09.09.2025

Vabariigi Valitsuse määruse „Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine“ eelnõu SELETUSKIRI

1. Sissejuhatus

1.1. Sisukokkuvõte

Määrusega muudetakse mikro- ja väikeettevõtjate ning kohaliku omavalitsuse hallatavate asutuste küberturvalisuse tagamise nõudeid. Nimetatud ettevõtjatele ja asutustele nähakse ette vaid esmaste turvameetmete täitmise kohustus senise Eesti infoturbestandardi või rahvusvahelise standardi ISO/IEC 27001 järgimise kohustuse asemel. Samuti kaotatakse riigikoolide Eesti infoturbestandardi täitmisel auditi tellimise kohustus, võrdsustades riigikoolid kohalike omavalitsuse üksuste hallatavate üldhariduskoolidega, millel see kohustus puudub. Eelnõukohase määruse jõustumisel väheneb mikro- ja väikeettevõtjate halduskoormus ning osa kohalike omavalitsuste hallatavate asutuste ja riigimuuseumite töökoormus.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talitus (e-post kybertalitus@justdigi.ee) Riigi Infosüsteemi Ameti ettepaneku alusel. Eelnõu on keeleliselt toimetanud Justiits- ja Digiministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Merike Koppel (e-post merike.koppel@justdigi.ee).

1.3. Märkused

Eelnõu on seotud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga.[1]

Eelnõukohase määrusega muudetakse Vabariigi Valitsuse 9. detsembri 2022. a määrust nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (edaspidi *määrus nr 121*) (RT I, 19.06.2024, 12).

Eelnõuga kavandatakse vähendada mikro- ja väikeettevõtjate halduskoormust ning osa kohalike omavalitsuste hallatavate asutuste ja riigimuuseumite töökoormust. Eelnõu on seotud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga.[2]
Nimetatud eelnõuga kavandatakse üle võtta Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiiv (EL) 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) (ELT L 333, 27.12.2022, lk 80–152) (edaspidi ka *küberturvalisuse 2. direktiiv*). Kuna küberturvalisuse 2. direktiivi ülevõtmisega suureneb küberturvalisuse seaduse subjektide arv, siis soovitakse sellest tulenevat halduskoormuse kasvu kõnesoleva eelnõukohase määrusega tasakaalustada.

[1] Eelnõude infosüsteemi toimik 24-1266.
[2] Eelnõude infosüsteemi toimik 24-1266.

2. Määruse eesmärk

Määruse eesmärk on esiteks vähendada mikro- ja väikeettevõtjatest ning kohaliku omavalitsuse hallatavatest asutustest küberturvalisuse seaduse subjektide haldus- või töökoormust nende võrgu- ja infosüsteemide küberturvalisuse tagamisel. Teiseks ühtlustatakse riigi- ja kohaliku omavalitsuse ülalpeetavatele põhikoolidele ja gümnaasiumitele esitatavaid nõudeid.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kahest paragrahvist.

Paragrahviga 1 muudetakse Vabariigi Valitsuse 9. detsembri 2022. a määrust nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“. Paragrahv koosneb kümnest punktist.

Määruse nr 121 § 1 senine tekst loetakse **lõikeks 1** ja paragrahvi täiendatakse uue **lõikega 2**. Täiendusega lisatakse õigusselguse huvides viited Euroopa Liidu õigusaktidele, millega kehtestatakse erandid küberturvalisuse 2. direktiivist. Lisatava lõike 2 järgi ei pea nimetatud ettevõtjad kohaldama loetletud õigusaktidega reguleeritavates tegevusvaldkondades küberturvalisuse seaduse ja selle alusel antud õigusaktide nõudeid, sealhulgas järgmisi määrusest nr 121 tulenevaid nõudeid:
a) finantssektori küberturvalisuse ja riskijuhtimise nõuded, mis tulenevad Euroopa Parlamendi ja nõukogu määrusest (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1–79) (edaspidi *DORA määrus*);
b) tsiviillennunduse sektori küberturvalisuse nõuded, mis tulenevad Euroopa Parlamendi ja nõukogu määrusest (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 09.04.2008, lk 72–84) ning Euroopa Parlamendi ja nõukogu määrusest (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 2111/2005, (EÜ) nr 1008/2008, (EL) nr 996/2010, (EL) nr 376/2014 ja Euroopa Parlamendi ja nõukogu direktiive 2014/30/EL ning 2014/53/EL ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrused (EÜ) nr 552/2004 ja (EÜ) nr 216/2008 ning nõukogu määrus (EMÜ) nr 3922/91 (ELT L 212, 22.08.2018, lk 1–122).

Tänu muudatusele on asjaosalistele paremini arusaadav, et näiteks elutähtsa teenuse osutajast krediidiasutus, kes rakendab DORA määruse nõudeid, ei pea samal ajal järgima küberturvalisuse seaduse alusel elutähtsa teenuse osutajale kehtestatud nõudeid. Kui krediidiasutusel on muid tegevusvaldkondi, kus DORA määrus ei kohaldu, kuid ta on teenuse osutaja küberturvalisuse seaduse tähenduses, siis neis valdkondades kehtib küberturvalisuse seaduse ja selle alusel antud õigusaktide järgimise kohustus.[3]

Määruse nr 121 § 2 täiendatakse **punktiga 3**. Täiendusega lisatakse Vabariigi Valitsuse määruse tasemel uus termin *pilvteenus* kui pilvandmetöötlusteenus või selliste andmetöötlusressursside kogumile juurdepääsu võimaldav teenus, mida saab paindlikult jagada

[3] Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta. Punkt 7, (EUR-Lex - 52023XC0918(01) - EN - EUR-Lex) (19.06.2025).

ning laiendada võrgu- ja infosüsteemi muutmata ning mida pakub kohaliku omavalitsuse üksus või küberturvalisuse seaduse § 3 lõike 4 punktides 12 ja 13 nimetatud asutus või isik.

