilitatakse küberintsidentide registris viis aastat alates küberintsidendi lahendamisest. Napilt toimumata jäänud küberintsidendi termini tekkimisega on vajalik ka KüTS § 13 lõike 5 punkti 1 muutmine. Muudatusega nähakse ette, et vaid küberintsidendi ja olulise mõjuga küberintsidendi andmeid säilitatakse viis aastat küberintsidendi lahendamisest arvates. Napilt toimumata jäänud küberintsidendi andmeid säilitatakse viis aastat alates registrisse kandmisest vastavalt KüTS § 13 lõike 5 punktile 2.

KüTS § 7 lõike 7 kehtetuks tunnistamisega jäetakse seaduse tasemel välja viide küberturvalisuse 2. direktiivi artikli 21 lõikes 5 nimetatud teenuseosutajate kohustusele lähtuda rakendusaktis sätestatud teenuse puhul sama rakendusaktiga kehtestatud nõuetest (edaspidi *rakendusmäärus*)[4]. Kehtiva KüTS versiooni sõnastus on ebaselge, kuna sellest ei nähtu üheselt, kas rakendusakti subjekt peab rakendusaktis nimetatud teenuse osutamisel lähtuma üksnes rakendusaktiga kehtestatud nõuetest või tuleb tal lisaks järgida ka KüTS-is sätestatud nõudeid.

Osapooled jäid KüTS töörühmas tolle lõike muutmise osas eri seisukohtadele.
ITL ning Justiits- ja Digiministeerium jõudsid ühisele seisukohale, et KüTS-i tuleks muuta nii, et:

- subjektidele kohalduvad direktiivi rakendusaktis sätestatud nõuded rakendusmääruses loetletud teenuste osas;

[3] Riigi Infosüsteemi Ameti põhimäärus (Riigi Infosüsteemi Ameti põhimäärus–Riigi Teataja)
[4] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1776846017801

- nimetatud ulatuses kohaldatakse rakendusmääruse nõudeid Eesti infoturbestandardi või selle alternatiivina kasutatava rahvusvahelise standardi ISO/IEC 27001 asemel;
- esmased turvameetmed kehtivad kõigile KüTSi subjektidele.

Riigi Infosüsteemi Amet ei nõustunud võimaliku lahendusega. Amet asus seisukohale, et rakendusmäärus täiendab olemasolevaid nõudeid, mitte ei asenda neid.

Riigi Infosüsteemi Amet on seisukohal, et rakendusmääruse nõuded peavad kehtima täiendavalt KüTS-i üldistele nõuetele. Ameti põhjendused:

- seda toetab rakendusmääruse tekst, viidates selle preambula punktile 7, mis sätestab, et *lisaks asjaomastele Euroopa ja rahvusvahelistele standarditele võivad asjaomastel üksustel aidata käesoleva määruse nõuete täitmist tõendada ka liikmesriikide siseriikliku õigusega ettenähtud raamistikud, juhised või muud mehhanismid*;
- rakendusmääruse subjektideks on muuhulgas usaldusteenuse osutajad, millele Eesti kui digiriik tugevalt toetub, seetõttu on vajalik, et ka neilt nõutaks konkreetse standardi (nagu Eesti infoturbestandard või rahvusvaheline standard ISO/IEC 27001) rakendamist;
- sarnane lähenemine on Saksamaal ja Soomes.

ITL-i hinnangul tuleks KüTS-i vastavat sätet muuta selliselt, et rakendusmäärus kohalduks KüTS subjektile esmajärjekorras ning subjektile ei kehtestataks siseriiklikult täiendavaid nõudeid nendes küsimustes, mis on juba rakendusmääruses reguleeritud. Näiteks ei peaks subjekt järgima Eesti infoturbestandardit või rahvusvahelist standardit ISO/IEC 27001, vaid lähtuks turvameetmete osas üksnes rakendusmääruses sätestatust. Eeltoodu ei piiraks siiski teiste KüTS-ist tulenevate nõuete kohaldamist valdkondades, mida rakendusmäärus ei reguleeri – näiteks oleks subjekt jätkuvalt kohustatud määrama vastutava juhatuse liikme vastavalt KüTS § 6[1] lõikele 1. Lisaks tõi ITL välja järgmise:

- vastasel juhul peab rakendusmääruse subjekt järgima sisuliselt mitut turvastandardit korraga, milles on teatud erisusi;
- eesmärgiks on võtta küberturvalisuse 2. direktiiv üle minimaalselt, millega ei ole kooskõlas täiendavate siseriiklike nõuete esitamine;
- rakendusmääruse mõte on piiriüleselt teenuseid osutavatele subjektile kehtestada ühesugused nõuded ning kohalikud lisanõuded on selle eesmärgiga vastuolus;
- seisukohta toetab ka Euroopa Komisjoni küberturvalisuse 2. direktiivi muutmise ettepanek, mille kohaselt ei tohi liikmesriik rakendusmääruse olemasolu korral sätestada täiendavaid tehnilisi, metoodilisi või valdkondlikke nõudeid.[5]

