23.11.2026

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

1. Sissejuhatus

Eelnõukohase määrusega täiendatakse avalike ülesannete täitmist oluliselt mõjutavate võrgu- ja infosüsteemide (edaspidi *süsteem*) toimepidevuse tagamise nõudeid. Muudatusega nähakse andmete pikaajalise säilimise eesmärgil ette säilituskoopia loomine ja selle hoidmine välisriigis asuvas turvalises andmekeskuses. Andmete taaskasutamise ja süsteemi toimepidevuse eesmärgil nähakse ette kohustus säilitada süsteemide krüptovõtmete koopiaid Eesti Vabariigi välisesinduses. Eelnõukohase määruse jõustumisel luuakse paremad eeldused olulise mõjuga teabe pikemaajaliseks säilitamiseks ning parandatakse võimalusi tagada andmete kättesaadavus ja taastamine.

Määruse eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku IKT taristu talituse IT arhitektuuri ja taristu nõunik Allan Allmere ja riikliku küberturvalisuse talituse õigusnõunik Guido Pääsuke (guido.paasuke@justdigi.ee). Eelnõu on keeletoimetanud sama ministeeriumi õigusloome korralduse talituse toimetaja Mari Koik (mari.koik@justdigi.ee).

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

Muudatus ei mõjuta ettevõtjate, inimeste ega vabaühenduste halduskoormust.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kahest paragrahvist.

Paragrahvis 1 on määruse nr 121 muutmise sätted.

Määruse nr 121 § 13 lg 1. Eelnõukohase määrusega loetakse määruse kehtiva versiooni § 13 tekst lõikeks 1 ja muudetakse selle lõike sõnastust. Muudatusega lisatakse kohustus säilitada sellise süsteemi kohta, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid, muu hulgas säilituskoopia välisriigis asuvas turvalises andmekeskuses (edaspidi *andmesaatkond*).

Säilituskoopia tegemise eesmärk arhiivinduses ja pikaajalise kasutatavuse seisukohast on luua võime säilitada olulise mõjuga süsteeme pika aja jooksul. Kui tavapärane varundus on mõeldud peamiselt lähimineviku andmete taastamiseks, siis pikaajalise säilitamise eesmärk on tagada, et avalike ülesannete täitmist oluliselt mõjutavate süsteemide (kriitilised andmekogud ja infosüsteemid) andmed oleksid avatavad, mõistetavad, kontrollitavad ja kasutatavad ka aastakümnete pärast. Säilituskoopia eesmärk ei ole seega asendada olemasolevat varundust ega katastroofitaaste võimekust, vaid luua uus pikaajaline varundus koos taastevõimekusega.

Pikaajalise säilitamise võimekuse vajadus tuleneb pikaajalisest riskist: kui riigi või kohaliku omavalitsuse üksuse tavapärane toimimine on pikemaks ajaks katkenud, ei pruugi aastakümnete pärast olla enam võimalik kasutada praeguseid varukoopiaid, tarkvara, andmebaasitehnoloogiat, taristut ega süsteemi tundvate spetsialistide teadmisi. Sellises olukorras peab olema alles andmestik koos piisava kirjeldusega, et selle tähendust oleks võimalik mõista ja vajaduse korral uues tehnilises keskkonnas kasutada. Seetõttu tuleb lisaks regulaarsele varundamisele luua andmesaatkonnas pikaajalise säilitamise teenus, mille kaudu koostatakse kriitilistest andmekogudest ja infosüsteemidest eraldi pikaajaliseks säilimiseks sobivad säilituskoopiad. Selline koopia ei tähenda üksnes andmefaili hoiule panemist. See peab sisaldama ka vajalikke metaandmeid, kirjeldusi, kontrollsummasid, versiooniteavet, sõltuvuste kirjeldust ja taastejuhendit. Eesmärk on säilitada mitte ainult andmed, vaid terviklik ja tõendatav kogum, mille abil on võimalik andmeid hiljem mõista, kontrollida ja vajaduse korral kasutada.

Määruse nr 121 § 13 lg 2. Eelnõukohase määrusega täiendatakse §-i 13 lõikega 2. Sätte kohaselt kehtestab säilituskoopia tegemise vajaduse ja varundamise sageduse valdkonna eest vastutav minister, kelleks praegu on justiits- ja digiminister. Kuigi säilituskoopia on mõeldud andmete taastamiseks pikema

aja möödudes, ei pruugi säilituskoopia tegemine igast andmesaatkonnas olevast avalike ülesannete täitmist oluliselt mõjutavast süsteemist olla vajalik. Vajadust hinnatakse koostöös Justiits- ja Digiministeeriumiga. Samuti tuleb süsteemi omanikul koostöös Justiits- ja Digiministeeriumiga hinnata, millise välbaga säilituskoopiat teha, et tagada võimalikult paljude andmete korrektsus. Säilituskoopia tegemisel tuleb arvestada, et mida pikem on välp, seda suurem on tõenäosus, et osa teavet erineb tegelikkusest, samuti seda, milline on lubatav eksimus, kui tekib vajadus säilituskoopia kasutamiseks. Andmesaatkonna juures varundatakse vaid ühte säilituskoopiat.