Termini kasutuselevõtmise eesmärk on koondada määrusesse ühe termini alla nii erasektori kui ka avaliku sektori pakutavad avalikud pilved (inglise keeles *public cloud*). Erasektori pakutav pilv on sätestatud küberturvalisuse seaduse § 2 punktis 7 kui pilvandmetöötlusteenus, mis on infoühiskonna teenus, mis võimaldab juurdepääsu andmetöötlusressursside kogumile, mis on paindlikult jagatav ning laiendatav süsteemi ennast muutmata. Samas ei saa avaliku sektori pakutavat pilve käsitada infoühiskonna teenusena, see tähendab avalik sektor ei paku avalikku pilve majandus- või kutsetegevuse raames[4]. Seega luuakse kahe erineva pakkuja andmetöötlusressursside kogumile juurdepääsu võimaldava teenuse tähistamiseks uus koondtermin.

„Pilvteenust“ ei kasutata Vabariigi Valitsuse määrustes esimest korda. Nimelt kasutatakse Vabariigi Valitsuse 3. jaanuari 2024. a määruse nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ § 2 lõikes 1 lühendterminit „pilvteenus“, mis hõlmab samuti eelnõuga samas ulatuses riigi- ja erasektori pakutavaid avalikke pilvi.[5]

Määruse nr 121 § 3 lõike 2 punkti 1 muudetakse, lisades määrusesse viite Eesti standardile. Eesti standard on toote nõuetele vastavuse seaduse § 40 lõike 1 kohaselt Eesti standardiorganisatsiooni vastuvõetud standard. Eesti standardi tähtlühend on „EVS“. Sama paragrahvi lõike 4 punkti 1 kohaselt võib Eesti standard olla ülevõetud rahvusvahelise või Euroopa standardiorganisatsiooni standard. ISO/IEC 27001 „Information security, cybersecurity and privacy protection — Information security management systems — Requirements“ on Rahvusvahelise Standardiorganisatsiooni koostatud standard, mille Mittetulundusühing Eesti Standardimis- ja Akrediteerimiskeskus on üle võtnud Eesti standardina EVS-EN ISO/IEC 27001 – „Infoturve, küberturve ja privaatsuskaitse. Infoturbe halduse süsteemid. Nõuded“. Eesti standardile viitamisega täpsustatakse, et teenuseosutajal on võimalik küberturvalisuse tagamisel lähtuda ka Eesti standardist, kui see on üle võetud ning vastab rahvusvahelisele standardile ISO/IEC 27001.

Määruse nr 121 § 3 täiendatakse uue **lõikega 2[1]**, millega nähakse ette erandid rahvusvahelise standardi ISO/IEC 27001 või Eesti standardi EVS-EN ISO/IEC 27001 (edaspidi koos *standard ISO/IEC 27001*) või Eesti infoturbestandardi järgimise kohustusest.

Punktiga 1 sätestatakse, et Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid ei pea vahetult kohaldama mikro- ja väikeettevõtjad, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastane bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades väikeettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L 124, 20.05.2003, lk 36–41). Mõlemad tingimused (nii töötajate arv kui ka finantsnäitajad) peavad olema täidetud.

[4] Infoühiskonna teenuse seaduse § 2 p 1: „*infoühiskonna teenus* – teenus, mida osutatakse majandus- või kutsetegevuse raames teenuse kasutaja otsesel taotlusel ja mille puhul andmeid töödeldakse, säilitatakse ja edastatakse digitaalkujul andmete töötlemiseks ja säilitamiseks mõeldud elektrooniliste vahendite abil, kusjuures osapooled ei viibi üheaegselt samas kohas. Infoühiskonna teenus peab olema täielikult üle kantud, edastatud ja vastu võetud elektrooniliste sidevahendite abil. Infoühiskonna teenus ei ole faksi ega telefonikõne abil edastatud teenus ega televisiooni- või raadioteenus;“.

[5] „(1) Teabepidaja, kes soovib avaliku teabe töötlemiseks kasutusele võtta avaliku sektori osutatava pilvteenuse või pilvandmetöötlusteenuse (edaspidi koos *pilvteenus*), peab hindama muu hulgas:“.

Muudatuses ei mainita vahetult mikroettevõtjaid[6], kuid kuna mikroettevõtjale kehtestatud nõuded mahuvad Euroopa Komisjoni soovituse piiridesse, siis tuleb lugeda eelnõu kohaselt ka mikroettevõtja vabastatuks Eesti infoturbestandardi või standardi ISO/IEC 27001 kohaldamisest oma võrgu- ja infosüsteemis küberturvalisuse tagamisel. Küll aga ei ole mikro- ja väikeettevõtja vabastatud eelnõuga määrusesse lisatavas §-s 5^1 sätestatavast turbevaldkondades esmaste turvameetmete järgimise kohustusest. Ettevõtjate suuruse arvestamisel tuleb järgida väikeste ja keskmise suurusega ettevõtjate määratlust käsitlevat teatmikku, mis sisaldab üldiseid suuniseid ettevõtjatele ja teistele sidusrühmadele, millest nad saavad suuruse kindlakstegemisel juhinduda.[7]

