Märkuste tabel

	Märkus	Märkusega arvestamine
	Kulutuuriministeerium kiri 02.07.2026 nr 1-12/650-2	
1.	2022. a arvati Vabariigi Valitsuse 09.12.2022 määruse nr 121 "Võrgu- ja infosüsteemide küberturvalisuse nõuded" kehtestamisel Eesti infoturbestandardi auditeerimise kohustuse erandite hulka muuseumid ja rahvaraamatukogud kui asutused, kelle IKT korralduslikud vahendid on oluliselt piiratumad tulenevalt IKT vahendite väiksemast olulisusest asutuse avalike ülesannete täitmisel. 2025. a muudatusega laiendati Eesti infoturbestandardi rakendamise erandit alla 50 töötajaga riigimuuseumide vabastamisega infoturbestandardi täies ulatuses järgimisest, kuna nimetatud asutustel ei ole üldjuhul suure mõjuga võrgu- ja infosüsteeme, sealhulgas andmekogusid, ja nad ei halda neid. Kultuuriministeerium teeb ettepaneku täiendada Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 3 lg 2^1 punkti 3 ning vabastada § 3 lõigete 1 ja 2 kohaldamisest peale vähem kui 50 töötajaga riigimuuseumide ka Kultuuriministeeriumi hallatavad väikesed riigiasutused Eesti Lastekirjanduse Keskus ja Võru Instituut. Eesti Lastekirjanduse Keskus kogub ja säilitab lastekirjandusega seotud trükiseid ja muud loomingut kui kultuuripärandit, koordineerib lastekirjanduse uurijate tegevust, korraldab huvitegevust,	**Arvestatud**

	teabepäevi, näitusi ja teisi kultuurisündmusi[1]. Võru Instituut kogub, säilitab, uurib ja vahendab ajaloolise Võrumaaga ehk Vana-Võromaaga seotud kultuuriväärtusliku materjali[2] ning enam kui pool instituudi personalist töötab muuseumiosakonnas ja instituudi neljas muuseumis[3]. Kummagi asutuse põhiülesannete hulka ei kuulu riiklike andmekogude pidamine ega suures mahus digitaalsete andmete töötlemine. Kultuuriministeeriumi hinnangul ei ole Eesti infoturbestandardi täies mahus rakendamine Eesti Lastekirjanduse Keskuse ja Võru Instituudi põhiülesannete, organisatsiooni suuruse, ressursside ega riskitaseme tõttu otstarbekas. Kultuuriministeeriumi arvates piisab neis asutustes töödeldava teabe turvalisuse tagamiseks esmaste turvameetmete rakendamisest.	
Regionaal- ja Põllumajandusministeerium 14.07.2026 nr 1.4-2/1566-1		
1.	Eelnõu seletuskirja IV osa „Määruse mõjud“ leheküljel 22 on märgitud: „Eelnõu muudatustega kaasneb mõju eelkõige riigi julgeolekule ja välissuhetele, samuti majandusele ning riigiasutuste ja kohaliku omavalitsuse korraldusele.“. Mõju kohaliku omavalitsuse korraldusele eelnõu seletuskirjas ei avata, vaid viidatakse küberturvalisuse seaduse seletuskirjale. Meie hinnangul tuleks siiski välja tuua eelnõu seletuskirjas detailsem mõju kohalikule omavalitsusele.	**Antud selgitus** Eelnõuga muudetakse nelja Vabariigi Valitsuse määrust, millest ainult ühe määruse muudatus vähesel määral mõjutav kohalikke omavalitsusi. Tegemist on muudatused, mis on seotud Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ lisa ehk esmaste turvameetmete muudatustega. Muudes eelnõuga tehtavates muudatuse on ka muudetuid sätteid, mis on seotud mh ka kohalike omavalitsustega, kuid need muudatused on tehnilised, st tegemist ei ole mingi uue nõude tekitamisega, vaid näiteks olemasoleva sätte viite parandamisega (vt eelviidatud määruse nr 121 § 2 punkti 3 muudatust kui ka

[1] Põhimäärus: Eesti Lastekirjanduse Keskuse põhimäärus-Riigi Teataja
[2] Põhimäärus: Võru Instituudi põhimäärus-Riigi Teataja
[3] Võru Instituudi muuseumiosakonna põhimäärus: Võru Instituudi muuseumiosakonna põhimäärus)