Kuulates ära Riigi Infosüsteemi Ameti ja ITL seisukohad, tegi Justiits- ja Digiministeerium järgmised ettepanekud:

- KüTS § 7 lõige 7 tunnistatakse kehtetuks ning see teema viiakse KüTS § 7 lõike 5 alusel antud Vabariigi Valitsuse määrusesse;
- Vabariigi Valitsuse määruses sätestatakse, et Eesti infoturbestandardit ja rahvusvahelist standardit ISO/IEC 27001 ei pea järgima teenuste osas, mis on hõlmatud rakendusmäärusega[6].

Ettepanekud on kooskõlas juba varem eelnõu (739 SE) aruteludes läbi räägitule, et turvameetmete rakendamisel on võimalik, sarnaselt kuni 01.01.2026 kehtinud KüTS

[5] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=COM%3A2026%3A0013%3AFIN

[6] Rakendusmäärus kohaldub domeeninimede süsteemi teenuse osutajatele, tippdomeeninimede registrite pidajatele, pilvandmetöötlusteenuse osutajatele, andmekeskusteenuse osutajatele, sisulevivõrguteenuse osutajatele, haldusteenuse osutajatele, infoturbeteenuse osutajatele, internetipõhise kauplemiskoha pidajatele, veebipõhise otsingumootori pakkujatele, sotsiaalmeediaplatvormi pakkujatele ja usaldusteenuse osutajatele.

versioonile lähtuda teenustest. Kuigi küberturvalisuse 2. direktiiviga laiendatakse turvanõuete rakendamise kohustus kogu organisatsioonile, siis rakendusaktidega on võimalik reguleerida turvameetmete rakendamise ulatust teenustepõhiselt, ilma organisatsiooni üldisest kohustusest vabastamata. Teiseks, kui tekitada lähenemine, et KüTSi subjektid kohaldavad terve üksuse üleselt turvameetmete kontekstis ainult rakendusmääruses ette nähtud nõudeid, siis see tähendab, et riigil puudub võimalus ette näha KüTSi subjektidele sama seaduse alusel või muudes õigusaktides nõudeid, mis on seotud küberturvalisuse 2. direktiivi artikli 21 ülevõtmise ja selle täpsustamisega. Samuti peaks rakendusmääruses mainitud teenuse tõttu konkreetne KüTSi subjekt rakendama ainult rakendusmääruse nõudeid ka teenustele, mis pole määruses nimetatud. Sel juhul tekib potentsiaalne õigusselgusetus, mil määral kohalduvad subjektidele ka teistes õigusaktides ette nähtud nõuded, mis on ennekõike Eesti spetsiifilised, kuid mis ei ole reguleeritud rakendusmääruses – nt infosüsteemide andmevahetuskihi ehk X-tee kasutamisega seotud nõuded või nõuded, mis on seotud riikliku elektroonilise isikutuvastamise ja digitaalse allkirjastamisega.

KüTS töörühma töö raames vaatas advokaadibüroo WIDEN ka Soome, Leedu, Läti ning Saksamaa lahendusi rakendusmääruse osas.

Soomes ei ole nende seaduse subjektidel üldist kohustust rakendada rahvusvahelist standardit ISO/IEC 27001 või muud konkreetset standardit lisaks rakendusmäärusele. Siiski võib valdkonnapõhises õigusaktist või järelevalveasutuse kehtestatud siduvas tehnilises regulatsioonist tulla täiendavaid nõudeid, sealhulgas kohustus järgida konkreetset standardit või hankida konkreetne sertifikaat.

Leedus on kõik subjektid, välja arvatud usaldusteenuse osutajad, kohustatud järgima üksnes rakendusmääruses toodud küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid. Usaldusteenuse osutaja peab järgima nii rakendusmääruses kui ka Leedu siseriiklikus õiguses sätestatud küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid.

Lätis peavad kõik subjektid eelkõige lähtuma rakendusmääruses toodud nõuetest ning muud nõuded kohalduvad neile üksnes ulatuses, milles need ei ole vastuolus rakendusmäärusega. Praktikas jääb ebaselgeks, kas olukorras, kus nt rahvusvaheline standard ISO/IEC 27001 näeb rakendusmäärusega võrreldes ette täiendava nõude, tuleb seda rakendada või mitte.