Ettevõtja, millel on 40 või vähem töötajat, ning mille aastakäive ja aastabilansi kogumaht jäävad alla 10 miljoni euro, on väikeettevõtja. Kui ettevõtjal on 40 töötajat, kuid bilansimaht ja aastakäive on mõlemad eraldi 10 miljonit eurot, siis on tegemist juba keskmise suurusega ettevõtjaga. Kui aga töötajaid on 40 ja bilansimaht on alla 10 miljoni euro, on 20miljonilise käibe korral tegemist siiski väikeettevõtjaga. Sama kehtib juhul kui 40 töötajaga ettevõtja bilansimaht ületab nõutut, kuid aastakäive jääb alla nõutava taseme. Kui töötajaid on keskmiselt 50 või enam, siis sõltumata kas bilansimaht või aastakäive jääb alla 10 miljoni euro, on tegemist keskmise suurusega ettevõtjaga. [8]

Punktiga 2 nähakse ette, et sarnaselt mikro- ja väikeettevõtjatele ei ole vajadust täies ulatuses järgida Eesti infoturbestandardis või standardiga ISO/IEC 27001 sätestatud turvameetmeid valla või linna ametiasutuste hallatavatel asutustel ja osavalla või linnaosa ametiasutuse hallatavatel asutustel, millel on kalendriaasta jooksul keskmiselt alla 50 töötaja. Erand ei laiene vallale või linnale kuuluvale üldhariduskoolile. Üldhariduskoolide puhul võeti arvesse nende suuremat seotust isikuandmete, sealhulgas alaealiste isikuandmete töötlemisega. Eesti infoturbestandardi või standardi ISO/IEC 27001 järgimise kohustus on ka riigile kuuluvatel üldhariduskoolidel.

Samuti tuleb märkida, et erand ei kehti kohaliku omavalitsuse ametiasutuste suhtes, kes oma suuruse poolest võiksid eelnõu kohaselt seatud piiridesse mahtuda.

Punktiga 3 sätestatakse, et Eesti infoturbestandardi või standardi ISO/IEC 27001 täies ulatuses järgimise kohustust ei ole ka riigimuuseumitel, kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja. Riigimuuseum on ministeeriumi hallatav riigiasutus. Riigimuuseumile erandi loomisel võeti arvesse, et sarnane erand on loodud ka kohaliku omavalitsuse hallatava asutusena tegutsevale muuseumile.

Punktides 2 ja 3 ettenähtud keskmise töötajate arvu arvutamisel tuleb kasutada sarnast põhimõtet mis ettevõtjate puhul. See tähendab, et töötajate arvu väljendatakse aastastes tööühikutes. Üheks ühikuks loetakse kogu vaatlusaasta jooksul asutuses või selle nimel töötanud isik. Isikute töö, kes ei töötanud terve aasta, osalise tööajaga isiku ja hooajatöötaja töö võetakse arvesse tööühiku murdosadena. Töötajate hulka ei arvata isikuid, kes on praktika või kutseõppelepingu alusel oskusi omandamas. Töötajate hulka ei arvata ka terve aasta rasedus-,

[6] Mikroettevõtja – ettevõtja, mis annab tööd kuni 10 inimesele ning mille käibe (määratud ajavahemikul saadud raha) või bilansi (ettevõtte varade ja kohustuste aruanne) maht ei ületa 2 miljonit eurot (https://eur-lex.europa.eu/ET/legal-content/summary/micro-small-and-medium-sized-enterprises-definition-and-scope.html) (19.05.2025).
[7] VKEde määratlust käsitlev teatmik - Publications Office of the EU (19.06.2025).
[8] Vaata ka Ettevõtluse ja Innovatsiooni Sihtasutuse (end EAS) selgitust lk 7, https://eis.ee/wp-content/uploads/2015/12/VKE_definitsiooni_selgitus_-_EK_mrus_651-2014_alusel_-_2015.pdf (29.08.2025).

sünnitus- või lapsehoolduspuhkusel olnud isikut. Kui isik jäi nimetatud puhkusele aasta sees, siis arvestatakse teda osa aastast töötanud isikuna. Selleks, et üksikud sündmused ei mõjutaks oluliselt asutuste kohustusi, on soovitatav aasta keskmist töötajate arvu vaadata kolme aasta võrdluses. Kui keskmine on 50 või enam tööühikut (töötajat), siis on ettevõtjal või asutusel Eesti infoturbestandardi või standardi ISO/IEC 27001 rakendamise kohustus, kui on 49,99 või vähem tööühikut, siis neil Eesti infoturbestandardi või standardi ISO/IEC 27001 täies ulatuses järgimise kohustust ei ole.

Punktiga 4 nähakse ette, et Eesti infoturbestandardi või standardi ISO/IEC 27001 täies ulatuses järgimise kohustust ei ole kohaliku omavalitsuse üksuste liidul, kellel on kalendriaasta jooksul keskmiselt alla 50 töötaja. Kohaliku omavalitsuse üksuste liitude seaduse kohaselt võib moodustada kolme liiki kohaliku omavalitsuse üksuste liite: maakonna kohaliku omavalitsuse üksuste liit, piirkonna kohaliku omavalitsuse üksuste liit ja üleriigiline kohaliku omavalitsuse üksuste liit. Üleriigilisi liite võib olla vaid üks. Praegu on selleks Eesti Linnade ja Valdade Liit. Erandi tegemisel võeti arvesse, et liidud ei kasuta iseseisvalt suure mõjuga võrgu- ja infosüsteeme ega paku ka oma liikmetele infotehnoloogiateenuseid. Kohaliku omavalitsuse üksuste liitude tegutsemisvorm on mittetulundusühing.

