04.06.2026

Vabariigi Valitsuse määruse „Vabariigi Valitsuse 23. detsembri 1996. a määruse nr 319 „Justiits- ja Digiministeeriumi põhimääruse kinnitamine“, Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning Vabariigi Valitsuse 3. jaanuari 2024. a määruse nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ muutmine“ eelnõu
SELETUSKIRI

1. Sissejuhatus

1.1. Sisukokkuvõte

Küberturvalisuse 2. direktiiv ehk NIS2-direktiiv võeti suuremas osas üle küberturvalisuse seaduse ja teiste seaduste muutmise seadusega (küberturvalisuse 2. direktiivi ülevõtmine) (eelnõu nr 739 SE) (edaspidi *ülevõtmisseadus*).[1] Kõnesoleva eelnõuga kavandatakse üle võtta ainult üksikud NIS2-direktiivi sätted (artikli 14 lõige 3, artikli 16 lõige 2 ning artikli 21 lõiked 2 ja 3), mille sisu ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega. Samuti tehakse tehnilisi täpsustusi, et tagada õigusselgus nii eelnõukohase määrusega muudetavate määruste kehtivate sätete kui ka eelnõukohase määrusega lisanduvate sätete rakendamisel.

Eelnõu määrusena vastuvõtmise tulemusena osaleb Justiits- ja Digiministeerium oma pädevuse kohaselt NIS2-direktiivi artiklis 14 nimetatud koostöörühma tegevuses ja artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku töös.

Küberturvalisuse seaduse § 7 kehtestab teenuseosutajatele nõude rakendada turvameetmeid. Eelnõukohase määrusega asendatakse seda kohustust miinimumtasemel reguleeriv lisa ehk esmaseid turvameetmeid täpsustav lisa. Ülevõtmisseaduse tulemusena peavad küberturvalisuse seaduse kohased teenuseosutajad rakendama turvameetmeid (st ka esmaseid turvameetmeid) kogu organisatsiooni suhtes. See lähenemisviis oli enne ülevõtmisseadusega tehtud muudatuste jõustumist juba avalikus sektoris kasutusel, kuid erasektori jaoks on see uus. Et tagada NIS2-direktiivi kitsendatud ülevõtmine, leevendatakse nende teenuseosutajate (ennekõike erasektori teenuseosutajate) nõudeid, kes peavad rakendama Eesti infoturbestandardit või selle alternatiiviks olevat standardit. Muudatusega nähakse ette, et ühe mainitud standardi nõudeid tuleb rakendada vähemalt selle teenuse, tegevusala või valdkonna puhul, mida pakkuv või millel tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. See tähendab, et standard peab käsitlema vastava teenuse, tegevusala või valdkonnaga seotud võrgu- ja infosüsteeme, kuid ülejäänud teenuste, tegevusalade ja valdkondadega seotud võrgu- ja infosüsteemide puhul saab rakendada paindlikumaid turvameetmeid, st ennekõike eelnõukohase määrusega uuendatud esmaseid turvameetmeid. Teenuseosutajatele (sh ennekõike erasektori teenuseosutajale) avalduv majanduslik mõju on väga erinev ning seda ei ole võimalik mõistlikult hinnata. Turvameetmete rakendamise rahaline kulu sõltub teenuseosutaja kasutatavate võrgu- ja infosüsteemide hulgast ja keerukusest ning varem rakendatud turvameetmetest (teenuseosutaja vastutustundlikkusest oma IT-lahenduste kasutamisel või muudest nõuetest, näiteks isikuandmete töötlemisel rakendatud tehnilistest ja

[1] Eelnõude infosüsteemi toimikud 24-1266 ja 25-0926. Riigikogus menetluses olnud eelnõu: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine/.

korralduslikest turvalisuse tagamise meetmetest). Teenuseosutajale avalduv rakendamiseks vajaliku kulu majanduslik mõju sõltub omakorda selle kulu osakaalust tema eelarves, ennekõike IT-lahendustega seotud eelarves. Esmaseid turvameetmeid täiendavate nõuete sisu ja olemus ei ole siiski sedavõrd märkimisväärne, et need tooks teenuseosutajatele kaasa olulist kulu. Seda enam, et küberturvalisuse seaduses on sätestatud ka üleminekuajad seaduse nõuete täitmiseks.
Kuna ülevõtmisseadus suurendas halduskoormust (küberturvalisuse seaduse kohaldamisala täiendati uute subjektidega, kes peavad seaduse nõudeid ja seeläbi ka selle seaduse alusel kehtestatud määruste nõudeid täitma), tasakaalustati seda halduskoormuse tõusu Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega.[2] Need muudatused jõustusid 1. oktoobril 2025. Kõnesolev eelnõukohane määrus näeb ette halduskoormuse mõningase kasvu, kuid samal ajal võimaldab eelnõuga kavandatav Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitlusala muudatus leevendada eelnõu mõju.
Kokkuvõtlikult sisaldab eelnõu ettevõtjatele nii halduskoormust suurendavaid kui ka vähendavaid muudatusi. Halduskoormus võib suureneda esmaste turvameetmete nõuete täpsustamise tõttu. Samas vähendab koormust standardi kohaldamisala piiramine ennekõike seaduse kohaldamisalasse kuuluvate teenuste või tegevustega seotud võrgu- ja infosüsteemidega. Muudatuste tegelik mõju halduskoormusele sõltub ettevõtja suurusest, tegevusvaldkonnast ja senisest turvatasemest. Halduskoormuse tasakaalustamise reeglit ei ole vaja rakendada.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse küberturvalisuse õigusnõunikud Raavo Palu ja Guido Pääsuke (riiklikkyber@justdigi.ee). Eelnõu ja seletuskirja on keeleliselt toimetanud sama ministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Merike Koppel (merike.koppel@justdigi.ee).

1.3. Märkused

Eelnõu on seotud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga nr 739 SE.[3] Selle seaduseelnõuga kavandatud muudatused jõustusid 1. jaanuaril 2026.

Eelnõukohase määrusega muudetakse järgmisi Vabariigi Valitsuse määrusi:

- 23. detsembri 1996. a määrus nr 319 „Justiits- ja Digiministeeriumi põhimääruse kinnitamine“ (RT I, 16.09.2025, 18) (edaspidi *määrus nr 319*);
- 9. detsembri 2022. a määrus nr 121„Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (RT I, 27.09.2025, 2) (edaspidi *määrus nr 121*);
- 3. jaanuari 2024. a määrus nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ (RT I, 09.01.2024, 25) (edaspidi *määrus nr 1*).

Eelnõukohase määrusega võetakse üle 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) (ELT L 333, 27.12.2022, lk 80–152) (edaspidi ka *NIS2-direktiiv*), artikli 14 lõige 3, artikli 16

[2] https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6
[3] Vt altviidet nr 1.

lõige 2 ning artikli 21 lõiked 2 ja 3 osas, mida ei reguleerita küberturvalisuse seaduse ega muude õigusaktidega.

Eelnõu on seotud 2025.–2027. aasta koalitsioonileppe riigikaitse ja julgeoleku valdkonna eesmärgiga „tagame Eesti digiühiskonna toimepidevuse nii, et teenused on küberturvaliselt kättesaadavad igas olukorras“ ning tõhusa asjaajamise valdkonna eesmärgiga „võtame Euroopa Liidu õiguse üle Eestile sobivaimal moel ja teeme Euroopas ettepanekud sobimatute normide muutmiseks, sealhulgas ettepanek lükata edasi kestlikkusaruandluse esitamine ja muuta need vabatahtlikuks“.[4] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027[5] ELi direktiivide valdkonna all nimetatud ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Kuna nii ülevõtmisseadusega kui ka kõnesoleva eelnõukohase määrusega suurendatakse teatavas ulatuses halduskoormust (küberturvalisuse seadust täiendati uute subjektidega, kes peavad täitma seaduse nõudeid, sh ka kõnesoleva eelnõuga kavandatavate muudatustega täpsustatavaid nõudeid), nähti halduskoormuse tasakaalustamine ette määruse nr 121 muudatustega, mis jõustusid 1. oktoobril 2025. Lisaks leevendatakse eelnõukohase määrusega nende teenuseosutajate (ennekõike erasektori, kuid põhimõtteliselt ka avaliku sektori teenuseosutajate) nõudeid, kes peavad Eesti infoturbestandardit või selle alternatiiviks olevat standardit rakendama. Muudatusega nähakse ette, et ühe mainitud standardi nõudeid tuleb rakendada vähemalt selle teenuse, tegevusala või valdkonna puhul, mida pakkuv või millel tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. See tähendab, et standard peab käsitlema vastavat teenust, tegevusala või valdkonnaga seotud võrgu- ja infosüsteeme, kuid ülejäänud teenuste, tegevusalade ja valdkondadega seotud võrgu- ja infosüsteemide puhul saab rakendada paindlikumaid turvameetmeid ehk ennekõike eelnõukohase määrusega täpsustatud esmaseid turvameetmeid. Seega on eelnõukohase määrusega tehtav Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitlusala muudatus halduskoormuse vähendamise lisameede, mis leevendab eelnõukohase määruse mõju.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kolmest paragrahvist.

Paragrahviga 1 muudetakse määrusega nr 319 kinnitatud „Justiits- ja digiministeeriumi põhimäärust”. Paragrahv koosneb kahest punktist.

Paragrahvi 1 punktiga 1 muudetakse punkti 54^1, täiendades seda alapunktiga 1^1.
Muudatus on seotud NIS2-direktiivi artikli 14 lõike 3 esimese lause ning artikli 16 lõike 2 ülevõtmisega. Kommenteeritava alapunktiga on kavas anda Justiits- ja Digiministeeriumile asjaomased volitused, kuna Vabariigi Valitsuse seaduse § 44 lõike 1 kohaselt on riiki volitatud esindama valitsusasutus või muu riigiasutus seadusest, oma põhimäärusest ja teistest õigusaktidest tulenevate ülesannete täitmisel. Sarnane esindusvolitus artiklite 14 ja 16 kontekstis anti ka Riigi Infosüsteemi Ametile ning need muudatused jõustusid 1. veebruaril 2026.[6]

[4] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[5] https://valitsus.ee/sites/default/files/documents/2023-05/VVTP%202023-2027_26.pdf
[6] Riigi Infosüsteemi Ameti põhimäärus (RT I, 29.01.2026, 2), § 8 lõike 4 punkt 3^1. https://www.riigiteataja.ee/akt/129012026002

Paragrahvi 1 punktiga 2 täiendatakse määrusega nr 319 kinnitatud „Justiitsministeeriumi põhimäärust" normitehnilise märkusega NIS2-direktiivi kohta.
Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 180 „Hea õigusloome ja normitehnika eeskiri" § 27 lõike 3 esimene lause näeb ette, et kui seaduseelnõu koostatakse Euroopa Liidu õiguse ülevõtmiseks, nimetatakse normitehnilises märkuses Euroopa Liidu õigusakti andja või andjad, akti liik, number, pealkiri ja avaldamismärge. Sama määruse § 51 kohaselt kehtib nimetatud põhinõue ka Vabariigi Valitsuse määruse ja ministri määruse eelnõu kohta.
Normitehniline märkus lisatakse määrusesse nr 319, kuna muudesse õigusaktidesse pole neid NIS2-direktiivi artikli 14 lõiget 3 ja artikli 16 lõiget 2 üle võtvaid sätteid, mis on seotud Justiits- ja Digiministeeriumiga, kavandatud.

Paragrahviga 2 muudetakse määrust nr 121. Paragrahv koosneb neljateistkümnest punktist.

Paragrahvi 2 punktiga 1 asendatakse määruses nr 121, välja arvatud § 4 lõikes 1^1, läbivalt sõnad „teenuse osutaja" liitsõnaga „teenuseosutajaga". Sama muudatus nähti ülevõtmisseadusega ette ka küberturvalisuse seaduses. Tegemist on tehnilise muudatusega, mille eesmärk on järgida eesti keele kokku- ja lahkukirjutuse põhimõtteid.
Kommenteeritava punktiga ei muudeta määruse nr 121 § 4 lõiget 1^1, kuna see muudaks hädaolukorra seaduse termini „elutähtsa teenuse osutaja" tähendust. Nimelt laiendab selle täiend „elutähtis" täiendit „teenus", mitte kogu järgnevat ühendit „teenuseosutaja".