Määruse nr 121 § 13[1]**.** Lisatava paragrahviga nähakse ette kohustus lisaks andmesaatkonnas talletatavale teabele hoida Eestist väljaspool ka avalike ülesannete täitmist oluliselt mõjutavate süsteemide krüptovõtmete koopiaid.

Krüptovõti on krüptograafilise algoritmiga kasutatav teave, mille abil andmeid krüpteeritakse või dekrüpteeritakse ehk muudetakse taas loetavaks. Kõnesoleva sätte kontekstis on oluline krüpteeritud andmete dekrüpteerimiseks vajalik võti. Krüpteeritud andmete varukoopia olemasolu üksi ei taga nende taastatavust, kui andmete avamiseks vajalik võti ei ole kättesaadav. Krüptovõtme koopia säilitamise eesmärk on seetõttu toetada varundatud andmete taastamist ka olukorras, kus tavapärane võtmehalduslahendus ei ole kasutatav.

Andmesaatkonda edastatavad andmed krüpteeritakse Eestis. Nende dekrüpteerimiseks vajaliku krüptovõtme koopiat säilitatakse krüpteeritud andmetest eraldi, eelnevalt kokkulepitud Eesti Vabariigi välisesinduses. Sellise korralduse eesmärk on vähendada riski, et Eestis aset leidnud ulatuslik kriisiolukord või taristu kahjustumine muudab kättesaamatuks ka andmete taastamiseks vajaliku võtme. Võtme koopia hoidmine välisesinduses võimaldab seda säilitada väljaspool Eestis asuvat tavapärast kasutuskeskkonda ja lahus andmesaatkonnas hoitavatest krüpteeritud andmetest.

Välisesinduses säilitatav krüptovõtme koopia täiendab, mitte ei asenda süsteemi igapäevast võtmehaldust. Taastamisvõime säilitamiseks on oluline, et hoiul olev võtme koopia vastaks säilitatavatele krüpteeritud andmetele ning selle kasutamiseks vajalik teave oleks ajakohane. Võtme kättesaamine ja taastamisel kasutamine peab toimuma volitatud isikute kontrollitud ja dokumenteeritud korras.

Krüptovõtme koopiat säilitatakse kokkulepitud Eesti välisesinduses. Selleks peab süsteemi vastutav töötaja tegema vastava kokkuleppe Välisministeeriumiga, mille tulemusel määratakse kindlaks, millises välisesinduses krüptovõtme koopiat hoidma hakatakse. Säte ei välista olukorda, mil on mõistlik jaotada krüptovõti omakorda osadeks ja hoida neid osasid eri välisesindustes.

Paragrahvis 2 nähakse ette määruse jõustumine 1. jaanuaril 2027. a. (vt ka p 6)

3. Eelnõu vastavus Euroopa Liidu õigusele
Eelnõu ei ole seotud Euroopa Liidu õigusega.

4. Määruse mõjud
Eelnõukohase määrusega nähakse ette avalike ülesannete täitmist oluliselt mõjutavate võrgu- ja infosüsteemide säilituskoopiate loomine ning andmesaatkonnas varundamine. Teiseks nähakse ette süsteemi krüptovõtme koopia säilitamine Eesti välisesinduses.

Määrusel on mõju järgmistes mõjuvaldkondades: riigivalitsemine, infotehnoloogia ja infoühiskond.

4.1. Mõju keskvalitsuse korraldusele (riigivalitsemise mõjuvaldkond)
Mõju sihtrühm: loetelus olevate andmekogude ja infosüsteemide vastutavad ja volitatud töötlejad, riigi pakutavate avalike teenuste kasutajad (Eesti residendid, eraõiguslikud ja avalik-õiguslikud asutused). Muudatuse mõju avaldub sihtrühmale olukorras, kus Eestis olevaid andmeid ei ole võimalik taaskasutada.