Määruse nr 121 § 4 lõiget 1 muudetakse ja sellesse lisatakse viide määruse § 3 lõikele 1. Muudatuse eesmärk on täpsustada, et Eesti infoturbestandardi tingimuste täitmise auditi peab läbi viima vaid teenuse osutaja, kellel on Eesti infoturbestandardi järgimise kohustus. Määruse § 121 § 3 lõike 2 kohaselt ei pea Eesti infoturbestandardi tingimuste täitmise auditit läbi viima teenuse osutaja, kes rakendab standardi ISO/IEC 27001 ning on esitanud selle vastavussertifikaadi Riigi Infosüsteemi Ametile. Eesti infoturbestandardi tingimuste täitmise auditit ei pea läbi viima ka eelnõuga lisatavas § 3 lõikes 2^1 nimetatud teenuse osutajad (vt ka § 3 lõike 2^1 selgitust).

Määruse nr 121 § 4 täiendatakse uue **lõikega 1^1**. Täienduse kohaselt peab ettevõtja, kes määratakse esimest korda elutähtsa teenuse osutajaks pärast 18. oktoobrit 2024, tegema Eesti infoturbestandardi tingimuste täitmise auditi hädaolukorra seaduse § 38 lõike 1 alusel antud haldusaktis määratud tähtajaks. Hädaolukorra seaduse § 38 lõike 1^3 punkti 3 kohaselt ei või nõuete täitmise tähtaeg olla pikem kui viis aastat. Kuna see tähtaeg on pikem kui määruse nr 121 § 4 lõikes 1 sätestatud kolm aastat, tehakse eelnõukohase määrusega muudatus, mis on kooskõlas 18. oktoobril 2024 jõustunud hädaolukorra seaduse muudatustega.

Säte ei kohaldu avaliku sektori asutusele, kes on elutähtsa teenuse osutaja või saab selleks, sest tal on Eesti infoturbestandardi või standardi ISO/IEC 27001 järgimise kohustus elutähtsa teenuse osutamisest sõltumata.

Määruse nr 121 § 4 lõikes 2 lisatakse lõike 1 viite järele ka viide sama paragrahvi lõikele 1^1, millega sätestatakse esimest korda elutähtsa teenuse osutajaks määratud ettevõtjale tähtaeg, millal tal tuleb viia läbi Eesti infoturbestandardi täitmise audit, kui otsustatakse nimetatud standardi järgimine.

Määruse nr 121 § 4 lõike 4 punkt 1 tunnistatakse kehtetuks, sest mikroettevõtjate kohustust järgida küberturvalisuse tagamiseks täies ulatuses Eesti infoturbestandardeid või standardit ISO/IEC 27001 muudetakse, mistõttu ei ole vaja eraldi märkida ka Eesti infoturbestandardi tingimuste täitmise auditi läbiviimise kohustuse kohaldamist (vt ka § 3 lõike 2^1 selgitust).

Määruse nr 121 § 4 lõiget 4 täiendatakse **punktiga 4,** mille kohaselt ei pea edaspidi Haridus- ja Teadusministeeriumi hallatava asutusena tegutsevad põhikoolid ja gümnaasiumid ehk riigikoolid[9] Eesti infoturbestandardi järgimisel tegema Eesti infoturbestandardi täitmise auditit. See erand ei kehti, kui kool on andmekogu vastutava töötleja või volitatud töötleja avaliku teabe seaduse tähenduses. Muudatusega võrdsustatakse riigikoolid kohalike omavalitsuste ülalpeetavate koolidega, kelle suhtes kehtib vabastus auditi läbiviimisest lähtuvalt määruse 121 § 4 lõike 4 punktist 2. Riigi Infosüsteemi Ameti hinnangul algavad auditi hinnad 10 000 eurost kolmeaastase auditiperioodi kohta. Audit hõlmab eelauditit, põhiauditit, vaheauditit ja järelauditit, seega väheneb koolile kaasnev töökoormus infoturbevaldkonnas auditikohustuse kaotamisega märkimisväärselt. Küll aga ei tohi auditikohustuse puudumist käsitada kui infoturbenõuete täitmise kohustuse puudumist ning järelevalve puudumist. Muudatus puudutab 81 riigikooli.

Määruse nr 121 3. peatüki 1. jagu täiendatakse **§-ga 5[1]**. Uue paragrahviga sätestatakse üheksa turbevaldkonda, milles kõik teenuse osutajad peavad kasutusele võtma esmased turvameetmed.