		Vabariigi Valitsuse 3. jaanuari 2024. a määruses nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel" tehtavaid muudatusi).
Eesti Infotehnoloogia ja Telekommunikatsiooni Liit 02.07.2026 nr 6.1-2/48-2		
1.	Avaldame ITL-ina toetust eelnõu muudatustele (§ 2 punktid 4 ja 5), millega leevendatakse teenuseosutajatele kehtivaid nõudeid selliselt, et ettenähtud standardeid tuleb rakendada vähemalt selle teenuse, tegevusala või valdkonna puhul, mida pakkuv või milles tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. Tegemist on olulise muudatusega, mis pakub oodatud leevenduse NIS2 direktiivi ülevõtmisega organisatsioonipõhisele lähenemisele üleminekuga kaasnenud fookuse hajumisele ja lisanduvale koormusele. Toetame, et standardeid kui kõige mahukamat küberturvalisuse seaduse alusel kehtestatud kohustust tuleb rakendada ainult küberturvalisuse seaduses loetletud tegevusaladega seotud süsteemidele, mitte kogu ettevõtte tegevustele.	**Võetud teadmiseks**
2.	Teeme ettepaneku lihtsustada eelnõu § 2 punktiga 9 määrusesse „Võrgu- ja infosüsteemide küberturvalisuse nõuded" lisatava § 5 lg 1^1 sõnastust järgmiselt: „Riskianalüüs peab sisaldama vähemalt süsteemi turvalisust ja toimepidevust mõjutavate riskide loetelu ning selles tuleb kindlaks määrata riskide realiseerumise tagajärgede raskusaste ja kirjeldada riskijuhtimismeetmeid." ITL-i ettepanek on jätta sättest välja „küberintsidente põhjustavate", sest see on ebavajalik ja segadust tekitav täiendus. Süsteemi turvalisust ja toimepidevust mõjutavate riskide loetelu ütleb kõik, sest ühe või teise riski realiseerumine võibki põhjustada küberintsidenti.	**Arvestatud**

	Eesti Linnade ja Valdade Liit 02.07.2026 kiri nr 2-3/150-2	
1.	Eelnõu paragrahvi 2 punktiga 2 soovitakse täiendada määruse nr 121 "Võrgu- ja infosüsteemide küberturvalisuse nõuded" § 2 punktidega 1^1 ja 1^2, lisades vastavalt terminid „andmekogu vastutav töötleja“ ja „andmekogu volitatud töötleja“ ning nende tähendused. Seletuskirja kohaselt on muudatuse eesmärk tagada õigusselgus, kuivõrd praktikas on tekkinud küsimusi määruse nr 121 § 4 lõike 4 punkti 2 tõlgendamisel (näiteks seoses omavalitsuste ning nende hallatavate asutustega), st millist vastutavat töötlejat ja volitatud töötlejat on selles sättes silmas peetud. Meie hinnangul ei taga kavandatud muudatus nimetatud eesmärki. Viide AvTS-is kasutatavatele mõistetele ei loo õigusselgust, kuna ka AvTS-is ei ole "andmekogu vastutav töötleja" ja "andmekogu volitatud töötleja" mõisted piisavalt üheselt mõistetavad olukordades, kus andmekogu kasutatakse mitme asutuse ülesannete täitmiseks. Kuna vastavad mõisted on ebaselged, siis ei lahenda kavandatav muudatus jätkuvalt küsimust, kas kohalike omavalitsuste hallatavad asutused on määruse nr 121 § 4 lõike 4 punkti 2 alusel infoturbe auditi kohuslased või mitte. Toome konkreetse näite dokumendiregistri näol. AvTS § 11 lõike 1 alusel on kohaliku omavalitsuse asutusel kohustus pidada andmekoguna dokumendiregistrit. Näiteks Tartu linnavalitsuse ametiasutused ning hallatavad asutused kasutavad kõik üht ja sama dokumendiregistrit.	**Selgitame** Seletuskirjas on vastava muudatuse selgituses viidatud küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine) 739 SE selgitustele[4] küberturvalisuse seaduse § 3 lõike 4 punkti 1 kohta, mis selgitavad isikuandmete vastutava ja volitatud töötlejate olemust avaliku teabe seaduse kui ka isikuandmete kaitse valdkonnas kasutatavate terminite tähenduses. Neid selgitusi ei korratud seletuskirjas ega siinses selgituses. Selgitame, et avaliku teabe seadus ei erista kaas-vastutavaid töötlejaid – nii nagu seda teeb isikuandmete kaitse valdkonna õigusaktid. Seetõttu ei ole kirjeldatud teema lahendatav Vabariigi Valitsuse 9. detsembri 2022. a määrusesse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ mõistete tekitamist, mis erinevad selle määruse aluseks oleva seaduse termineid – vt küberturvalisuse seaduse § 3 lõike 4 punkti 1. Lisaks selgitame, et avaliku teabe seaduse kohaste andmekogude puhul on vajalik, et see on asutatud (ennekõike) seaduse alusel (vt avaliku teabe seaduse § 43^1 lõike 1 sõnastust[5]), kuid dokumendiregistrid ei ole käesoleval hetkel asutatud seaduse alusel.