Paragrahvi 2 punktiga 2 täiendatakse määruse nr 121 § 2 punktidega 1^1 ja 1^2, lisades vastavalt terminid „andmekogu vastutav töötleja" ja „andmekogu volitatud töötleja" ja nende tähenduse.
Andmekogu vastutav töötleja on andmekogu vastutav töötleja avaliku teabe seaduse § 43^4 lõike 1 tähenduses ehk *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.*
Andmekogu volitatud töötleja on andmekogu volitatud töötleja avaliku teabe seaduse § § 43^4 lõike 2 tähenduses. Selle lõike 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.*
Kommenteeritav muudatus tehakse õigusselguse tagamise huvides, kuna praktikas on tekkinud määruse nr 121 § 4 lõike 4 punkti 2 (näiteks seoses omavalitsuste ning nende hallatavate asutustega) tõlgendamisel eri osalistel küsimus, millist vastutavat töötlejat ja volitatud töötlejat on selles punktis mõeldud – kas tegemist on avaliku teabe seaduse terminitega või isikuandmete kaitse valdkonnas kasutatavate terminitega. Nende kahe valdkonnaga seotud terminite eristamise kohta vt ülevõtmisseaduse kohase küberturvalisuse seaduse § 3 lõike 4 punkti 1 selgitust. 2025. aasta 1. oktoobril jõustus määruse nr 121 § 4 lõike 4 muudatus, millega lisati sellesse lõikesse uus punkt 4 (seoses Haridus- ja Teadusministeeriumi hallatava asutusena tegutsevate põhikoolide ja gümnaasiumitega), milles on samuti kasutatud väljendit „andmekogu vastutava töötleja ja volitatud töötleja". Ka selle punkti puhul on juba tekkinud sarnaseid küsimusi mis sama lõike punkti 2 puhul. Võimalike väärarusaamade vähendamiseks tagatakse kõnealuse muudatusega õigusselgus viidatud lõike punktides kasutatavates terminites.

Paragrahvi 2 punktiga 3 muudetakse määruse nr 121 § 2 lõiget 3.

Muudetavas lauses viidatakse küberturvalisuse seaduse § 3 lõike 4 punktidele 12 ja 13, mis kuni 31. detsembrini 2025 hõlmas järgmisi üksusi: valitsusasutus, valitsusasutuse hallatav riigiasutus, valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald, linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus, kohaliku omavalitsuse üksuste ühisamet ja -asutus. Uues tekstiosas on kasutatud sõnu „valitsusasutus“ (vt Vabariigi Valitsuse seaduse § 39), „valitsusasutuse hallatav riigiasutus“ (vt Vabariigi Valitsuse seaduse § 43 lõige 1) ja „kohaliku tasandi avaliku halduse üksus (vt küberturvalisuse seaduse § 2 punkt 16). Seeläbi tagatakse kooskõla küberturvalisuse seadusega.

Paragrahvi 2 punktiga 4 täiendatakse määruse nr 121 § 3 lõikega 1^1.
Eesti Infotehnoloogia ja Telekommunikatsiooni Liit tegi ülevõtmisseaduse menetluse käigus ettepaneku *lähtuda nõuete rakendamisel ka küberturvalisuse 2. direktiivis rõhutatud riskipõhisusest ehk võimaldada subjektidel määratleda, kus ja millised on tema organisatsioonis olulisemad riskid ja võtta kasutusele vastavad meetmed.* Liit leiab, *et selle täienduse lisamine on vajalik, et siduda nendes sätetes toodud kohustused ehk [küberturvalisuse seaduse] alusel kehtestatud turvameetmed ettevõtete ja asutuste konkreetsete teenustega, mille osutamise tõttu nad on [seaduse] mõistes üliolulised või olulised üksused. Sellega jäetakse ettevõtetele ja asutustele õigus ise hinnata, mis on nende vaatest kriitiline ja lähtuda tehtud riskihinnangutest.*
Eelnõu koostaja toetab ettepanekut. Vabariigi Valitsuselt Riigikokku esitatud seaduseelnõus kavandati näha Vabariigi Valitsusele võrgu ja infosüsteemi küberturvalisuse nõuete kehtestamisel ette volitusnorm täpsustada alalisi asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke turvameetmeid ning rakendamise nõudeid ja tingimusi. Et oleks selge, et Vabariigi Valitsusel on õigus nende nõuete kehtestamisel arvesse võtta ka tegevusalasid, mille osutamise tulemusel tekib ettevõtjal küberturvalisuse nõuete järgimise kohustus, täiendati ülevõtmisseaduse menetluse käigus vastavat volitusnormi. Selle täienduse kohaselt võib Vabariigi Valitsus arvestada määrusega nr 121 kehtestatavate nõuete puhul küberturvalisuse seaduse § 3 lõigetes 2–5 sätestatut. Nimetatud lõigetes on loetletud teenused, tegevusalad ja valdkonnad, mida pakkuvat või kus tegutsevat üksust käsitatakse üliolulise või olulise üksusena. Seega võimaldab muudatus Vabariigi Valitsusel ette näha paindlikkust turvameetmete rakendamisel.
Kommenteeritav lõige toob kaasa asjaolu, et sama paragrahvi lõike 1 alusel kehtestatud nõudeid (st Eesti infoturbestandardi nõudeid) rakendatakse vähemalt kommenteeritavas lõikes viidatud tegevusala või tegevusaladega – olenevalt sellest, kas üksus on ühe või mitme tegevusala tõttu ülioluline üksus või oluline üksus – seotud võrgu- ja infosüsteemidele. Kommenteeritavas lõikes on kasutatud sõna „vähemalt“ tagamaks, et Eesti infoturbestandardi rakendamine hõlmab tegevusala(sid), kus tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. Teenuseosutaja ise valib, kas ta soovib ka oma muude tegevusalade või teenustega seotud võrgu- ja infosüsteemide suhtes rakendada Eesti infoturbestandardist tulenevaid nõudeid. Kui teenuseosutaja seda valikut ei tee, siis peab ta nende muude tegevusalade, teenuste või valdkondadega seotud võrgu- ja infosüsteemide suhtes rakendama miinimumnõudeid ehk esmaseid turvameetmeid (vt määruse nr 121 § 5^1 ja sama määruse lisa ning ka eelnõu § 2 punkt 13).
Eelnõuga kavandatav muudatus säilitab peamiselt Eesti infoturbestandardi rakendamise kontekstis ennekõike nende ettevõtjate olukorra, kes pidid enne ülevõtmisseadusega tehtud muudatuste jõustumist (st kuni 31.12.2025) küberturvalisuse nõudeid järgima ainult konkreetse teenuse või tegevusala puhul. Kõnealune muudatus ei kohaldu nendele teenuseosutajatele, kes on ülioluline üksus või oluline üksus oma tegevusvormi, mitte tegevusvaldkonna tõttu: näiteks avalik-õiguslikud juriidilised isikud, keskvalitsuse avaliku halduse üksused ja kohaliku omavalitsuse avaliku halduse üksused. Seda seetõttu, et nimetatud üksused kuulusid ka enne

ülevõtmisseadusega tehtud muudatuste jõustumist ja kuuluvad ka edaspidi terve organisatsioonina küberturvalisuse seaduse kohaldamisalasse. Samuti on kaheldav, kas tegevusvormi alusel küberturvalisuse seaduse kohaldamisalasse liigituva teenuseosutaja puhul oleks võimalik hakata eristama konkreetset tegevusala, teenust või valdkonda ning nendega seotud võrgu- ja infosüsteeme.
Lühendsõna „süsteem“ on võetud kasutusele määruse nr 121 § 1 lõike 1 punktis 2, st see on moodustatud terminist „võrgu- ja infosüsteem“. Selle termini kohta vt küberturvalisuse seaduse § 2 punkt 37.

Paragrahvi 2 punktiga 5 täiendatakse määruse nr 121 § 3 lõike 2 punkti 1.
Määruse nr 121 § 3 lõige 2 näeb ette Eesti infoturbestandardi alternatiivi ehk rahvusvahelise standardi ISO/IEC 27001 või Eesti standardi EVS-EN ISO/IEC 27001 nõuete rakendamise. Kui eelnimetatud standardite käsitlusala on sama ulatusega nagu Eesti infoturbestandardi oma, siis kohaldub määruse nr 121 § 3 lõige 2. See tähendab, et teenuseosutaja on 1) asjakohaste rakendusala(de) suhtes rakendanud turvameetmeid lähtuvalt rahvusvahelisest standardist ISO/IEC 27001 või Eesti standardist EVS-EN ISO/IEC 27001 ning 2) on esitanud Riigi Infosüsteemi Ametile kehtiva vastavussertifikaadi, mis kinnitab ühe eelmainitud standardi nõuete täitmist. Asjakohaste rakendusalade all mõeldakse neid tegevusalasid, kus tegutsev teenuseosutaja kuulub üliolulise üksuse või olulise üksusena küberturvalisuse seaduse kohaldamisalasse.
Kõnealune muudatus tagab, et eelnõu § 2 punktis 3 kavandatud muudatus kohaldub ka juhul, kui teenuseosutaja on otsustanud Eesti infoturbestandardi asemel rakendada alternatiivset standardit. Seetõttu käivad eelnõu § 2 punkti 3 selgitused ka kõnealuse muudatuse kohta.

Paragrahvi 2 punktiga 6 muudetakse määruse nr 121 § 3 lõike 2^1 sissejuhatava lause sõnastust. Kõnesoleva eelnõuga lisatakse sellesse paragrahvi uus lõige (vt eelnõu § 2 punkt 4), mistõttu tuleb õigusselguse huvides kommenteeritava lõike sissejuhatavat lauset muuta. Muudatuse tulemusena ei kohaldata määruse nr 121 § 3 lõikeid 1, 1^1 ja 2 üksustele, keda on nimetatud sama paragrahvi lõikes 2^1.

Paragrahvi 2 punktiga 7 asendatakse määruse nr 121 § 3 lõike 2^1 punktis 1 sõna „määratlemise“ sõnaga „määratluse“. Tegemist on tehnilise muudatusega (parandatakse pealkirja sõnastust), kuna selles punktis viidatud Euroopa Komisjoni soovituse tegelik pealkiri on „Komisjoni soovitus, mis käsitleb mikro-, väikeste ja keskmise suurusega ettevõtjate määratlust“.[7]

Paragrahvi 2 punktiga 8 täiendatakse määruse nr 121 § 3 lõigetega 2^2 ja 2^3.
Kuigi NIS2-direktiivi artikli 2 lõike 1 teine lõik võeti üle ülevõtmisseaduse kohase küberturvalisuse seaduse § 3 lõikega 6, siis kõnealuse muudatusega (lisanduv **lõige 2^2**) tagatakse selgus, et viidatud seaduse sättes sisalduv nõue kohaldub oma sisult ja mõttelt ka Eesti infoturbestandardi või selle alternatiivina kasutatava standardi järgimise kohustuse kontekstis. Euroopa Komisjoni soovituse 2003/361/EÜ lisa artikli 3 lõige 4 kehtestab üldreegli, mille kohaselt ei ole ettevõtja väike- ega keskmise suurusega, kui tema kapitalist või hääleõigusest 25% või enamat kontrollivad otseselt või kaudselt, ühiselt või üksikult, üks või mitu avaliku sektori organisatsiooni (ingl *controlling public body*). Vt selle kohta ka nimetatud soovituse põhjendus 13:

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202490772

(13) Vältimaks kunstlikku vahetegemist liikmesriigi erinevate avalik-õiguslike asutuste vahel ja arvestades vajadust õiguskindluse järele, peetakse vajalikuks kinnitada, et VKE ei ole ettevõte, mille kapitalist või hääleõigustest 25% või enam kontrollib avalik-õiguslik asutus.
NIS2-direktiivi artikli 2 lõike 1 teine lõik täpsustab, et viidatud soovituse artikli 3 lõiget 4 ei arvestata NIS2-direktiivi puhul. Kuna küberturvalisuse seadusesse lisati sama nõue, siis selguse huvides lisatakse sarnane nõue ka Eesti infoturbestandardi või selle alternatiivina kasutatava standardi järgimise nõudele. Eeltoodu tõttu on muudatuse tulemusena võimalik mõnda üksust pidada väike- või keskmise suurusega ettevõtjaks, kui seda kontrollib (osaliselt) avaliku sektori organisatsioon ning tingimusel, et kommenteeritava paragrahvi lõike 2^1 punktis 1 nimetatud tingimused (töötajate arv ja finantsnäitajad) on täidetud. NIS2-direktiiv ei näe ette nõudeid selle kohta, kuidas teha kindlaks töötajate arv ja finantsnäitajad avaliku sektori organisatsioonide puhul. Need üksused kuuluvad NIS2-direktiivi artikli 2 lõike 2 punkti f ja lõike 5 punkti a kohaselt NIS2-direktiivi kohaldamisalasse, olenemata üksuse suurusest. Soovitusega 2003/361/EÜ ei ole mõeldud reguleerida seda, kuidas toimida kontrolli omavate avaliku sektori organisatsioonidega, ja see ei sisalda selgeid reegleid selle teema kohta. Selle soovituse reeglite järgimine kontrolli omavate avaliku sektori organisatsioonide puhul (tuvastamaks nende seost partner- ja sidusettevõtjatega väike- või keskmise suurusega ettevõtjate puhul) tekitaks Euroopa Liidu liikmesriikide seas killustatust ja õiguslikku segadust. Seetõttu ei tule eraldiseisva kontrolli omava avaliku sektori üksuse töötajate arvu ja finantsnäitajaid arvesse võtta, kui selgitatakse kommenteeritava lõike kohaselt välja ettevõtjate töötajate arvu ja finantsnäitajaid. Vt lisaks ülevõtmisseaduse § 3 selgituse alguses esitatud selgitusi soovituse 2003/361/EÜ kohta.

Lisanduva **lõikega 2^3** sätestatakse lisareegel üksuse töötajate arvu, aastakäibe ja aastabilansimahu arvestamise kohta partner- ja sidusettevõtjate puhul. Sellise reegli loomise võimalusele viitab NIS2-direktiivi põhjendus 16, mis on sõnastatud järgmiselt:
(16) Vältimaks seda, et üksusi, millel on partnerettevõtjad või mis on sidusettevõtjad, peetaks elutähtsateks[8] või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohaldamisel võtta arvesse üksuse oma partneritest või sidusettevõtjatest sõltumatuse määra. Eelkõige on liikmesriikidel võimalik võtta arvesse asjaolu, et üksus on oma partner- või sidusettevõtjatest sõltumatu teenuste osutamisel kasutatavate võrgu- ja infosüsteemide osas, ja teenuste osas, mida üksus osutab. .. .
Arvestades NIS2-direktiivi ülevõtmisel järgitud üldpõhimõtet, et riigisiseselt ei sätestata NIS2-direktiivis ette nähtud miinimumnõuetest rangemaid nõudeid, on lõikesse 2^2 lisatud NIS2-direktiivi põhjenduses 16 sätestatud võimalus jätta partner- ja sidusettevõtjate töötajate arv ning käibe- või bilansimaht arvestamata. Seeläbi on võimalik Eesti infoturbestandardi või selle alternatiivina kasutatava standardi kohaldamise nõude kohaldamisalast välja jätta sellised üksused, kes vastaks töötajate arvu ning käibe- või bilansimahu poolest standardi rakendamise nõudele just seetõttu, et partner- ja sidusettevõtja vastavad näitajad lisanduvad konkreetse üksuse näitajatele – st, et vaadeldav üksus enda näitajate järgi piirmäärasid ei ületaks, kuid teeks seda siis, kui tuleb arvestada ka partner- ja sidusettevõtjate näitajaid. Selline lahendus on nendele ettevõtjatele ka palju soodsam. Kommenteeritavas lõikes ette nähtud välistust on võimalik rakendada, kui asjaomasel partner- või sidusettevõtjal on otsustav mõju enda infotehnoloogiasüsteemide toimimise üle ehk kui ta on enda IT-lahenduste korraldamisel sõltumatu. Selline sõltumatus infotehnoloogiasüsteemide toimimise üle otsustamisel on olemas eelkõige siis, kui partner- ja sidusettevõtja saab omal vastutusel teha põhilisi otsuseid infotehnoloogiasüsteemide, selle komponentide ja protsesside üle. Kui partner- või sidusettevõtja on selliste otsuste tegemisel vaba, siis ei arvestata üksuse töötajate arvu ja käibe-

[8] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulisеks üksuseks“.

või bilansinäitajate kindlakstegemisel tema töötajate arvu, käivet ega bilansimahtu. Kõnealuse välistuse kohaldamine ei tule aga kõne alla juhul, kui IT-lahendusi rakendatakse terves kontsernis ühetaoliselt, näiteks otsustab kõik IT-süsteemidega seotud küsimused emaettevõtja.

Paragrahvi 2 punktiga 9 täiendatakse määruse nr 121 § 5 lõikega 1^1.
Kommenteeritava lõikega määratakse kindlaks, mida riskianalüüs peab sisaldama. Kõnealuse sättega võetakse üle NIS2-direktiivi artikli 21 lõike 2 punkt a (*[l]õikes 1 osutatud meetmed põhinevad kõiki ohte hõlmaval lähenemisviisil, mille eesmärk on kaitsta võrgu- ja infosüsteeme ning nende süsteemide füüsilist keskkonda intsidentide eest, ning hõlmavad vähemalt järgmist: a) riskianalüüsi ja infosüsteemide turbe põhimõtteid;*) ning säilitatakse kuni 31. detsembrini 2025 kehtinud küberturvalisuse seaduse § 7 lõike 2 punkti 1 sisu[9].
Kommenteeritava punktiga on seotud ka infoturvariskide kaardistamine ja nende haldamine. AKITi kohaselt on infoturvarisk (ingl *information security risk*) määramatuse toime teabe turvalisusele, ohu potentsiaal tekitada kahju teabe ja sellega kaasnevate varade turvalisuse rikkumisega ning seda mõõdetakse ohu realiseerumise sündmuse võimalikkuse ja tagajärgedega.[10] Eesti infoturbestandardi portaalis on seda terminit selgitatud järgnevalt: *võimalus, et mingi oht kasutab ära mingi vara või varade rühma nõrkuse ning seeläbi tekitab organisatsioonile kahju*.[11]
Lühendsõna „süsteem“ on võetud kasutusele määruse nr 121 § 1 lõike 1 punktis 2, st see on moodustatud terminist „võrgu- ja infosüsteem“. Selle termini kohta vt küberturvalisuse seaduse § 2 punkt 37. Termini „risk“ kohta vt küberturvalisuse seaduse § 2 punkt 25. Lühendväljend „süsteemi turvalisus“ on moodustatud terminist „võrgu- ja infosüsteemi turvalisus“, mille kohta vt küberturvalisuse seaduse § 2 punkt 38. Termini „küberintsident“ kohta vt küberturvalisuse seaduse § 2 punkt 19.
Sõna „toimepidevus“ puhul saab teatava paralleeli tuua hädaolukorra seaduse § 2 lõikes 5 sätestatud elutähtsa teenuse toimepidevuse määratlusega, mille kohaselt on see *elutähtsa teenuse osutaja järjepideva toimimise suutlikkus ja järjepideva toimimise taastamise võime pärast elutähtsa teenuse katkestust*. Riigikogus arutlusel oleva kriisiolukorra ja riigikaitse seaduse eelnõu § 23 lõikes 1 on toimepidevus defineeritud kui *püsiva kriisiülesandega asutuse ja isiku, sealhulgas elutähtsa teenuse osutaja ja kohaliku omavalitsuse üksus, ning põhiseadusliku institutsiooni suutlikkus ja valmidus järjepidevalt toimida ning igal ajal oma ülesandeid täita ja teenuseid osutada*.[12] Sõna „toimepidevus“ selgitab Eesti Keele Instituudi ühendsõnastik kui võimelisust, suutlikkust toimida edaspidi, jätkata alustatud tegevust.[13] Eelnõus on sõna „toimepidevus“ seotud võrgu- ja infosüsteemidega seotud toimepidevusega, mitte laiema toimepidevusega.
Riskianalüüsi puhul saab paralleeli tuua teatud üksuste[14] suhtes kohaldatavate nõuetega, mis on sätestatud NIS2-direktiivi artikli 21 lõike 5 alusel vastu võetud komisjoni rakendusmääruses

[9] Kuni 31.12.2025 kehtinud küberturvalisuse seaduse (RT I, 21.06.2024, 15) § 7 lõike 2 punkt 1:
(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:
1) koostama süsteemi riskianalüüsi, milles tuleb esitada süsteemi turvalisust ja teenuse toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu, määrata riskide realiseerumisel tekkiva küberintsidendi tagajärgede raskusaste ning kirjeldada küberintsidendi lahendamise abinõusid.
[10] https://akit.cyber.ee/term/711-infoturvarisk-turvarisk
[11] https://eits.ria.ee/et/abimaterjalid/seletav-soonaraamat
[12] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/679eeee7-62b9-4817-a660-745e6642a8d9/kriisiolukorra-ja-riigikaitse-seadus
[13] https://sonaveeb.ee/search/unif/dlall/dsall/toimepidevus/1/est
[14] Küberturvalisuse seaduse termineid kasutades on nendeks üksusteks: domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registrite pidajad, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalmeediaplatvormi pakkujad ja usaldusteenuse osutajad. Vt

(EL) 2024/2690,[15] konkreetsemalt selle rakendusmääruse artiklis 2 ja rakendusmääruse lisa punktides 1 ja 2 ning mõlema punkti alapunktides.
Ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati kõnealuse sätte kohta järgmine kommentaar (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), Riigi Infosüsteemi Ameti kommentaar nr 17.39):
Teeme ettepaneku sõnastada [küberturvalisuse seaduse eelnõu] § 7 lg 2 p 1-3 ja 9-14 järgmiselt: „(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud: 1) koostama ja rakendama infoturvariskide haldamise metoodika ja protseduurid; 2) koostama ja kehtestama infoturbe eesmärgid ja infoturvapoliitika; .. 14) viima läbi süsteemi riskihalduse protseduurid, mille käigus koostatakse süsteemi turvalisust mõjutavate riskide loetelu, määratakse riskide raskusaste ning kirjeldatakse ja rakendatakse riskikäsitlusmeetmed vastavalt rakendamise tähtaegadele. Selgitame: .. Väljend „Koostama ja kehtestama" on seotud plaani loomise ja ametliku kehtestamisega. Sõna „Teostama" viitab sellele, et varade haldamine toimub praktikas, järgitakse kehtestatud juhiseid ja toimingud viiakse ellu; 6) p 14 osas: antud paranduse eesmärk on parandada arusaadavust. Lisaks palume kaaluda punkti 1) asendamist siinse punktiga, kuna antud punkt juba katab ära 1) sisu, milles nõutav protseduur peaks seisnema. Vältimaks turvameetmete jäämist vaid plaanimise tasemele, siis on soovitav lisada ka rakendamise nõue. Seda viimast eriti olukorras, kus rakendusplaan riskikäsitlusmeetmetega saab olema võimalik koostada automaatselt. Sellisel juhul nõue saaks justkui täidetud, kuid turve ei paraneks, kui meetmete rakendamist ei toimu.
Eeltoodud kommentaari on kõnealuse sätte koostamisel arvestatud. Kommentaaris mainitud punkti 14 sisu on lisatud kõnealusesse sättesse. Eelnõu koostamise käigus kaaluti, kas kommenteeritava punkti alguses võiks kasutada sõna „riskianalüüs" asemel sõnu „riskihalduse protseduurid", kuid sellest loobuti, kuna küberturvalisuse seaduse § 7 lõike 1 punkt 1 sätestab teenuseosutaja kohustuse hallata riske, mis ohustavad teenuseosutaja tegevuses või teenuse osutamisel kasutatava süsteemi turvalisust, sealhulgas tuleb tal koostada vastav riskianalüüs. Kui kasutada kõnealuses lõikes muud sõna kui „riskianalüüs", siis ei pruugi olla selge, mil moel on viidatud seaduse punkt ja kõnealune lõige seotud.
Selle muudatuse kohta vt ka eelnõu § 2 punkt 13 ning selle selgitusi.