Saksamaal sätestab BSI-Gesetz (BSIG), et rakendusmääruse nõuded on ülimuslikud Saksamaa siseriiklike nõuete osas, mis puudutavad konkreetseid turvanõudeid. BSIG § 30 lg 5 sätestab, et kui rakendusmääruse turvameetmed ei ole piisavad, võib rakendusmääruse turvanõudeid laiendada ja täpsustada. Saksamaa nõuab ka konkreetset standardit, näiteks avaliku sektori asutused peavad lähtuma IT-Grundschutz'ist.

Arvestades kirjeldatud muudatusega seonduvat otsustas Justiits- ja Digiministeerium jätkuvalt toetada KüTS § 7 lõike 7 kehtetuks tunnistamist ning vastava teema reguleerimist Vabariigi Valitsuse 09.12.2022. a määruses nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“. (vt ka seletuskirja lisa)

Sätte kehtetuks tunnistamisega on seotud ka **KüTS § 18^2 lõike 1** ja **18^3 lõike 1** muudatused. Nimetatud sätetest jäetakse välja viide kehtetuks tunnistatavale sättele.

KüTS § 17^4 lõike 2, lõike 4 ja § 17^5 lõike 1 muutmisega viiakse sätted kooskõlla küberintsidendi termini muutmisega ja napilt toimumata jäänud küberintsidendi termini lisamisega. Muudatuse tulemusel omab Riigi Infosüsteemi Amet jätkuvalt õigust jagada asjaomaste asutustega teavet muuhulgas napilt toimumata jäänud küberintsidentide kohta.

4. Eelnõu terminoloogia

Eelnõuga võetakse kasutusele järgmised uued terminid:

- *napilt toimumata jäänud küberintsident* - sündmus, mis oleks võinud kahjustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust, kuid mis õnnestus ära hoida või mis ei tekkinud;
- *turvaaudit* – võrgu- ja infosüsteemi andmike ja toimingute sõltumatu läbivaatus ning uurimine, et kontrollida üksuse võrgu- ja infosüsteemi turvameetmete adekvaatsust ning vastavust kehtivale infoturvapoliitikale ja tööprotseduuridele, avastada turvarikkeid ning soovitada võimalikke järelduvaid meetme-, poliitika- ja protseduurimuudatusi.

5. Eelnõu vastavus Euroopa Liidu õigusele

Käesolev eelnõu on kooskõlas Euroopa Parlamendi ja nõukogu 14.12.2022. a. direktiiviga 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv).
Kuna küberturvalisuse 2. direktiiv võeti üle ennekõike eelnõuga (739 SE), on selle materjalide hulgas ka direktiivi ja tolle ülevõtmisseaduse vastavustabel. Siinkohal esitatakse need sätted, mis on seotud kommenteeritava eelnõuga:
1) artikli 6 punkt 5 = KüTS § 2 p 22^1;
2) artikli 6 punkt 6 = KüTS § 2 p 19;
3) artikli 13 lõige 3 = Riigi Infosüsteemi Ametil on pädeva asutuse, ühtse kontaktpunkti ja CSIRTi ülesannetes (KüTS § 5 lg 3 punktid 1 ja 3), kuid kuna julgeolekuasutused on piiratud ulatuses pädev asutus (KüTS § 5 lg 4), siis koostöö kohta kehtivad KüTS § 17^4 lg 1 p 6 ja lg 4;
4) artikli 13 lõige 5 = KüTS § 17^4 lg 2 ja 4. Seotud on ka KüTS § 8, § 12 lg 3, § 13 lg 1, Riigi Infosüsteemi Ameti põhimääruse § 8 lg 4 p 3 ja 4 ning § 13 lg 1 p 1-4;
5) artikli 21 lõige 5 = Vabariigi Valitsuse 09.12.2022. a määrus nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (vt seletuskirja lisa);
6) artikli 23 lõike 9 esimene lause = KüTS § 12 lg 4^1 ja § 20 lg 3;
7) artikli 23 lõige 10 = KüTS § 17^4 lg 2, kuid seotud on ka KüTS § 6 p 4, Riigi Infosüsteemi Ameti põhimääruse § 8 lg 1 p 13 ja lg 2 ning § 13 lg 1 p 2;
8) artikli 29 lõige 1 = KüTS § 17^5 lg 1;
9) artikli 29 lõige 2 = KüTS § 17^5 lg 1, 2 ja 3;
10) artikli 30 lõige 1 = KüTS § 8^1 lg 1 p 1 ja 2; teemaga on seotud ka KüTS § 13 ja selle alusel antud määrus ning turvahaavatavusest teavitamise aspekt (vt KüTS § 5 lg 3 p 4, millega seotud ülesanne on reguleeritud Riigi Infosüsteemi Ameti põhimääruse[7] § 13 lg 3^1;
11) artikli 30 lõike 2 teise lõigu esimene lause = puudub üle võtmise vajadus, kuna Riigi Infosüsteemi Ametil on CSIRTi, pädeva asutuse ja ühtse kontaktpunkti ülesanded (KüTS § 5 lg 3 p 1 ja 3). Julgeolekuasutuste ja Riigi Infosüsteemi vahelise koostöö kohta on ette nähtud KüTS § 17^4 lg 1 p 6 ja lg 4;
12) artikli 32 lõike 2 punkt a = HMS § 5 ja kaudselt § 6, KüTS § 15 lg 1, § 16 lg 1^1 p 1 ja § 17 lg 1^1 p 1, KorS §-id 30, 31, 32, 49, 50 ja 51, VVS § 75^2 lg 1 p-d 3 ja 5. VTMS § 2, § 24 lg 1, § 31 lg 1 ja lg 1^1 ning § 35, KrMS §-id 63, 68, 69, 69^2, 83, 86, 91, 91^1, 93, 95, 109^1. Vt ka KüTS § 2 p 14;[8]
13) artikli 32 lõike 2 punkt b = KüTS § 16 lg 1^1 p-d 2 ja 2^1, § 17 lg 1^1 p-d 2 ja 2^1, § 16 lõike 1^2 ja § 17 lõike 1^2 alusel kehtestatud ministri määrus (määrus koostamisel). VTMS § 2, § 24 lg 1,