[4] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine

[5] Sõnastuse sisu (vt allajoonitud osa). Andmekogu on riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks.

	Andmekogu vastutav töötleja on AvTS § 43^4 lõikes 1 defineeritud kui „riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.“ Sama paragrahvi lõike 2 kohaselt võib andmekogu vastutav töötleja „volitada andmete töötlemise ja andmekogu majutamise teisele riigi- või kohaliku omavalitsuse asutusele, avalik-õiguslikule juriidilisele isikule või hanke- või halduslepingu alusel eraõiguslikule isikule vastutava töötleja poolt ettenähtud ulatuses“. Antud juhul on selge, et Tartu Linnavalitsus kui ametiasutus on dokumendiregistri puhul andmekogu vastutav töötleja, sest vastutab andmekogu arendamise eest ning koordineerib keskselt, et hallatavad asutused linnas üht ja sama dokumendiregistrit peaks. Samas jääb ebaselgeks hallatavate asutuste roll - kas neid tuleb käsitleda vastutavate või kaasvastutavate töötlejatena, kuivõrd nad korraldavad dokumendiregistris oma teenuste ja andmete haldamist, või hoopis volitatud töötlejatena, sest Tartu Linnavalitsus on neile andnud dokumendiregistri kasutusse oma asutuse andmete töötlemiseks. Sellest tulenevalt ei pruugi pelgalt AvTS mõistetele viitamine anda soovitud õigusselgust auditikohustuslaste ringi määratlemisel. Kui eelnõu tegelik eesmärk on vähendada halduskoormust ning vältida olukorda, kus ühise infosüsteemi iga kasutaja muutub eraldi auditikohustuslaseks, tuleks see regulatsioonis sõnaselgelt välja öelda. Üldjuhul käsitletakse volitatud töötlejana pigem välist teenuseosutajat, kes dokumendiregistrile haldus- ja arendusteenust pakub. Kui kohaliku omavalitsuse hallatavad asutused kasutavad ühist dokumendihaldussüsteemi samamoodi nagu linna- või vallavalitsus	