Paragrahvi 2 punktiga 10 muudetakse määruse nr 121 § 5 lõiget 4, võimaldades koostada sama määruse kolmanda peatüki 1. jaos olevaid dokumente ka muu õigusakti alusel koostatava dokumendi osana. Kehtiv säte kehtestab selle võimaluse ainult § 5 lõikes 1 sätestatud dokumentatsioonile, kuid muudatusega tehakse dokumentide koostamine teenuseosutajale paindlikumaks. Selle tulemusena võib teenuseosutaja näiteks koostada ühise dokumentatsiooni nii määruse nr 121 § 5 (turvameetmete dokumentatsioon) kui ka § 5^1 (esmased turvameetmed) ja sellega seotud sama määruse lisas ette nähtud nõuete täitmiseks.

Paragrahvi 2 punktiga 11 muudetakse määruse nr 121 § 5^1 lõiget 1. Küberturvalisuse seaduse § 7 lõige 6 viitab, et määruses nr 121 saab täpsustada alalisi asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ja korralduslikke turvameetmeid ning rakendamise nõudeid ja tingimusi, sealhulgas võib nende puhul võtta arvesse sama seaduse § 3 lõigetes 2–5 nimetatud

täpsemalt küberturvalisuse seaduse § 7 lõige 7 ja ülevõtmisseaduse eelnõu seletuskirjas selle lõike kohta esitatud selgitused.
[15] Rakendusakt jõustus 7. novembril 2024 ja on kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1730728447038; lisainfo aadressil https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en ja https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=PI_COM:Ares(2024)4640447&qid=1728309190768.

tegevusalasid. Kõnealuse muudatusega sätestatakse, et määruses nr 121 ette nähtud esmased turvameetmed ongi needsamad alalisse kasutusse võetavad nõuded.

Paragrahvi 2 punktiga 12 muudetakse määruse nr 121 § 5^1 lõike 1 punkti 4, asendades sõnad „tarnijate, väliste teenuste osutajate ja partnerite haldus“ sõnadega „väliste partnerite haldus“. Tegemist on tehnilise muudatusega.

Paragrahvi 2 punktiga 13 asendatakse määruse nr 121 lisa (edaspidi *lisa*), mis on seotud määruse §-s 5^1 nimetatud küberturvalisuse valdkondade täpsustamisega. Lisa asendatakse, et tagada selle sõnastuse selgus ning samal ajal ka võtta lõplikult üle NIS2-direktiivi artikli 21 lõiked 2 ja 3.
Ülevõtmisseaduse koostamisel lähtuti loogikast, et küberturvalisuse seaduse §-s 7 jäetakse alles teenuseosutaja võrgu- ja infosüsteemi suhtes kohaldatavatele turvameetmetele ette nähtud üldised nõuded. Turvameetmete definitsiooni kohta vt küberturvalisuse seaduse § 2 punkt 33. Täpsemad nõuded selle kohta, kuidas teenuseosutajad peavad turvameetmeid rakendama, nähakse ette määruses nr 121. Määruse nr 121 kohaldumise ulatust käsitleb küberturvalisuse seaduse § 7 lõige 7 – vt selle lõike selgitusi ülevõtmisseaduse eelnõu seletuskirjas.
Ülevõtmisseaduse eelnõu koostamise protsessis toimunud eelnõu kooskõlastusringi ja sellele eelnenud arutelude tulemusel otsustati, et kõik küberturvalisuse seaduse subjektid ei pea järgima Eesti infoturbestandardi või selle alternatiivina kasutatava rahvusvahelise standardi ISO/IEC 27001 või Eesti standardi EVS-EN ISO/IEC 27001 nõudeid ega allu selle kohustuse täitmisel välise auditeerimise nõudele,[16] vaid teatud teenuseosutajate suhtes kehtivad esmaste turvameetmete nõuded, võimaldades turvameetmete rakendamise täpse viisi valida teenuseosutajal endal. Seda käsitlust kõnesoleva eelnõuga ei muudeta.
Küberturvalisuse seaduse § 7 lõikes 1 nähakse ette üldine kohustus rakendada alaliselt turvameetmeid ja selle eesmärgid. Sama paragrahvi lõikes 2 nähakse ette, mida tuleb turvameetmete rakendamisel arvestada, sealhulgas võetakse selle lõikega üle ka NIS2-direktiivi artikli 21 lõike 2 sissejuhatav osa. Need nõuded kohalduvad ka kommenteeritavas lisas esitatud esmaste turvameetmete suhtes. Vt selle lõike selgitusi ülevõtmisseaduse eelnõu seletuskirjas. Ülevõtmisseadusega ei olnud kavas muuta küberturvalisuse seaduse § 7 lõiget 3 ega sama paragrahvi lõikes 5 sätestatud volitusnormi, kuid selle eelnõu menetlemise käigus lisati seaduse samasse paragrahvi lõige 6, mis täpsustab määrust nr 121 (vt ka eelnõu § 2 punktid 4 ja 5 ning nende selgitused).
Algselt kaaluti kõnesoleva eelnõu puhul eraldi paragrahvi loomist, mis võtaks üle NIS2-direktiivi artikli 21 lõigete 2 ja 3 sisu (alalised turvameetmed). Eelnõu koostamise käigus sellest reguleerimisvariandist loobuti, et ei tekiks segadust alaliste turvameetmete ja esmaste turvameetmete kattuvuse küsimuses. Kuna ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati ka tolle kavandatava paragrahvi kohta kommentaare, on lisa asjakohaste muudatuste selgituses vastavad kommentaarid ka esitatud.
NIS2-direktiivi artikli 21 lõikes 2, konkreetsemalt selle punktides, on sätestatud täpsemad alalised nõuded selle kohta, mida peavad turvameetmed hõlmama. Seetõttu sätestatakse kommenteeritavas lisas need tegevused ja asjaolud, mida teenuseosutaja peab turvameetme rakendamisel tegema või arvestama.
Kommenteeritava lisaga on seotud ennekõike NIS2-direktiivi põhjendused 77–86 ja 88–91 ning konkreetsemate üksuste (näiteks usaldusteenuse osutajad, sh kvalifitseeritud usaldusteenuse

[16] Vt eelnõude infosüsteemi toimikut 25-0715: Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine – https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6. Need muudatused jõustusid 1. oktoobril 2025.

osutajad, üldkasutatava elektroonilise side võrgu teenuse osutaja ja üldkasutatava elektroonilise side teenuse osutaja) puhul ka põhjendused 93–100:
(77) Vastutus võrgu- ja infosüsteemi turvalisuse tagamise eest lasub suurel määral elutähtsatel[17] ja olulistel üksustel. Tuleks edendada ja arendada riskijuhtimiskultuuri, mis hõlmab riskihindamisi ja riskile vastavate küberturvalisuse riskijuhtimismeetmete rakendamist.
(78) Küberturvalisuse riskijuhtimismeetmetes peaks võtma arvesse, mil määral elutähtis[18] või oluline üksus võrgu- ja infosüsteemidest sõltub, ning hõlmama meetmeid intsidendiriskide tuvastamiseks, vältimiseks, avastamiseks, neile reageerimiseks ja neist taastumiseks ning nende mõju leevendamiseks. Võrgu- ja infosüsteemide turvalisus peaks hõlmama salvestatavate, edastatavate ja töödeldavate andmete turvalisust. Küberturvalisuse riskijuhtimismeetmetega tuleks tagada süsteemne analüüs, milles võetakse arvesse inimtegurit, et saada võrgu- ja infosüsteemi turvalisusest terviklik pilt.
(79) Kuna võrgu- ja infosüsteemide turvalisust ähvardavatel ohtudel võib olla erinev põhjus, peaksid küberturvalisuse riskijuhtimismeetmed tuginema kõiki ohte hõlmavale käsitusele, mille eesmärk on kaitsta võrgu- ja infosüsteeme ja nende füüsilist keskkonda selliste olukordade eest nagu vargus, tulekahju, üleujutus, telekommunikatsiooni- või elektrikatkestus või loata füüsiline juurdepääs elutähtsa või olulise üksuse teabe- ja teabetöötlusrajatistele ning nende kahjustamine ja häirimine, mis võib ohustada võrgu- ja infosüsteemides salvestatud, edastatud või töödeldud andmete või nende süsteemide pakutavate või nende kaudu juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust. Seepärast peaksid küberturvalisuse riskijuhtimismeetmed käsitlema ka võrgu- ja infosüsteemide füüsilist turvalisust ja keskkonnaohutust, hõlmates selliste süsteemide kaitsmist süsteemirikete, inimliku eksimuse, pahatahtliku tegevuse või loodusnähtuste eest kooskõlas Euroopa ja rahvusvaheliselt tunnustatud standarditega, näiteks ISO/IEC 27000 seeria standarditega. Sellega seoses peaksid elutähtsad[19] ja olulised üksused oma küberturvalisuse riskijuhtimismeetmete osana käsitlema ka personali turvalisust ja kehtestama asjakohased juurdepääsukontrolli põhimõtted. Need meetmed peaksid olema kooskõlas [CER-direktiiviga].
(80) Selleks et tõendada vastavust küberturvalisuse riskijuhtimismeetmetele ja kui puuduvad Euroopa Parlamendi ja nõukogu määrusele (EL) 2019/881 vastavad asjakohased Euroopa küberturvalisuse sertifitseerimise kavad, peaksid liikmesriigid konsulteerides koostöörühma ja Euroopa küberturvalisuse sertifitseerimise rühmaga edendama asjaomaste Euroopa ja rahvusvaheliste standardite kasutamist elutähtsate[20] ja oluliste üksuste poolt, või liikmesriigid võivad üksustelt nõuda, et nad kasutaksid sertifitseeritud IKT-tooteid, IKT-teenuseid ja IKT-protsesse.
(81) Et vältida elutähtsatele[21] ja olulistele üksustele ebaproportsionaalse finants- ja halduskoormuse panemist, peaksid küberturvalisuse riskijuhtimismeetmed olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riski tasemega ning lähtuma selliste meetmete tehnilisest tasemest ning, kui see on kohaldatav, Euroopa ja rahvusvahelistest standarditest ning nende rakendamise kuludest.
(82) Küberturvalisuse riskijuhtimismeetmed peaksid olema proportsionaalsed elutähtsa[22] või olulise üksuse riskidele avatuse määraga ning intsidendi ühiskondliku ja majandusliku mõjuga. Elutähtsatele[23] ja olulistele üksustele kohandatud küberturvalisuse riskijuhtimismeetmete

[17] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulistel üksustel“.
[18] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliololuline üksus“.
[19] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[20] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliololiste üksuste“.
[21] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulistele üksustele“.
[22] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuse“.
[23] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulistele üksustele“.

kehtestamisel tuleks igakülgselt arvesse võtta elutähtsate[24] ja oluliste üksuste erinevat avatust riskidele, näiteks üksuse kriitilisuse määra, riske, sealhulgas ühiskondlikke riske, millega ta kokku puutub, üksuse suurust, intsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.

(83) Elutähtsad[25] ja olulised üksused peaksid tagama oma tegevuses kasutatavate võrgu- ja infosüsteemide turvalisuse. Nende puhul on eelkõige tegemist privaatsete võrgu- ja infosüsteemidega, mida haldavad kas elutähtsa[26] või olulise üksuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. [NIS2-direktiivis] sätestatud küberturvalisuse riskijuhtimismeetmeid ning teatamiskohustust tuleks kohaldada asjaomaste elutähtsate[27] ja oluliste üksuste suhtes olenemata sellest, kas kõnealused üksused hooldavad oma võrgu- ja infosüsteeme ise või tellivad selleks hooldusteenuse väljast.