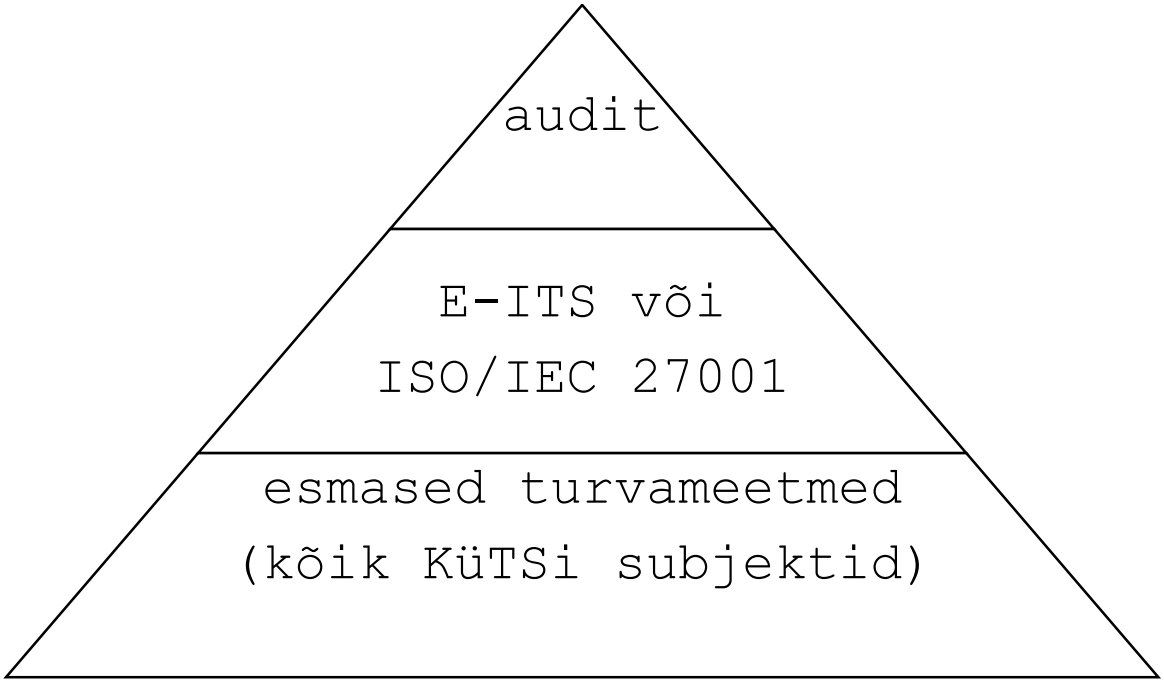
Küberturvalisuse 2. direktiivi artikli 21 lõike 1 kohaselt tagavad liikmesriigid, *et elutähtsad ja olulised üksused võtavad asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, ning et ennetada või minimeerida intsidentide mõju nende teenuste saajatele ja muudele teenustele*. Sellest tulenevalt on Riigi Infosüsteemi Amet teinud ettepaneku kehtestada esmased turvameetmed, mis on jaotatud üheksa valdkonna vahel. Esmased turvameetmed kehtivad kõigile küberturvalisuse seaduse subjektidele. Subjektid, kes järgivad Eesti infoturbestandardit või standardit ISO/IEC 27001, peavad ka vaatama, kas nende rakendatavad turvameetmed on kooskõlas määrusesse lisatavate esmaste turvameetmetega. Näiteks kui standardi ISO/IEC 27001 järgimisel ei ole mõne esmase turvameetme rakendamist ette nähtud, siis tuleb selle nõude täitmine eraldi ette näha.

Joonisel 1 on kujutatud esmaste turvameetmete koht teiste küberturvalisuse tagamisega seotud meetmete rakendamise järjekorras. Esmased turvameetmed on nii-öelda baastase, mida peavad rakendama kõik küberturvalisuse seaduse subjektid (teenuse osutajad). Järgmine tase on Eesti infoturbestandardi või standardi ISO/IEC 27001 nõuete rakendamine. Nende vahetu järgimise kohustus puudub mikro- ja väikeettevõtjatel ning eelnõuga määrusesse lisatava § 3 lõike 2[1] punktides 2 ja 3 sätestatud tingimustele vastavatel kohaliku omavalitsuse hallataval asutusel ja riigimuuseumil. Kolmas tase küberturvalisuse nõuete rakendamisel on auditi läbiviimise kohustus. Standardit ISO/EIEC 2700 rakendav teenuse osutaja peab auditi tegema igal juhul, et saada kätte standardi rakendamise kinnituseks vajalik vastavussertifikaat (vt ka määruse nr 121 § 3 lõike 2 punkt 2). Eesti infoturbestandardi tingimuste täitmise auditi läbiviimise kohustusest vabastatud isikud on sätestatud määruse nr 121 § 4 lõikes 4. Nendeks on riigimuuseum, avalik-õigusliku isiku muuseum, valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus ning kohaliku omavalitsuse üksuste ühisamet ja -asutus ning kohaliku omavalitsuse üksuste liit, kui tegemist ei ole andmekogu vastutava töötlejaga või volitatud töötlejaga. Riigimuuseumi ja kohaliku omavalitsuse hallatavate asutuste ning liitude kohta sätestatakse seejuures

[9] Põhikooli ja gümnaasiumiseaduse § 1 lõige 2: „Käesolev seadus reguleerib valla või linna ametiasutuse hallatavate asutustena tegutsevate koolide (edaspidi *munitsipaalkool*) ning Haridus- ja Teadusministeeriumi hallatavate asutustena tegutsevate koolide (edaspidi *riigikool*) tegevust. Munitsipaalkooli pidajaks on vald või linn. Riigikooli pidajaks on riik. Eraõigusliku juriidilise isiku asutusena tegutsevale koolile (edaspidi *erakool*) kohaldatakse käesolevat seadust niivõrd, kuivõrd erakooliseadus ei sätesta teisiti."

eelnõukohase määrusega, et nõue kehtib vaid siis, kui tal on kalendriaasta jooksul keskmiselt 50 või enam töötajat (vt ka eelnõukohase määrusega lisatava § 3 lõike 2^1 punktide 2–4 selgitust).