	ning täidavad selles oma ülesandeid, on põhjendatud käsitleda nende rolli sarnaselt sellele, nagu on kavandatud riigi uue dokumendihalduse infosüsteemi DORIS puhul, kus süsteemi kasutavad asutused on määratletud kaasvastutavate töötlejatena (Dokumendihalduse riikliku infosüsteemi kaasvastutavad töötlejad on Riigi Tugiteenuste Keskus ja infosüsteemi kasutavad asutused ning volitatud töötlejad on Registrite ja Infosüsteemide Keskus ning Siseministeeriumi infotehnoloogia- ja arenduskeskus, AvTS ja teiste seaduste muutmise seadus, eelnõu 30.04.2026). Analoogia alusel tuleks ka kohaliku omavalitsuse dokumendiregistrit kasutavaid hallatavaid asutusi käsitleda kaasvastutavate töötlejatena. Selline tõlgendus tähendab aga, et kohalike omavalitsuste hallatavad asutused on hetkel määruse nr 121 § 4 lõike 4 punkti 2 alusel jätkuvalt infoturbe auditi kohuslased (kuna on andmekogu kaasvastutavad töötlejad). Seega ei ole eelnõu eesmärk auditiga kaasnevat töökoormust vähendada õnnestunud. Eeltoodust tulenevalt ei aita eelnõus kavandatud muudatus lisada määrusesse "andmekogu vastutava töötleja" ja "andmekogu volitatud töötleja" mõisted viitega AvTS-ile kaasa õigusselguse saavutamisele ei mõistete sisustamisel ega infoturbe auditi kohuslaste adressaatide määratlemisel. Kui eesmärk on tagada õigusselgus, siis tuleb vältida regulatsiooni sidumist mõistetega, mis tekitavad tõlgendamisruumi ning ei võimalda üheselt määratleda, millised isikud või asutused on infoturbe auditi kohuslased. Palume tõstatatud probleemi valguses eelnõu üle vaadata ja leida lahendused kohalikule omavalitsusele. Näiteks võib mõelda lahendusele, kus täpsustatakse, et infoturbe auditit ei pea eraldi läbi viima kohaliku omavalitsuse allasutus, kes kasutab teenuste ja andmete haldamiseks omavalitsuse ametiasutuse poolt pakutavat andmekogu ning ei teosta selle arendamist ega tehnilist haldamist või juhul kui mitu kohaliku omavalitsuse asutust kasutavad ühist	

	andmekogu, mille suhtes on infoturbe audit läbi viidud andmekogu vähemalt ühe (kaas)vastutava töötleja tasandil (olukorras, kus kõik kasutavad asutused on kaasvastutavad töötlejad), ei kohaldata sama andmekogu teistele (kaas)vastutavatele asutustele eraldi auditikohustust.	
Eesti Perearstide Selts 02.07.2026 kiri		
1.	Eesti Perearstide Selts on jätkuvalt seisukohal, et infoturve on perearstide töös oluline ning avaldame veelkord heameelt, et ministeerium on võtnud arvesse meie varasemat tagasisidet ning muutnud „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ määruse muudatuse kaudu perearstide suhtes kehtivad nõuded oluliselt proportsionaalsemaks. Oleme veendunud, et lihtsamad, organisatsiooni suurust arvestavad ning jõukohasemad meetmed aitavad kaasa perearstide infoturbe taseme tõstmise eesmärgi saavutamisele, kuivõrd perearstid tulevad arusaadavamate ja hoomatavamate nõuete rakendamisega paremini toime.	**Võetud teadmiseks**
2.	Seekordses tagasisides keskendume ettepanekutele, mida määruse nr 121 lisana kehtestatud dokumendis „Esmased turvameetmed“ tuleks meie hinnangul täiendavalt muuta. Teeme ettepaneku lisada preambuli viimasesse alapunkti sõna „proportsionaalsed“ ning sõnastada see järgmiselt „Teenuseosutaja ei pea käesolevas lisas sätestatud meedet rakendama, kui meede ei ole asjakohane, proportsionaalne või rakendatav ning kui ta on rakendamata jätmisega kaasnevad riskid teadvustanud.“ Kuigi proportsionaalsuse nõue tuleneb üldpõhimõttena küberturvalisuse seadusest, aitab selle otsene kajastamine ka käesolevas lisas tagada nõuete ühetaolisema tõlgendamise ning rakendamise ja vähendada perearstide seas tekkinud ebakindlust selles, kas meetmete	**Mittearvestatud** Sõna „proportsionaalne“ on hõlmatud juba küberturvalisuse seaduse § 7 lõike 1 sissejuhatavas lauses kui ka sama paragrahvi lõike 2 punktis 4 ning need sätted kohalduvad ka esmaste turvameetmete suhtes. Seetõttu tolles lisas seda sõna ei korrata.