(84) Võttes arvesse nende piiriülest olemust, tuleks domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite[28], pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate[29], hallatud teenuse osutajate[30], turbetarnijate[31], internetipõhise kauplemiskohtade[32], internetipõhiste otsingumootorite[33], sotsiaalvõrguteenuse platvormi pakkujate[34] ja usaldusteenuse osutajate suhtes kohaldada liidu tasandil suuremat ühtlustamist. Seetõttu tuleks küberturvalisuse riskijuhtimismeetmete rakendamise hõlbustamiseks seoses kõnealuste üksustega võtta vastu rakendusakt.

(85) Eriti oluline on tegeleda riskidega, mis tulenevad üksuse tarneahelast ja suhetest tema tarnijatega, näiteks andmete talletamise ja töötlemise teenuse osutajate või turbeteenuse osutajate ja sisutoimetajatega, kui võtta arvesse selliste intsidentide esinemise sagedust, mille puhul üksused on langenud võrgu- ja infosüsteemi vastu suunatud küberrünnete ohvriks ning kurjategijad on suutnud kahjustada üksuse võrgu- ja infosüsteemide turvalisust, kasutades ära kolmandate isikute tooteid ja teenuseid mõjutavaid nõrkusi. Seepärast peaksid elutähtsad[35] ja olulised üksused hindama ja arvesse võtma toodete ja teenuste üldist kvaliteeti ja vastupidavust, nendesse integreeritud küberturvalisuse riskijuhtimismeetmeid, samuti oma tarnijate ja teenuseosutajate[36] küberturvalisuse tavasid, sealhulgas nende turvalise arenduse menetlusi. Elutähtsaid[37] ja olulisi üksusi tuleks eelkõige julgustada lisama küberturvalisuse riskijuhtimismeetmeid oma otseste tarnijate ja teenuseosutajatega sõlmitavatesse lepingutesse. Kõnealused üksused võiksid võtta arvesse ka riske, mis tulenevad muu tasandi tarnijatest ja teenuseosutajatest.

(86) Teenuseosutajate seas on intsidentide ennetamisel, tuvastamisel, lahendamisel ja neist taastumisel üksuste jaoks eriti oluline tugiroll turbetarnijatel[38] sellistes teenusevaldkondades

---

[24] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuste“.
[25] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[26] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuse“.
[27] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuste“.
[28] Ülevõtmisseaduse kohases küberturvalisuse seaduses „tippdomeeninimede registrite pidajad“.
[29] Ülevõtmisseaduse kohases küberturvalisuse seaduses „sisulevivõrguteenuse osutajate“.
[30] Ülevõtmisseaduse kohases küberturvalisuse seaduses „haldusteenuse osutajate“.
[31] Ülevõtmisseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajate“.
[32] Ülevõtmisseaduse kohases küberturvalisuse seaduses „internetipõhiste kauplemiskohtade pidajate“.
[33] Ülevõtmisseaduse kohases küberturvalisuse seaduses „veebipõhise otsingumootori pakkujate“.
[34] Ülevõtmisseaduse kohases küberturvalisuse seaduses „sotsiaalmeediaplatvormi pakkujate“.
[35] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[36] Siin ei ole pigem mõeldud ülevõtmisseaduse kohase küberturvalisuse seaduse § 3 lõikes 1 kasutatavat terminit „teenuseosutaja“, vaid neid üksusi, kes selle seaduse kohaldamisalasse kuuluvale üksusele teenust osutavad. Samas võivad sellisteks üksusteks olla nt ka ülevõtmisseaduse järgse küberturvalisuse seaduse kohased haldusteenuse osutajad või infoturbeteenuse osutajad. See märkus käib ka käesoleva tekstilõigu kahe järgmise lause kohta.
[37] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliololulisi üksusi“.
[38] Ülevõtmisseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajatel“.

nagu intsidentide lahendamine, läbistustestimine, turvaaudit ja konsultatsioonid. Turbetarnijad[39] on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on üksuste tegevusse tihedalt lõimitud, kaasneb nendega eriline risk. Seega peaksid elutähtsad[40] ja olulised üksused olema turbetarnija[41] valimisel iseäranis hoolikad.

(88) Elutähtsad[42] ja olulised üksused peaksid tähelepanu pöörama ka sellistele riskidele, mis tulenevad nende suhtlemisest ja suhetest teiste sidusrühmadega laiemas ökosüsteemis, et muu hulgas tõkestada tööstusspionaaži ja kaitsta ärisaladusi. Täpsemalt peaksid üksused võtma asjakohaseid meetmeid tagamaks, et nende koostöö akadeemiliste ja teadusasutustega toimub kooskõlas nende küberturvalisuse poliitikaga ning et selles koostöös järgitakse teabele turvalise juurdepääsu ja selle levitamisega seotud üldisi häid tavasid ja eelkõige intellektuaalomandi kaitsega seotud tavasid. Võttes arvesse andmete olulisust ja väärtust elutähtsate[43] ja oluliste üksuste tegevuse jaoks, peaksid kõnealused üksused kolmandate isikute poolt osutatavatele andmete teisendamise ja analüüsi teenustele tuginedes võtma kõik asjakohased küberturvalisuse riskijuhtimismeetmed.

(89) Elutähtsad[44] ja olulised üksused peaksid kasutusele võtma mitmesugused küberhügieeni põhitavad, näiteks usaldamatuse põhimõtte, tarkvarauuendused, seadme konfiguratsiooni, võrgu segmenteerimise, identiteedi ja juurdepääsu halduse ning kasutajateadlikkuse, ning pakkuma oma töötajatele koolitusi ning suurendama teadlikkust küberohtude, andmepüügi ja inimestega manipuleerimise meetodite kohta. Lisaks peaksid kõnealused üksused hindama oma küberturvalisuse võimekust ning püüdma võtta asjakohasel juhul kasutusele küberturvalisust suurendavad tehnoloogiad, näiteks tehisintellekti või masinõppesüsteemid, et suurendada oma võimekust ning võrgu- ja infosüsteemide turvalisust.

(90) Et käsitleda põhjalikumalt peamisi tarneahelariske ning aidata asjakohaselt juhtida [NIS2-direktiivi] kohaldamisalasse kuuluvates sektorites tegutsevatel elutähtsatel[45] ja olulistel üksustel tarneahela ja tarnijatega seotud riske, peaks koostöörühm tegema koostöös komisjoni ja ENISAga ning asjakohasel juhul pärast asjakohaste sidusrühmadega, sealhulgas tööstusega konsulteerimist koordineeritud kriitilise tähtsusega tarneahelate turberiski hindamise (nagu tehti 5G-võrkude kohta vastavalt soovitusele (EL) 2019/534 (5G-võrkude küberturvalisuse kohta)), eesmärgiga määrata iga sektori jaoks kindlaks kriitilise tähtsusega IKT-teenused, IKT-süsteemid või IKT-tooted, asjaomased ohud ja nõrkused. Sellise turberiski koordineeritud hindamise käigus tuleks kindlaks teha meetmed, leevenduskavad ja parimad tavad, millega võidelda kriitilise tähtsusega sõltuvuse vastu, potentsiaalsete nõrkade lülide, ohtude, nõrkuste[46] ja muude riskide vastu, mis on seotud tarneahelaga, ning uurida, kuidas saaks elutähtsaid[47] ja olulisi üksusi julgustada neid ulatuslikumalt kasutusele võtma. Võimalikud muud kui tehnilised riskitegurid, nagu kolmanda riigi lubamatu mõju tarnijatele ja teenuseosutajatele, eelkõige alternatiivsete juhtimismudelite puhul, hõlmavad varjatud nõrkusi[48] või tagauksi ja võimalikke süsteemseid tarnehäireid, eriti tehnoloogilise kinnistumise või teenuseosutajast sõltuvuse korral.

(91) Kriitilise tähtsusega tarneahela turberiskide koordineeritud hindamisel tuleks asjaomase sektori omadusi silmas pidades võtta arvesse nii tehnilisi kui ka asjakohasel juhul muid kui

---

[39] Ülevõtmisseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajad“.
[40] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[41] Ülevõtmisseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutaja“.
[42] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[43] Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.
[44] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.
[45] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulistel üksustel“.
[46] Ülevõtmisseaduse kohases küberturvalisuse seaduses „turvahaavatavuste“.
[47] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulisi üksusi“.
[48] Ülevõtmisseaduse kohases küberturvalisuse seaduses „turvahaavatavusi“.

tehnilisi tegureid, sealhulgas neid, mis on kindlaks määratud soovituses (EL) 2019/534, 5G-võrkude küberturvalisusega seotud ELi koordineeritud riskihindamist käsitlevas aruandes ja koostöörühma kokkulepitud ELi 5G-küberturvalisuse meetmepaketis. Et teha kindlaks tarneahelad, mille suhtes peaks kohaldama turberiski koordineeritud hindamist, tuleks arvesse võtta järgmisi kriteeriume: i) kui suurel määral elutähtsad[49] ja olulised üksused kindlaid kriitilise tähtsusega IKT-teenuseid, IKT-süsteeme või IKT-tooteid kasutavad ning nendele tuginevad; ii) kindlate kriitilise tähtsusega IKT-teenuste, IKT-süsteemide või IKT-toodete asjakohasus kriitilise tähtsusega või tundlike funktsioonide (sealhulgas isikuandmete töötlemine) täitmisel; iii) alternatiivsete IKT-teenuste, IKT-süsteemide või IKT-toodete kättesaadavus; iv) IKT-teenuste, IKT-süsteemide või IKT-toodete tarneahela kui terviku vastupidavusvõime kogu nende olelusringi jooksul häirivate sündmuste korral või v) kui tegemist on kujunemisjärgus IKT-teenuste, IKT-süsteemide või IKT-toodetega, siis nende potentsiaalne tulevane tähtsus üksuste tegevuse jaoks. Lisaks tuleks erilist tähelepanu pöörata IKT-teenustele, IKT-süsteemidele või IKT-toodetele, mille suhtes kehtivad kolmandatest riikidest tingitud erinõuded.

(93) [NIS2-direktiivis] sätestatud küberturvalisuse kohustusi tuleks käsitada täiendusena nõuetele, mis on kehtestatud usaldusteenuse osutajatele määrusega (EL) nr 910/2014. Usaldusteenuse osutajatelt tuleks nõuda, et nad võtaksid kõik asjakohased ja proportsionaalsed meetmed, et juhtida oma teenuseid ohustavaid riske, sealhulgas seoses klientide ja teenustest sõltuvate kolmandate isikutega, ning teataksid [NIS2-direktiivi] kohaselt intsidentidest. Sellised küberturvalisuse kohustused ja teatamiskohustus peaksid hõlmama osutatavate teenuste füüsilist kaitset. Määruse (EL) nr 910/2014 artiklis 24 kvalifitseeritud usaldusteenuse osutajate suhtes sätestatud nõudeid kohaldatakse ka edaspidi.

(94) Liikmesriigid võivad määrata usaldusteenuste eest vastutavaks pädevaks asutuseks määruse (EL) nr 910/2014 kohase järelevalveasutuse, et tagada praeguste tavade jätkumine ning kasutada nimetatud määruse kohaldamisel saadud teadmisi ja kogemusi. Sellisel juhul peaksid [NIS2direktiivi] kohased pädevad asutused tegema tihedalt ja aegsasti koostööd kõnealuste järelevalveasutustega, vahetades asjakohast teavet, et tagada tulemuslik järelevalve ja see, et usaldusteenuse osutajad täidavad [NIS2-direktiivis] ja määruses (EL) nr 910/2014 sätestatud nõudeid. Kui see on kohaldatav, peaks CSIRT või käesoleva direktiivi kohane pädev asutus viivitamata teavitama määruse (EL) nr 910/2014 kohast järelevalveasutust igast teatatud olulisest küberohust või intsidendist, mis mõjutab usaldusteenuseid, ning igast [NIS2-direktiivi] rikkumisest usaldusteenuse osutaja poolt. Liikmesriigid võivad, kui see on kohaldatav, kasutada teatamiseks ühtset kontaktpunkti, mis on loodud selleks, et tagada ühtne ja automaatne intsidentidest teatamine nii määruse (EL) nr 910/2014 kohasele järelevalveasutusele kui ka [NIS2-direktiivi] kohasele CSIRTile või pädevale asutusele.