Joonis 1. Küberturvalisuse meetmete rakendamine



Legend: E-ITS – Eesti Infoturbestandard
ISO/IEC 27001 – rahvusvaheline standard ISO/IEC 27001 ja Eesti standard EVS-EN ISO/IEC 27001
KüTS – küberturvalisuse seadus

Riigi Infosüsteemi Amet aitab kaasa seaduses ja selle alusel antud õigusaktides sätestatud nõuete täitmisele. Kaasaaitamine seisneb subjektide nõustamises, rakendamise toetamiseks soovituslike suuniste, rakendamise ettepanekute ja selgituste avaldamises jne. Sellise teabe saab Riigi Infosüsteemi Amet avaldada asjaomasel veebilehel. Nii näiteks on Riigi Infosüsteemi Amet Eesti infoturbestandardi paremaks ja ühtlasemaks rakendamiseks loonud eraldi veebilehe.[10]

Määruse lisa. Määruse lisas kirjeldatakse turbevaldkondade kaupa üksikasjalikke esmaseid turvameetmeid, mida kõik teenuse osutajad peavad rakendama, et subjekti võrgu- ja infosüsteemidele rakendatud meetmed saaks lugeda piisavaks, et olla küberturvalisuse seaduses sätestatud turvanõuetega kooskõlas. Lisa on seotud eelnõuga määrusesse lisatava § 3 lõikega 2^1, mille kohaselt ei pea osa teenuse osutajatest edaspidi Eesti infoturbestandardi või standardi ISO/IEC 27001 nõudeid täies ulatuses järgima (vt ka eelnõukohase määrusega lisatava § 5^1 selgitust).

Paragrahviga 2 nähakse ette määruse jõustumise aeg, milleks on 1. oktoober 2025 (vt seletuskirja punkti 8).

4. Eelnõu terminoloogia

Eelnõukohase määrusega võetakse Vabariigi Valitsuse määruse tasemel kasutusele termin „pilvteenus“.

[10] https://eits.ria.ee/ (13.05.2025).

Pilvteenus on pilvandmetöötlusteenus või selliste andmetöötlusressursside kogumile juurdepääsu võimaldav teenus, mida saab paindlikult jagada ning laiendada võrgu- ja infosüsteemi muutmata ning mida pakub kohaliku omavalitsuse üksus või küberturvalisuse seaduse § 3 lõike 4 punktides 12 ja 13 nimetatud asutus või isik (vt ka määruse nr 121 § 3 punkti 3 selgitust).

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu ei ole seotud Euroopa Liidu õiguse ülevõtmisega. Määrus vastab Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiivi (EL) 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), artikli 21 lõikele 1 (vt ka lisatava § 5^1 selgitust).

6. Määruse mõjud

Eelnõukohane määrus mõjutab majanduskeskkonda, infotehnoloogia- ja infoühiskonda ning riigivalitsemist.

6.1. Mikro- ja väikeettevõtjatelt ei nõuta Eesti infoturbestandardi või standardi ISO/IEC 27001 täismahus järgimist

Eelnõukohase määruse jõustumisel muudetakse mikro- ja väikeettevõtjate kohustuse ulatust küberturvalisuse turvameetmete rakendamisel ning kaotatakse vahetu kohustus järgida kasutatavates võrgu- ja infosüsteemides Eesti infoturbestandardi või standardi ISO/IEC 27001 nõudeid. Ühtlasi ei nõuta edaspidi väikeettevõtjatelt ka Eesti infoturbestandardi või standardi ISO/IEC 27001 täitmise auditi läbiviimist.

Mõjuvaldkond: halduskoormus (mõju majandusele)

Mõju sihtrühm: küberturvalisuse seaduse subjektidest mikro- ja väikeettevõtjad
Muudatus mõjutab küberturvalisuse seaduse § 3 lõikes 1 nimetatud subjektidest mikro- ja väikeettevõtjate halduskoormust võrgu- ja infosüsteemide turvameetmete rakendamisel. Muudatus mõjutab umbes 200 ettevõtjat.

Avalduv mõju ja mõju olulisus
Eelnõukohase määruse jõustumise järel ei pea mikro- ja väikeettevõtjad enam oma võrgu- ja infosüsteemide turvameetmete rakendamisel järgima täismahus Eesti infoturbestandardit või standardit ISO/IEC 27001 ega viima läbi ka nende täitmise auditit. Selle tulemusel muutub ka ettevõtja kohustus turvameetmete rakendamist või rakendamata jätmist üksikasjalikult fikseerida (näiteks koostada ja rakendada detailset infoturbehalduse süsteemi), sealhulgas tegevustes või vahendite kasutamisel, mida ettevõtja oma väiksusest lähtudes ei pruugi teha või omada. Mikro- ja väikeettevõtjate puhul on arvesse võetud ka asjaolu, et ettevõtjal ei pruugi olla eraldi infoturbe eest vastutavat isikut ning Eesti infoturbestandardi järgimise kohustuse täitmisest tulenevat halduskoormust kannab personal, kellel puuduvad valdkonnateadmised. Samuti ei ole mikro- ja väikeettevõtjal üldjuhul suure mõjuga võrgu- ja infosüsteeme.