[7] https://www.riigiteataja.ee/akt/129012026002
[8] Haldusmenetlus, sh riiklik järelevalve ja haldusjärelevalve (HMS, KorS, VVS ja KüTSi viited) ning väärteomenetluse korral (KarS, KrMS ja VTMS viited).

§ 31 lg 1 ja lg 1^1 ning § 35, KrMS §-id 63, 68, 69, 69^2, 83, 86, 91, 91^1, 93, 95, 109^1. Vt ka KüTS § 2 p 26;
14) artikli 32 lõike 2 punkt c = KüTS § 16 lg 1^1 p 1^1 ja § 17 lg 1^1 p 1^1. VTMS § 2, § 24 lg 1, § 31 lg 1 ja lg 1^1 ning § 35, KrMS §-d 63, 68, 69, 69^2, 83, 86, 91, 91^1, 93, 95, 109^1.
15) artikli 32 lõige 9 = KüTS § 17^4 lg 2;
16) artikli 33 lõike 2 punkt a = HMS § 5 ja kaudselt § 6, KüTS § 15 lg 1, § 16 lg 1^1 p 1 ja § 17 lg 1^1 p 1, KorS §-id 30, 31, 32, 49, 50 ja 51, VVS § 75^2 lg 1 p-d 3 ja 5. VTMS § 2, § 24 lg 1, § 31 lg 1 ja lg 1^1 ning § 35, KrMS §-id 63, 68, 69, 69^2, 83, 86, 91, 91^1, 93, 95, 109^1. Vt ka KüTS § 2 p 14;
17) artikli 34 lõige 4 = KüTS § 18^2 lg 1 (füüsilised isikud) ja 2 (juriidilised isikud);
18) artikli 34 lõige 5 = KüTS § 18^3 lg 1 (füüsilised isikud) ja 2 (juriidilised isikud).
Kehtiva õiguse suhtes kohaldub ka NIS2-direktiivi artikkel 5, mis näeb ette järgmist: *käesolev direktiiv ei takista liikmesriike tarbijate kaitseks vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.*

6. Seaduse mõjud

Seaduseelnõuga tehakse tehnilisi muudatusi lähtuvalt küberturvalisuse 2. direktiivist, mistõttu eelnõu jõustumisel vahetu mõju kõigis mõjuvaldkonades puudub.

7. Seaduse rakendamisega seotud eeldatavad kulud riigieelarvele

Eelnõu rakendamisega ei kaasne tulu ega kulu riigieelarvele.

8. Rakendusaktid

Eelnõukohase seaduse jõustumisel tuleb muuta (kavandid seletuskirja lisas):

1. Vabariigi Valitsuse 09.12.2022. a määrust nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“;
2. majandus- ja infotehnoloogiaministri 17.08.2023. a määrust nr 53 „Küberintsidentide registri põhimäärus“;
3. justiits- ja digiministri 05.03.2026. a määrust nr 7 „Küberintsidendist teavitamisel esitatavad andmed ja teavitamise kord”.

9. Seaduse jõustumine

Käesolev seadus jõustub üldises korras.

Algatab riigikaitsekomisjon 04.05.2026.

(allkirjastatud digitaalselt)
Kalev Stoicescu
Riigikaitsekomisjoni esimees