(95) Kui see on asjakohane ja et vältida tarbetuid häireid, tuleks [NIS2-direktiivi ülevõtmisel arvesse võtta olemasolevaid riiklikke suuniseid, mis on võetud vastu direktiivi (EL) 2018/1972 artiklites 40 ja 41 sätestatud turvameetmetega seotud normide ülevõtmiseks, tuginedes seega teadmistele ja oskustele, mis on direktiivi (EL) 2018/1972 alusel seoses turvameetmete ja intsidenditeadetega juba omandatud. ENISA võib koostada üldkasutatavate elektroonilise side võrkude pakkujate[50] või üldkasutatavate elektrooniliste side teenuste osutajate jaoks ka turvanõudeid ja teatamiskohustust käsitlevad suunised, et hõlbustada ühtlustamist ja üleminekut ning minimeerida häireid. Liikmesriigid võivad anda elektroonilise side eest vastutava pädeva asutuse rolli direktiivi (EL) 2018/1972 kohastele riigi reguleerivatele asutustele, et tagada praeguste tavade jätkumine ning kasutada nimetatud direktiivi rakendamisel saadud teadmisi ja kogemusi.

[49] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused".

[50] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üldkasutatava elektroonilise side võrgu teenuse osutajate".

(96) Võttes arvesse, et direktiivis (EL) 2018/1972 määratletud numbrivaba isikutevahelise side teenuste olulisus kasvab, tuleb tagada, et ka nende teenuste kohta kehtiksid asjakohased, nende eripära ja majanduslikku tähtsust arvestavad turvanõuded. Ründepinna üha laienedes muutuvad levinud sihtmärkideks numbrivaba isikutevahelise side teenused, näiteks sõnumiteenused. Kurjategijad kasutavad platvorme suhtlemiseks ja selleks, et meelitada ohvreid avama nakatatud veebisaite, suurendades seeläbi isikuandmete ärakasutamise ja laiemalt ka infosüsteemide turvalisusega seotud intsidentide esinemise tõenäosust. Numbrivaba isikutevahelise side teenuste pakkujad peaksid tagama riskitasemele vastava võrgu- ja infosüsteemide turvalisuse taseme. Arvestades, et numbrivaba isikutevahelise side teenuste osutajatel puudub tavaliselt tegelik kontroll võrkudes signaalide edastamise üle, võib selliste teenustega seotud riske pidada mõnes mõttes väiksemaks kui riske, mis esinevad tavapäraste elektroonilise side teenuste puhul. Sama kehtib ka selliste direktiivis (EL) 2018/1972 määratletud isikutevahelise side teenuste kohta, mille puhul kasutatakse numbreid ja millel puudub tegelikult kontroll signaaliedastuse üle.

(97) Siseturg sõltub interneti toimimisest rohkem kui kunagi varem. Peaaegu kõigi elutähtsate[51] ja oluliste üksuste teenused sõltuvad interneti kaudu pakutavatest teenustest. Et tagada elutähtsate[52] ja oluliste üksuste pakutavate teenuste sujuv osutamine, on oluline, et kõikidel üldkasutatavate elektroonilise side võrkude pakkujatel[53] oleksid asjakohased küberturvalisuse riskijuhtimismeetmed ja et nendega seotud olulistest intsidentidest teataks. Liikmesriigid peaksid tagama üldkasutatavate elektroonilise side võrkude turvalisuse säilimise ning oma eluliste julgeolekuhuvide kaitse sabotaaži ja spionaaži eest. Kuna rahvusvaheline ühenduvus edendab ja kiirendab liidu ja selle majanduse konkurentsipõhist digitaliseerimist, tuleks merealuseid sidekaableid mõjutavatest intsidentidest teavitada CSIRTi või, kui see on kohaldatav, pädevat asutust. Kui see on asjakohane, tuleks merealuste sidekaablite küberturvalisust riiklikus küberturvalisuse strateegias arvesse võtta ning see peaks hõlmama võimalike küberturvalisuse riskide kaardistamist ja leevendusmeetmeid, et tagada nende kaitse kõrgeimal tasemel.

(98) Üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste turvalisuse tagamiseks tuleks edendada krüpteerimistehnoloogiate kasutamist, eelkõige otspunktkrüpteerimist ja andmekeskseid turbekontseptsioone, nagu kartograafia, segmenteerimine, märgistamine, juurdepääsupoliitika ja juurdepääsu haldamine ning automatiseeritud juurdepääsu otsused. Vajaduse korral peaks üldkasutatavate elektroonilise side võrkude pakkujatele[54] või üldkasutatavate elektroonilise side teenuste osutajatele olema [NIS2-direktiivi] kohaldamisel kohustuslik kasutada krüpteerimist, eelkõige otspunktkrüpteerimist, kooskõlas turbe ja privaatsuse vaikesätteid ja sisseprojekteerimist käsitlevate põhimõtetega. Otspunktkrüpteerimise kasutamine tuleks ühildada liikmesriikide volitustega tagada nende oluliste julgeolekuhuvide ja avaliku julgeoleku kaitse ning võimaldada kuritegude ennetamist, uurimist, avastamist ja nende eest vastutusele võtmist kooskõlas liidu õigusega. Sellega ei tohiks aga kaasneda otspunktkrüpteerimise nõrgestamine, kuna see on tõhusa andmekaitse, privaatsuse ja side turvalisuse jaoks olulise tähtsusega tehnoloogia.

(99) Üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste turvalisuse tagamiseks ning nende kuritarvitamise ja manipuleerimise vältimiseks tuleks

---

[51] Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

[52] Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

[53] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üldkasutatava elektroonilise side võrgu teenuse osutajatel“.

[54] Ülevõtmisseaduse kohases küberturvalisuse seaduses „üldkasutatava elektroonilise side võrgu teenuse osutajatele“.

edendada koostalitlusvõimeliste turvaliste marsruutimisstandardite kasutamist, et tagada marsruutimisfunktsioonide terviklus ja töökindlus kogu internetiühenduse teenuse osutajate ökosüsteemis.
(100) Et kaitsta interneti funktsionaalsust ja terviklust ning edendada domeeninimede süsteemi turvalisust ja vastupanuvõimet, tuleks asjaomaseid sidusrühmi, sealhulgas liidu erasektori üksusi, üldkasutatavate elektroonilise side teenuste osutajaid, eelkõige internetiühenduse teenuse osutajaid, ja internetipõhise otsingumootori teenuse osutajaid[55]*, innustada võtma vastu domeeninimede süsteemi teisendamise mitmekesistamise strateegia. Ühtlasi peaksid liikmesriigid innustama avaliku ja turvalise Euroopa domeeninimede süsteemi teisendamise teenuse väljatöötamist ja kasutamist.*
NIS2-direktiivi artikli 21 lõike 2 punktides sätestatud nõuded on sisuliselt samad, mida näeb ette küberturvalisuse seaduse § 7 lõike 5 alusel kehtestatud Eesti infoturbestandard (edaspidi *E-ITS*)[56] või rahvusvaheline standard ISO/IEC 27001:2002. Seda illustreerib tabel 1.
Tabel 1. NIS2-direktiivi artikli 21 lõigete 1–3 võrdlus Eesti infoturbestandardiga (E-ITS) ja rahvusvahelise standardiga ISO/IEC27001:2002

Art 21 lõige 1	E-ITSi moodul põhitasemel	E-ITSi moodul standardtasemel	Kommentaar E-ITSi kohta	ISO/IEC27001:2022
Terve lõige	E-ITS	E-ITS	E-ITSi puhul tuleneb proportsionaalsus just selle modulaarsest ise-loomust ja astmelisusest. Liikmesriik saab kehtestada enda standardid või standardsed nõuded, et eesmärki saavutada, nt E-ITSi või nõude kasutada ISO/IEC27001	Kuna see on liikmesriigi tegevus, siis otsest vastet pole, kuid liikmesriik saab kehtestada enda standardid või standardsed nõuded, et eesmärki saavutada, nt E-ITSi või nõude kasutada ISO/IEC27001
Terve lõige	ORP	ORP	Kui üksus nõuab meetmeid oma tarneahela partneritelt, siis on vastavalt varadele võimalik samuti meetmed võtta otse E-ITSist	Üksus võib rakendada meetmeid, lähtudes esitatud nõuetest ISO/IEC27001 vastavussertifikaadi asjakohase käsitlusalaga
Terve lõige			E-ITSi meetmete regulaarne uuendamine peab tagama nende vastavuse küberintsidentidele ja uutele tehnoloogiatele. E-ITSi uuendamisega tegelebki Riigi Infosüsteemi Amet	ISO/IEC27001 uuendamine ei võta arvesse Eesti eripärasid. Läbivaatuse tsükkel on umbes 5 aastat. Üksus peab ise lähtuma

[55] Ülevõtmisseaduse kohases küberturvalisuse seaduses „veebipõhise otsingumootori pakkujaid".
[56] Kättesaadav ettevõtlus- ja infotehnoloogiaministri 16.12.2022 määruse nr 101 „Eesti infoturbestandard" lisadest (vt https://www.riigiteataja.ee/akt/130012024007?leiaKehtiv) või Eesti infoturbestandardi portaalist https://eits.ria.ee/.

				riskianalüüsist ja arvestama ühiskonnas ja küberruumis toimuvat oma meetmete uuendamisel, soovitavalt lähtuma Riigi Infosüsteemi Ameti soovitustest ja seega ka E-ITSi uuendustest
Art 21 lõige 2	E-ITSi moodul põhitasemel	E-ITSi moodul standardtasemel	Kommentaar E-ITSi kohta	ISO/IEC27001:2022
Punkt a	ISMS, ORP, OPS, DER, APP, SYS, INF	ISMS, ORP, OPS, CON, DER, APP, SYS, IND	Meetmed on jaotunud kõigisse protseduurilistesse moodulitesse, osad täpsustused ja sõltuvalt kasutatavatest varadest süsteemi moodulites	Põhiosa 5.2, 6.1, 10 Läbivalt kogu lisa A. A5.1, A5.8, A5.12, A5.13, A5.31, A5.32, A5.33, A5.34, A5.36, A7.1, A8.11,
Punkt b	OPS, DER, ORP	OPS, DER, IND, NET, INF	Põhisisu OPSi ja DERi moodulites	A5.5, A5.6, A5.24, A5.25, A5.26, A2.27, A5.28, A5.29, A6.8, A8.16,
Punkt c	CON, OPS, DER, APP, SYS, IND, NET, INF	CON, OPS, DER, APP, SYS, IND, NET, INF	Põhisisu CONi, OPSi ja DERi moodulites, teistes täpsustused varade põhiselt	A5.5, A5.6, A5.29, A5.30, A7.5, A8.13
Punkt d	ISMS, OPS, CON, DER, APP, SYS, IND, NET, INF	OPS, CON, APP, IND, INF	Põhisisu OPSi moodulis, teistes täpsustused	Põhiosa 4.2 A5.14, A5.19, A5.20, A5.21, A5.22, A5.23, A5.37, A8.30
Punkt e	CON, OPS, DER, APP,	CON, OPS, DER, APP,	Protseduurilised teemad valdavalt CONi ja OPSi moodulites, muudes moodulites täpsustused;	Põhiosa 4.2 A5.7, A5.8, A5.23, A7.11, A7.12, A7.13, A7.14, A8.1, A8.6,