Küberturvalisuse 2. direktiivi üle võtva seaduse eelnõu kooskõlastamisel juhtisid ettevõtjad ja ettevõtjate esindusorganisatsioonid tähelepanu auditi nõude proportsionaalsusele ja audiitorite kättesaadavusele. Võttes arvesse eelnõule saadud tagasisidet, on Riigi Infosüsteemi Amet

teinud ettepaneku vabastada lisaks mikroettevõtjatele Eesti infoturbestandardi või standardi ISO/IEC 27001 tingimuste täitmise auditi läbiviimise kohustusest ka väikeettevõtjad.

Justiits- ja Digiministeerium ning Riigi Infosüsteemi Amet kaalusid ka varianti piirduda ülevõtmisel vaid nende küberturvalisuse valdkondade esiletoomisega, milles küberturvalisuse seaduse subjekt peab toiminguid tegema. Riigi Infosüsteemi Ameti ettepanekul jäeti see lahendus kasutamata, kuivõrd vastasel juhul puuduks järelevalve tegemisel selge raamistik, mida kontrollida, ning nõuete detailsus tagab subjektide jaoks konkreetselt sõnastatud nõuded, mida subjekt peab täitma, et tema üldised turvameetmed oleksid korrektselt rakendatud.

Määrusele on turvameetmete rakendamist abistava teabena koostatud esmaste turvameetmete lisa. Lisaks on Riigi Infosüsteemi Amet oma veebilehel avaldanud teabe, mis aitab kaasa üldiste turvameetmete rakendamisele.[11] Riigi Infosüsteemi Amet uuendab ja ajakohastab seda teavet pidevalt.

Järeldus mõju olulisuse kohta
Muudatuse tulemusel väheneb küberturvalisuse seaduse subjektidest mikro- ja väikeettevõtjate halduskoormus. Riigi Infosüsteemi Ameti hinnangul kulub üldiste turvameetmete hindamiseks 1–2 tundi ühe hindamiskorra kohta. Samuti väheneb väikeettevõtjate halduskoormus täismahus Eesti infoturbestandardi täitmise auditi tegemise võrra, sama nõude kaotamisega väheneb ka ettevõtjate võimalik kulu auditi tellimiseks. Lähtudes eeltoodust on nimetatud ettevõtjate ajaline kokkuhoid halduskoormuse vähendamise kaudu märkimisväärne ning mõju ettevõtjate tegevusele märgatav.

6.2. Vähem kui 50 töötajaga kohalike omavalitsuste hallatavate asutuste ja riigimuuseumite vabastamine Eesti infoturbestandardi või standardi ISO/IEC 27001 täismahus järgimise kohustusest

Eelnõukohase määrusega asendatakse vähem kui 50 töötajaga kohaliku omavalitsuse hallatava asutuse (välja arvatud üldhariduskool) ja riigimuuseumi kohustus järgida oma võrgu- ja infosüsteemide turvameetmete rakendamisel täismahus Eesti infoturbestandardit või standardit ISO/IEC 27001 kohustusega rakendada esmaseid turvameetmeid.

Mõjuvaldkond: mõju kohaliku omavalitsuse korraldusele ja finantseerimisele ning keskvalitsuse korraldusele (mõju riigivalitsemisele)

Mõju sihtrühm: küberturvalisuse seaduse subjektidest väikesed (alla 50 töötajaga) valla või linna ametiasutuse hallatavad asutused ning osavalla või linnaosa ametiasutuse hallatavad asutused ning riigimuuseumid. Muudatus mõjutab umbes 1000 asutust, sealhulgas lasteaiad, kultuuri- ja huvikeskused, muuseumid, raamatukogud, sotsiaalkeskused, vabaajaasutused, rahvamajad, spordikeskused.

Avalduv mõju ja mõju olulisus
Eelnõukohase määruse jõustumise järel ei pea enam vähem kui 50 töötajaga kohaliku omavalitsuse hallatav asutus või riigimuuseum oma võrgu- ja infosüsteemide turvameetmete rakendamisel järgima täielikult Eesti infoturbestandardit või standardit ISO/IEC 27001. Selle tulemusel muutub ka nimetatud asutuste kohustus turvameetmete rakendamist või rakendamata jätmist üksikasjalikult fikseerida (näiteks koostada ja rakendada detailset infoturbehalduse

[11] https://eits.ria.ee/et/abimaterjalid/veits (19.05.2025).

süsteemi), sealhulgas tegevustes või vahendite kasutamisel, mida ettevõtja oma väiksusest lähtudes ei pruugi teha või omada. Muudatuse puhul on arvesse võetud ka asjaolu, et asutusel ei pruugi olla eraldi infoturbe eest vastutavat isikut ning Eesti infoturbestandardi järgimise kohustuse täitmisest tulenevat töökoormust kannab töötaja, kellel puuduvad valdkonnateadmised. Samuti ei ole nimetatud asutustel üldjuhul suure mõjuga võrgu- ja infosüsteeme, sealhulgas andmekogusid, ja nad ei halda neid.

Järeldus mõju olulisuse kohta
Muudatuse tulemusel väheneb vähem kui 50 töötajaga kohaliku omavalitsuse hallatava asutuse või riigimuuseumi töökoormus. Riigi Infosüsteemi Ameti hinnangul kulub üldiste turvameetmete hindamiseks 1–2 tundi ühe hindamiskorra kohta. Sellest lähtudes on see ajaline kokkuhoid, mis saavutatakse töökoormuse vähendamise kaudu tegevust toetavate ülesannete vähendamise teel, märkimisväärne ning mõju asutuse tegevusele märgatav.