	rakendamisel saab proportsionaalsuse põhimõttest lähtuda. Mõni meede võib olla küll asjakohane ja tehniliselt rakendatav, kuid selle rakendamise kulu, halduskoormus või nõutav kompetents võib olla väikese teenuseosutaja jaoks ebamõistlikult suur võrreldes maandatava riskiga. Sellistes olukordades on oluline, et teenuseosutaja mõistaks, et tal on võimalik lähtuda mitte üksnes meetme asjakohasusest ja rakendatavusest, vaid ka selle proportsionaalsusest.	
3.	Teeme ka ettepaneku vaadata esmaste turvameetmete sõnastused tervikuna üle selliselt, et need kirjeldaksid eelkõige teenuseosutaja juhtimis- ja korralduslikku vastutust ja tegevust, mitte tehniliste tegevuste vahetut teostamist. Väikestes perearstikeskustes osutatakse valdav osa IT-teenuseid väliste professionaalsete teenusepakkujate kaudu. Sellises mudelis on realistlik ja põhjendatud nõuda, et perearstikeskus näiteks teaks ja otsustaks, kellel on ligipääs infosüsteemidele, kes tellib uue kasutaja loomise, kes sulgeb lahkunud töötaja konto, kelle poole pöörduda logide või taastamise küsimuses ning kuidas käitutakse katkestuse või intsidendi korral. Samas ei ole realistlik eeldada, et perearstikeskus ise teostaks või kontrolliks detailselt kõiki tehnilisi tegevusi, mille tegemiseks puudub tal vajalik kompetents ja ligipääs. Esmaste meetmete sõnastuses võiks seetõttu selgemalt eristada tehnilist teostust ja perearstikeskuse vastutust. Väikese keskuse puhul ei peaks näiteks nõude sisuks olema kõigi logide ja varukoopiate iseseisev haldamine, vaid arusaam sellest, kelle ülesandeks on korraldada oluliste teenuste ligipääsude haldamine, logimine, varundamine ja taastamine ning – iseäranis kriitiliste süsteemide puhul – otsustamine, kas süsteemides rakendatavad standardlahendused on organisatsiooni vajadusi ja riske arvestades piisavad.	**Mittearvestatud ja selgitame** Esmased turvameetmed on need universaalsed baasnõuded, millede rakendamise täpsemat korraldust ja ülesannete jaotust ei ole ette nähtud. Pakutud ettepanek muudaks põhimõtet, mis osas vastutab teenuseosutaja, kuna tekitaks rollid (või vastutused) teenuseosutajale kui ka tema välisele partnerile. See lähenemine ei ühtiks ka küberturvalisuse seaduse § 7 lõikes 3 ette nähtud nõudega: *Kui teenuseosutaja volitab süsteemi haldamise teisele isikule või majutab süsteemi teise isiku juures, vastutab teenuseosutaja selle eest, et teine isik tagab süsteemi turvameetmete rakendamise.*

4.	Lisaks palume jätkuvalt analüüsida tervishoiusektorit tervikuna ning kaaluda sektoripõhise regulatsiooni loomist, mis võimaldaks nõudeid kehtestada sihitumalt ja vajaduspõhisemalt. Tervishoiusektoris sõltub üksiku teenuseosutaja infoturbe tase olulisel määral ka kesksetest infosüsteemidest, tarkvaratootjatest, pilveteenustest ning riiklikest taristutest. Seetõttu ei pruugi üksikutele perearstikeskustele suunatud üldised kohustused viia alati kõige tõhusama riskide maandamiseni. Sektoripõhine regulatsioon võimaldaks suunata täiendavad nõuded just neile osapooltele, kellel on tegelik võimekus ja mõju infoturbe taseme kujundamisel. Kokkuvõttes oleme seisukohal, et perearstikeskus peab tagama infoturbe teadliku korraldamise, kuid nõuded peaksid rohkem keskenduma sellele, mida väike tervishoiuteenuse osutaja saab tegelikult juhtida ja mõjutada.	**Selgitame** Praeguses etapis ei ole planeeritud koostada tervishoiusektorile tervikuna mõeldud regulatsiooni. See vajab täiendavat analüüsi, mida käesoleva eelnõu raames pole võimalik teha. Seda eriti juhul, kui ootus on tekitada nõuded ka üksustele, kes ei ole hetkel küberturvalisuse seaduse kohaldamisalas.

Haridus- ja Teadusministeerium, Rahandusministeerium, Siseministeerium ning Sotsiaalministeerium kooskõlastasid märkusteta. Riigikogu Kantseleil, Andmekaitse Inspektsioonil, Finantsinspektsioonil, Registrite ja Infosüsteemide Keskusel ning Riigi Info- ja Kommunikatsioonitehnoloogia Keskusel tähelepanekud puudusid.