	SYS, IND, NET, INF	SYS, IND, NET, INF	DER lisab nõrkuse halduse, mis kajastub ka varapõhistes moodulites	A8.8, A8.9, A8.10, A8.12, A8.14, A8.16, A8.18, A8.19, A8.20, A8.21, A8.22, A8.23, A8.25, A8.26, A8.27, A8.28, A8.29, A8.30, A8.31, A8.32, A8.33, A8.34
Punkt f	ISMS, CON, DER, INF	ORP, DER, SYS, IND, NET, INF	Riskipõhist tegutsemist eeldab just infoturbe tervikhaldus ning etalonturve on selle üks osa	Põhiosa 9, 10 A5.35, A5.36, A7.4, A8.15, A8.16, A8.17, A8.34
Punkt g	ORP, CON, OPS, SYS, NET, INF	ORP, OPS, DER, APP, NET, INF	Koolitused ORPi moodulis, kuid mujal moodulites on täpsustused teemade kohta, mis vajavad eraldi koolitust	Põhiosa 7.3 A5.17, A5.37, A6.3, A6.4, A6.7, A6.8, A7.6, A7.7, A8.1
Punkt h	CON, OPS, APP, SYS, NET	ISMS, ORP, CON, OPS, APP, SYS, NET	Üldine krüptograafia kajastatud CONi moodulis; muudes moodulites spetsiifilised täpsustused sõltuvalt konkreetsematest kasutuskohtadest	A8.1, A8.24
Punkt i	ISMS, ORP, CON, OPS, APP, SYS, IND, NET, INF	ORP, CON, OPS, APP, SYS, IND, NET, INF	Pääsuhaldus katab pea kõiki mooduleid, põhiline ORPis	Põhiosa 5.3 A5.2, A5.3, A5.9, A5.10, A5.11, A5.15, A5.16, A5.18, A6.1, A6.2, A6.5, A6.6, A6.7, A7.2, A7.3, A7.6, A7.8, A7.9, A7.10, A7.14, A8.2, A8.3, A8.4, A8.5
Punkt j	ORP, OPS, APP, SYS	ORP, CON, OPS, APP, SYS, NET	Mitmikautentimise lahenduse (ehk MFA) kasutamise ning ühendatud side- ja koostöölahenduste (ehk UCC) teemad kajastatud kasutuskohtades ja ORPi moodulis	A8.1
Art 21 lõige 3	E-ITSi moodul põhitasemel	E-ITSi moodul standardtasemel	Kommentaar E-ITSi kohta	ISO/IEC27001:2022
Terve lõige	OPS	OPS	On kaetud OPSi mooduliga	Põhiosa 4.2

				A5.14, A5.19, A5.20, A5.21, A5.22, A5.23, A5.37, A8.30

Eeltoodud tabel on esitatud selleks, et selgitada NIS2-direktiivi artikli 21 lõigete 2 ja 3 ning E-ITSi ja rahvusvaheline standardi ISO/IEC 27001:2002 vahelist seost. See on abiks neile teenuseosutajatele, kellel ei ole võimalik piirduda ainult esmaste turvameetmetega ehk kes peavad rakendama kas E-ITSi või selle alternatiive (vt määruse nr 121 § 3 lõiked 2–3). Lisaks abistab see ka neid teenuseosutajaid, kes peavad määruse nr 121 § 3 lõike 2^1 kohaselt rakendama ainult esmaseid turvameetmeid, kuid kes siiski soovivad vabatahtlikult lähtuda detailsematest nõuetest ehk E-ITSist või selle alternatiivsetest standarditest. Siiski tuleb arvestada, et nii E-ITS kui ka mainitud rahvusvaheline standard on oma sisu ja nõuete poolest tunduvalt detailsem kui kommenteeritav lisa ja selles sätestatud esmased turvameetmed.
Riigi Infosüsteemi Ameti teenistujate osalusel on arendamisel ka E-ITSi järgimise tugirakendus, mis aitab rakendajal luua vajaduspõhist turvameetmete rakendusplaani, seejuures vähendada vigu meetmete valimisel, ja suunab rakendaja kohe meetmete rakendamisele. Tugirakenduse eesmärk on vähendada E-ITSi rakendamise protsessi keerukust. See on interaktiivne rakendusjuhend, mis aitab läbida infoturbehalduse protsessi teatud etappe ning annab võimaluse olla standardi kataloogi uuendustega pidevalt kursis. Seejuures säilib siiski kogu standardi olemus ning meetmetes järeleandmisi ei tehta – küberruumi olukord nõuab vähemalt põhimeetmete rakendamist, NIS2-direktiivi artikli 21 nõuded on seejuures kõikehõlmavad. Riigi Infosüsteemi Amet ei hakka organisatsioonide turvet haldama ega haldamisteavet hoidma. Amet tegeleb E-ITSi arendamisega ja püüab leida lahendusi, et aidata rakendajal leida E-ITSist oma organisatsioonile võimalikult ressursse säästvalt õiged meetmed, kuid teenuseosutaja peab neid oma tööriistadega rakendama ja haldama. E-ITSi tugirakenduse leiab siit: https://eits.ria.ee/et/abimaterjalid/tugirakendus. E-ITSi juhendid on asjakohases portaalis, vt https://eits.ria.ee/et/avalehe-menueue/koolitusvideod, https://eits.ria.ee/et/avalehe-menueue/juhendid, https://eits.ria.ee/et/avalehe-menueue/kogukond ja https://eits.ria.ee/et/avalehe-menueue/suendmused.

Kuna kommenteeritavas lisas on täpsustatud esmaste turvameetmete sisu, siis võrreldakse järgnevalt ka NIS2-direktiivi artikli 21 lõigete 1–3 sisu ja esmaseid turvameetmeid. Lisa sätete vastavus Euroopa Liidu õigusele on toodud seletuskirja punktis 3.

Eelnõu koostamisel otsustati asendada määruse nr 121 kehtiv lisa tervikuna, et tagada lisa kui terviku komplektsus. See ei tähenda siiski, et kõik lisa punktid on muudetud. Käesolevas seletuskirjas selgitatakse ainult kommenteeritava lisa neid punkte, mida muudetakse.

Ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati kommentaar kogu lisa kohta. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit esitas järgmise kommentaari (vt eelnõu nr 739 SE seletuskirja lisa 3 (märkuste tabel). kommentaar nr 24.48): *Eelnõu § 1 p 26 – KüTS § 7 lg 2 […] Teeme ettepaneku tõlkida turvameetmete nimekiri täpselt NIS2-direktiivist, praegu on tekitatud meetmeid juurde sõnastuste muudatustega. Isegi kui need on väikesed ning sisuliselt on proovitud osa teemasid lahti lüüa eraldi punktideks.* Kõnesoleva eelnõu puhul ongi lähtutud ennekõike NIS2-direktiivi sõnastusest. Samas ei soovita selle eelnõuga hakata esmaste turvameetmete sisu kardinaalselt ümber sõnastama, vaid selle asemel täiendatakse lisa neid punkte, mida vaja, et NIS2-direktiiv saaks üle võetud.

Lisas asendatakse läbivalt sõnad „teenuse osutaja“ sõnaga „teenuseosutaja“. Vt eelnõu § 2 punkt 1 ja selle selgitus. Lisas tehakse ka lisaks järgnevalt selgitatud muudatustele ka muid

tehnilisi muudatusi (lisa punktid 3.4, 6.1, 6,4 ja 7.3), mille eesmärk on järgida õigusaktide normitehnika sõnastuse põhimõtteid ja tagada lausete sõnastuste selgus.

Lisa punkti 4 pealkirja muudetakse, lähtuvalt määruse teksti § 2 punktis 12 tehtavast muudatusest (määruse nr 121 § 5^1 lõike 1 punkti 4 muutmine).

Lisa punktis 7.3 asendatakse sõna „nõrkuste“ sõnaga „turvahaavatavuste“. Muudatuse põhjuseks on soov viia terminikasutus kooskõlla küberturvalisuse seaduse § 2 punktis 31 defineeritud terminiga „turvahaavatavus“. Samuti parandati lause sõnastust. Mõlema muudatuse puhul on tegemist tehnilise muudatusega.

Lisa punktis 7.4 tehakse tehniline muudatus, asendades lause lõpus olev sõna „ja“ sõnaga „või“. Tolle punkti puhul on praegu võimalik välja lugeda, et tarkvara peab kasutusest eemaldamiseks olema nii aegunud kui ka kasutust mitteleidev. See tähendab, et eemaldamiseks peavad mõlemad tingimused olema korraga täidetud, st tarkvara ei kasutata ja see on aegunud, kuid kui seda kasutatakse, olenemata sellest, et see on aegunud, siis seda kasutuselt eemaldama ei pea. See tähendaks, et kui üks tingimustest on täitmata, siis meedet rakendama ei pea. Tegelikkuses on tolle punkti puhul algusest saadik mõeldud, et tarkvara eemaldamiseks on alus, kui korraga kehtib vähemalt üks kahest nimetatud tingimusest. Seetõttu on tolle punkti lõpu sõnastus edaspidiselt: *.. tarkvara, mis on aegunud või mida ei kasutata*. Praktikas võib olla edaspidi ka nii, et jätkuvalt on mõlemad tingimused täidetud.

Paragrahv 2 punktiga 14 täiendatakse määrust nr 121 normitehnilise märkusega, lisades viite NIS2-direktiivile.
Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 27 lõike 3 esimene lause näeb ette, et kui seaduseelnõu koostatakse Euroopa Liidu õiguse ülevõtmiseks, siis nimetatakse normitehnilises märkuses Euroopa Liidu õigusakti andja või andjad, akti liik, number, pealkiri ja avaldamismärge. Sama määruse § 51 kohaselt kehtib nimetatud põhinõue ka Vabariigi Valitsuse määruse ja ministri määruse eelnõu kohta.
Normitehniline märkus lisatakse määrusesse nr 121, kuna muudesse õigusaktidesse pole NIS2-direktiivi artikli 21 lõikeid 2 ja 3 üle võtvaid sätteid kavandatud.

Paragrahviga 3 muudetakse määrust nr 1. Paragrahv koosneb kahest punktist.
Tegemist on ennekõike tehnilise muudatusega, mille eesmärk on tagada üksuste õigesti nimetamine muudetavas lõikes. Muudatus on tingitud ülevõtmisseadusest, kuna nimetatud seadusega muudeti küberturvalisuse seaduse § 3 sõnastust. Määruses nr 1 tehtavate muudatuste tulemusena ei lisata määruse kohaldamisalasse uusi üksusi ning ühtegi üksust ei jäeta ka selle määruse kohaldamisalast välja võrreldes kuni 31. detsembrini 2025 kehtinud küberturvalisuse seaduse ja selle alusel kehtestatud määrusega nr 1.

Paragrahvi 3 punktiga 1 muudetakse määruse nr 1 § 1 lõike 1 sissejuhatavat lauset.
Muudetavas lauses viidatakse küberturvalisuse seaduse § 3 lõikele 4, mis hõlmas kuni 31. detsembrini 2025 järgmisi üksusi: andmekogu vastutav ja volitatud töötleja, Arenguseire Keskus, Eesti Pank, kohaliku omavalitsuse üksus, kohaliku omavalitsuse üksuste liit, kohtuasutus, riigi valimisteenistus, Riigikogu Kantselei, Riigikontroll, Riigimetsa Majandamise Keskus, seaduse alusel asutatud avalik-õiguslik juriidiline isik, Vabariigi Presidendi Kantselei, valitsusasutus, valitsusasutuse hallatav riigiasutus, valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald, linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus, kohaliku omavalitsuse üksuste ühisamet ja -asutus ning Õiguskantsleri Kantselei.

Kommenteeritava punktiga tehtava muudatusega viidatakse küberturvalisuse seaduse § 3 lõike 2 punktidele 3 ja 4 ning lõike 4 punktidele 1–4 ja 6. Sellega tagatakse, et tegemist on samade eelmainitud üksustega ning seega määruse nr 1 kohaldamisala ei muutu.

Paragrahvi 3 punktiga 2 muudetakse määruse nr 1 § 1 lõike 1 punkti 1.
Muudetavas lauses viidatakse küberturvalisuse seaduse § 3 lõike 4 punktidele 12 ja 13, mis kuni 31. detsembrini 2025 hõlmas järgmisi üksusi: valitsusasutus, valitsusasutuse hallatav riigiasutus, valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald, linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus, kohaliku omavalitsuse üksuste ühisamet ja -asutus. Uues tekstiosas on kasutatud sõnu „valitsusasutus“ (vt Vabariigi Valitsuse seaduse § 39), „valitsusasutuse hallatav riigiasutus“ (vt Vabariigi Valitsuse seaduse § 43 lõige 1) ja „kohaliku tasandi avaliku halduse üksus (vt küberturvalisuse seaduse § 2 punkt 16). Seeläbi tagatakse kooskõla küberturvalisuse seadusega.