Säilituskoopia tegemisega vähendatakse sõltuvust tehnoloogia arengust, st säilituskoopia formaat peab võimaldama selle kasutamist ka uute tehnoloogiatega. Määrusega kaasneb positiivne mõju riigi julgeolekule, kuna andmete varundamine andmesaatkonnas toetab Eesti omariikluse ja digitaalset järjepidevust. Säilituskoopia tegemine ei ole igapäevane ülesanne, vaid koopia tehakse kokkulepitud välba möödumisel. Andmesaatkonnas säilitatakse vaid ühte koopiat. Sellega võib tekkida olukord, kus

säilituskoopia kasutamise vajaduse tekkimisel ei pruugi selles olla viimased andmed, mis olid registris, kui selle kasutamine muutus võimatuks.

Kui juurdepääs Eestis paiknevale teabele on komplitseeritud või puudub, tagab varundamine andmesaatkonnas teabe kättesaadavuse ja avalike teenuste toimimise. Seega on määrusel nimetatud olukordades suur mõju teabe kättesaadavusele ja avalike teenuste toimimisele.

4.2. Mõju infotehnoloogilistele arendustele (infotehnoloogia ja infoühiskonna mõjuvaldkond)
Mõju sihtrühm: andmesaatkonna varundatud andmekogude ja infosüsteemide vastutavad töötlejad.
Riigi andmekogude ja infosüsteemide töötlejad tegelevad pidevalt infosüsteemide ja andmete varundamisega, mistõttu säilituskoopia tegemisega või krüoptovõtme koopia moodustamisega olulist muudatust töökorralduses ei kaasne. Mõju sihtrühmale on väike.

4.3. Mõju elektroonilisele sidele ja teenustele (infotehnoloogia ja infoühiskonna mõjuvaldkond)
Mõju sihtrühm: andmesaatkonnas varundatud andmekogude ja infosüsteemide vastutavad töötlejad.
Säilituskoopia ja krüptovõtme koopia loomine ei mõjuta vahetult avalike teenuste igapäevast kättesaadavust. Mõju sihtrühmale on väike.

4.4. Mõju e-riigile (infotehnoloogia ja infoühiskonna mõjuvaldkond)
Mõju sihtrühm: riigi- ja kohaliku omavalitsuse asutused, mis kasutavad oma ülesannete täitmisel andmesaatkonnas varundatud süsteeme.
Andmesaatkonnas asuv varundus, säilituskoopia ja krüptovõtme koopia ei ole kasutatavad igapäevases tegevuses, seega mõju sihtrühmale on väike.
Olukorras, kus Eestis asuvale süsteemile ei ole võimalik saada juurdepääsu, võimaldavad krüptovõtme koopia ja säilituskoopia vastavalt taastada juurdepääsu süsteemile või kasutada kopeeritud teavet andmete taastamiseks, vähendades sellega andmekadu teabe uuesti kogumise alustamisel ning kiirendades oluliselt juba olemas oleva teabe kasutuselevõtmist. Seega kaudne mõju sihtrühmale on suur.

4.5. Mõju küberkeskkonnale ja küberhügieen (infotehnoloogia ja infoühiskonna mõjuvaldkond)
Mõju sihtrühm: loetelus olevate andmekogude ja infosüsteemide vastutavad töötlejad.
Määrusel ei ole vahetut mõju kodanikele, ettevõtjatele, loetelus olevate andmekogude või infosüsteemides olevate andmete kasutajatele ega andmeandjatele. Samas on säilituskoopia või krüptovõtme koopia vahend, mida saab kasutada andmekogu või infosüsteemi töö või andmete taastamisel, kui andmekogus või infosüsteemis olevat teavet või selle toimimist on rikutud ja süsteemi kasutamine on takistatud või süsteem on vaja uuesti luua. Mõlemal juhul on tegemist andme ja küberturbega seotud elemendiga, millel puudub igapäevane mõju, kuid mille mõju võib avalduda erandlikes olukordades. Seega on tagatud andmekogude ja infosüsteemide parem toimepidevus.

5. Määruse rakendamisega seotud tegevused, eeldatavad kulud ja tulud
Määruse jõustumisega ei kaasne riigieelarvele otseseid kulusid ega saada tulu.

6. Määruse jõustumine
Eelnõukohane määrus jõustub 1. jaanuaril 2027. Jõustumisaja kehtestamise juures on arvestatud, et see oleks piisav aeg süsteemide, millel on oluline mõju riigi ja kohaliku omavalitsuse üksuse võimele täita avalikke ülesandeid, vastutavatele töötlejatele muudatustega tutvumiseks ja oma tegevuste kavandamiseks.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon
Eelnõu esitatakse kooskõlastamiseks eelnõude infosüsteemi kaudu ministeeriumitele ja Riigikantseleile ning Eesti Linnade ja Valdade Liidule. Eelnõu saadetakse arvamuse avaldamiseks Andmekaitse Inspektsioonile, Rahvusarhiivile, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Riigi Infosüsteemi Ametile ning Registrite ja Infosüsteemide Keskusele.