6.3. *Eesti infoturbestandardi või standardi ISO/IEC 27001 täismahus järgimise kohustusega ettevõtjate ja asutuste arvu vähenemine*

Eelnõukohase määruse jõustumisel väheneb nende teenuse osutajate arv, kellel on vahetu kohustus järgida kasutatavates võrgu- ja infosüsteemides täies mahus Eesti infoturbestandardi või standardi ISO/IEC 27001 nõudeid, mis asendatakse esmaste turvameetmete järgimise kohustusega.

Mõjuvaldkond: mõju küberkeskkonnale ja küberhügieenile (infotehnoloogia ja infoühiskonna valdkond)

Mõju sihtrühm: küberturvalisuse seaduse subjektist mikro- ja väikeettevõtja ning alla 50 töötajaga valla või linna ametiasutuse hallatav asutus ning osavalla või linnaosa ametiasutuse hallatav asutus ja riigimuuseum (edaspidi koos *väike organisatsioon*).

Avalduv mõju ja mõju olulisus
Eelnõuga vähendatakse väikeste organisatsioonide küberturbenõuete detailsust, säilitades meetmed üldisel kujul, võimaldades organisatsioonidel arvestada paremini tegevusest tulenevaid eripärasid. Kui väike organisatsioon järgib riskipõhiselt infoturbe ja küberhügieeni põhimõtteid oma võrgu- ja infosüsteemide kasutamisel, sealhulgas teeb koostööd asjaomaste asutustega, ei ole ette näha suurenenud ohtu üldisele küberkeskkonnale, sealhulgas avalikele teenustele. Muudatusega ei võeta väikestelt organisatsioonidelt vastutust puudulikust infoturbest tulenevate tagajärgede eest ei küberturbe ega ka andmekaitse valdkonnas.

Järeldus mõju olulisuse kohta: eelnõuga kavandatakse vähendada küberturvalisuse seaduse subjektidest väikestele organisatsioonidele kohalduva korra detailsust. Eelnõukohase määrusega ei kaotata väikeste organisatsioonide kohustust tagada kasutatavate võrgu- ja infosüsteemide turvalisus ega vastutust selle eest, seega on eelnõu mõju üldisele küberkeskkonnale väike.

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

Eelnõu määrusena jõustumise korral ei kaasne riigieelarvele ega kohaliku omavalitsuse üksuste eelarvele lisakulu ega -tulu. Alla 50 töötajaga valla või linna ametiasutuse hallatava asutuse ning osavalla või linnaosa ametiasutuse hallatava asutuse ning riigimuuseumi töökoormuse

vähenemisega ei kaasne kohalikele omavalitsustele ega riigiasutustele kulu. Samas ei ole ette näha ka otsese kulu vähenemist ega vajadust kedagi koondada. Haridus- ja Teadusministeeriumi hallatavate asutustena tegutsevatel koolidel ei ole edaspidi Eesti infoturbestandardi täitmise auditi tegemise kohustust ning rahalised vahendid saab suunata koolis küberturvalisuse taseme hoidmiseks ja tõstmiseks.

8. Määruse jõustumine

Määrus jõustub 1. oktoobril 2025. Jõustumisaja kehtestamisel on arvestatud Riigi Infosüsteemi Ameti vajadusega üle vaadata haldus- ja riikliku järelevalvega seonduv dokumentatsioon ning viia see kooskõlla muudatustega.

9. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

9.1. Eelnõu esitati eelnõude infosüsteemi kaudu kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

9.2. Eelnõu saadeti arvamuse avaldamiseks Eesti Pangale, Riigi Infosüsteemi Ametile, Finantsinspektsioonile, Eesti Pangaliidule, Eesti Turvaettevõtete Liidule, Eesti Haiglate Liidule, Eesti Arstide Liidule, Eesti Perearstide Seltsile, Eesti Vee-ettevõtete Liidule, Eesti Kiirabi Liidule, Eesti Ravimihulgimüüjate Liidule, Ravimitootjate Liidule, Eesti Proviisorapteekide Liidule, Eesti Apteekrite Liidule ja Eesti Proviisorite Kojale, Eesti Elektritööstuse Liidule, Eesti Jõujaamade ja Kaugkütte Ühingule, Eesti Gaasiliidule, Eesti Transpordikütuste Ühingule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule, Eesti Kaubandus-Tööstuskojale, Eesti Põllumajandus-Kaubanduskojale, Eesti Toiduainetööstuse Liidule, Eesti Kaupmeeste Liidule ja Andmekaitse Inspektsioonile.

9.3. Eelnõu kooskõlastasid märkusteta Kultuuriministeerium, Riigikantselei ja Kaitseministeerium.

9.4. Eelnõu kooskõlastasid vaikimisi Haridus- ja Teadusministeerium, Regionaal- ja Põllumajandusministeerium, Kliimaministeerium ning Välisministeerium.

9.5. Eelnõu toetasid esitatud kujul Eesti Kiirabi Liit, Riigi Infosüsteemi Amet, Finantsinspektsioon, Andmekaitse Inspektsioon ja Eesti Vee-ettevõtete Liit.

9.6. Eelnõu kohta tegid märkusi ja ettepanekuid Rahandusministeerium, Siseministeerium, Sotsiaalministeerium, Majandus- ja Kommunikatsiooniministeerium, Eesti Esmatasandi Tervisekeskuste Liit, Eesti Haiglate Liit, Eesti Perearstide Selts, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Linnade ja Valdade Liit ning Eesti Kaubandus-Tööstuskoda.

9.7. Märkuste ja ettepanekutega arvestamise tabel on esitatud seletuskirja lisas.