3. Eelnõu vastavus Euroopa Liidu õigusele
Eelnõu järgib NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiivi võttis ennekõike üle ülevõtmisseadus, on selle seaduseelnõu materjalide hulgas ka NIS2-direktiivi ja ülevõtmisseaduse vastavustabel. Siinkohal esitatakse need sätted, mis on seotud kommenteeritava eelnõuga:
1) artikli 14 lõike 3 esimene lause = määrusega nr 319 kinnitatud „Justiits- ja digiministeeriumi põhimääruse” punkti 54^1 alapunkt 1^1;
2) artikli 16 lõige 2 = määrusega nr 319 kinnitatud „Justiits- ja digiministeeriumi põhimääruse” punkti 54^1 alapunkt 1^1;
3) artikli 21 lõike 2 punkt a = määruse nr 121 lisa punkt 1 tervikuna;
4) artikli 21 lõike 2 punkt b = määruse nr 121 lisa punkt 5 tervikuna, kuid seotud on ka punktid 7.8.–7.11;
5) artikli 21 lõike 2 punkt c = määruse nr 121 lisa punktid 3.1, 3.6, 5.3 ja 7.6;
6) artikli 21 lõike 2 punkt d = määruse nr 121 lisa punkt 4 tervikuna, kuid seotud on ka punkt 1.3;
7) artikli 21 lõike 2 punkt e = määruse nr 121 lisa punktid 6.1, 7.1–7.3 ja 7.12–7.14;
8) artikli 21 lõike 2 punkt f = määruse nr 121 lisa punkt 1.3, kuid seotud on ka punktid 3.1, 4.1, 4.2, 6.6 ja 7.14;
9) artikli 21 lõike 2 punkt g = määruse nr 121 lisa punkt 2 tervikuna, kuid seotud on ka punktid 5.1 ja 6.1–6.5;
10) artikli 21 lõike 2 punkt h = määruse nr 121 lisa punktid 3.3, 3.4 ja 7.7, kuid seotud on ka punktid 2.6, 7.12, 7.13;
11) artikli 21 lõike 2 punkt i = määruse nr 121 lisa punktid 1.1, 1.4, 2.3, 2.4, 2.6, 3.2, 3.5, 3.7, 6.2, 7.3, 7.5 ning punktid 8 ja 9 tervikuna;
12) artikli 21 lõike 2 punkt j = määruse nr 121 lisa punkt 2.5 ja 5.3, kuid seotud on ka punkt 6.4;
13) artikli 21 lõige 3 = määruse nr 121 lisa punkt 4.1.

Iga muudatuse juures on hinnatud muudetava sätte vastavust Euroopa Liidu õigusele, vajaduse korral on toodud ka võimalikud sõnastusalternatiivid.

Kehtiva õiguse suhtes (mida nt ei muudeta) kohaldub ka NIS2-direktiivi artikkel 5, mis näeb ette järgmist: *[NIS2-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.*

4. Määruse mõjud

Eelnõu muudatustega kaasneb mõju eelkõige riigi julgeolekule ja välissuhetele, samuti majandusele ning riigiasutuste ja kohaliku omavalitsuse korraldusele. Otsest sotsiaalset mõju (sh demograafilist), mõju elu- ja looduskeskkonnale ning regionaalarengule ei kaasne. Muudatuste tulemusel suureneb õigusselgus ja tagatakse NIS2-direktiivi nõuete ülevõtmine ning täpsustub Justiits- ja Digiministeeriumi roll EL tasandi küberkoostöös. Muudatused puudutavad eelkõige küberturvalisuse seaduse kohaldamisalasse kuuluvaid teenuseosutajaid (avalikust ja erasektorist) kui konkreetselt ka Justiits- ja Digiministeeriumi.

Määruses nr 319 tehtaval muudatusel ei ole olulist mõju, kuna tegemist on ülesannetega, mida Justiits- ja Digiministeerium täidab suuremal või vähemal määral juba praegu.

Määruses nr 121 tehtavatel muudatustel on teatav mõju. Selle mõju laadi ja ulatust on hinnatud ülevõtmisseaduse eelnõu seletuskirjas (vt ülevõtmisseaduse eelnõu seletuskirja[57] punkt 6.1.), mistõttu mõjuhindamist siin ei korrata. Lisaks leevendatakse eelnõuga nende teenuseosutajate (ennekõike erasektori teenuseosutajate) nõudeid, kes peavad rakendama Eesti infoturbestandardit või selle alternatiiviks olevat standardit. Selles nähakse ette, et ühe mainitud standardi nõudeid tuleb rakendada vähemalt sellel tegevusalal või tegevusaladel, kus tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. See tähendab, et standard peab käsitlema vastava teenuse, tegevusala või valdkonnaga seotud võrgu- ja infosüsteeme, kuid ülejäänud teenuste, tegevusalade ja valdkondadega seotud võrgu- ja infosüsteemide puhul saab kasutada paindlikumaid turvameetmeid (st esmaseid turvameetmeid). Seeläbi on eelnõuga kavandatav Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitlusala muudatus halduskoormuse vähendamise lisameede, mis leevendab eelnõukohase määruse mõju.
Teenuseosutajatele (sh ennekõike erasektori teenuseosutajale) avalduv majanduslik mõju on väga erinev ning seda ei ole praegu võimalik mõistlikult hinnata. Turvameetmete rakendamise rahaline kulu sõltub teenuseosutaja kasutatavate süsteemide hulgast ja keerukusest ning varem rakendatud turvameetmetest (subjekti vastutustundlikkusest oma IT-lahenduste kasutamisel või muudest nõuetest, näiteks isikuandmete töötlemiseks rakendatud tehnilistest ja korralduslikest turvalisuse tagamise meetmetest). Teenuseosutajale avalduv rakendamiseks vajaliku kulu majanduslik mõju sõltub omakorda selle kulu osakaalust tema eelarves, ennekõike IT-lahendustega seotud eelarves. Eelnõuga kavandatavate nõuete sisu ja olemus ei ole siiski sedavõrd märkimisväärne, et need tooks teenuseosutajatele kaasa olulist kulu. Lisaks eeltoodule on siin asjakohane asjaolu, et küberturvalisuse seaduses on sätestatud ka üleminekuajad, mis leevendab eelnõukohase määrusega tehtavate muudatuste mõju ulatust.

Määruses nr 1 tehtavatel muudatustel ei ole olulist mõju, kuna tegemist on tehnilise muudatusega.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamisega eeldatavad kulud

Eelnõukohase määruse rakendamisega ei prognoosita tulusid.

[57] Vt altviidet nr 1.

Määruses nr 319 tehtav muudatus ei tohiks tekitada Justiits- ja Digiministeeriumile lisakulutusi, kuna ta täidab neid ülesandeid juba praegu. Kui neid peaks siiski tekkima, analüüsitakse neid riigieelarve planeerimise protsessis.

Määrusesse nr 121 tehtavate muudatustega (st ennekõike selle lisa asendamisega) seotud riigi ja kohaliku omavalitsuse tegevusi ja kulusid on hinnatud ülevõtmisseaduse eelnõu seletuskirjas (vt seletuskirja punkt 7), mistõttu selle tulemusi siin ei korrata. Seda enam, et esmaste turvameetmetega seotud nõuded on samaväärsed kehtivate küberturvalisuse tagamise nõuetega, mistõttu puudub vajadus täpsemalt hinnata nende kulu. Viidatud ülevõtmisseaduse eelnõu seletuskirja[58] punktis (vt punkt 7.4) on selgitatud ka riigi pakutavat muud tuge, koolitusi ja toetusi. Näiteks asjaolu, et Riigi Infosüsteemi Ameti teenistujate osalusel on arendamisel Eesti infoturbestandardi järgimise tugirakendus,[59] mis aitab rakendajal luua vajaduspõhist turvameetmete rakendamise plaani, seejuures vähendada vigu meetmete valimisel, ja suunab rakendaja kohe meetmete rakendamisele. Sama tugirakendust on võimalik kasutada ka esmaste turvameetmete nõude täitmise kontrolliks. Lisaks leevendatakse eelnõukohase määrusega nende teenuseosutajate (ennekõike erasektori teenuseosutajate) nõudeid, kes peavad rakendama Eesti infoturbestandardit või selle alternatiiviks olevat standardit. Selles nähakse ette, et ühe mainitud standardi nõudeid tuleb rakendada vähemalt sellel tegevusalal või tegevusaladel, kus tegutsev teenuseosutaja kuulub küberturvalisuse seaduse kohaldamisalasse. See tähendab, et standard peab käsitlema vastava teenuse, tegevusala või valdkonnaga seotud võrgu- ja infosüsteeme, kuid ülejäänud teenuste, tegevusalade ja valdkondadega seotud võrgu- ja infosüsteemide puhul saab kasutada paindlikumaid turvameetmeid (st esmaseid turvameetmeid). Seega on eelnõukohase määrusega tehtav Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitlusala muudatus halduskoormuse vähendamise lisameede, mis leevendab eelnõukohase määruse mõju.

Määruses nr 1 tehtavad muudatused ei too kaasa riigi ja kohaliku omavalitsuse tegevusi ega kulusid, kuna tegemist on tehnilise muudatusega.

6. Määruse jõustumine

Määrus jõustub üldises korras, sest tegemist on ülevõtmisseadusest tuleneva rakendusaktiga.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

1. Enne eelnõu koostamist toimusid kaasamised seoses NIS2-direktiivi ülevõtmisega. Nende käigus sai anda tagasisidet muu hulgas ka kommenteeritava eelnõuga kavandatavate nõuete kohta. Asjaomase tagasiside leiab ülevõtmisseaduse eelnõu dokumentide juurest. Samuti on seletuskirjas vajaduse korral selgitatud märkusi, mis saadi ülevõtmisseaduse eelnõu kohta enne selle esitamist Riigikogule.

2. Eelnõu avaldati eelnõude infosüsteemis 13.03.2026 (toimik 26-0331). 24.03.2026 katkestas Justiits- ja Digiministeerium eelnõu menetluse. Katkestatud eelnõule esitas märkustega kooskõlastuse Väliministeerium, märkusteta kooskõlastas eelnõu Siseministeerium. Eelnõu kohta avaldasid arvamust Riigi Info- ja Kommunikatsioonitehnoloogia Keskus ning Registrite ja Infosüsteemide Keskus. Nimetatud eelnõule esitatud märkused on toodud seletuskirja lisas.

[58] Vt altviidet nr 1.
[59] https://eits.ria.ee/et/abimaterjalid/tugirakendus

3. Eelnõu esitatakse uuesti eelnõude infosüsteemi kaudu kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

Eelnõu saadakse arvamuse avaldamiseks Riigikogu Kantseleile, Riigikontrollile, Vabariigi Presidendi Kantseleile, Õiguskantsleri Kantseleile, Andmekaitse Inspektsioonile, Eesti Pangale, Riigi Infosüsteemi Ametile, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Registrite ja Infosüsteemide Keskusele, Riigiside Sihtasutusele, , Finantsinspektsioonile, Eesti Pangaliidule, 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, Eesti Elektritööstuse Liidule, Eesti Jõujaamade ja Kaugkütte Ühingule, Eesti Gaasiliidule, Eesti Transpordikütuste Ühingule, Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule,

Vabariigi Valitsuse määruse „Vabariigi Valitsuse 23. detsembri 1996. a määruse nr 319 „Justiits- ja Digiministeeriumi põhimääruse kinnitamine“, Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ning Vabariigi Valitsuse 3. jaanuari 2024. a määruse nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ muutmine“ eelnõu seletuskirja lisa

Märkuste tabel

	Märkus	Märkusega arvestamine
Välisministeerium kiri 02.04.2026 nr 15.1-3/1658-1		
1.	Lisa punktis 4 seatakse nõuded väliste partnerite haldusele, sealhulgas nende tausta kontrollile. Välisministeeriumi hinnangul ei saa üksnes tausta teadmine olla aluseks näiteks lepingute sõlmimisele, riigihankes diskvalifitseerimisele või riigihanke luhtunuks kuulutamisele. Meie hinnangul tuleks taustakontrolli küsimuste lahendamiseks välja töötada usalduskontrolli üldregulatsioon (näiteks taustakontrolli seadus), mis reguleeriks füüsiliste ja juriidiliste isikute usaldusväärsuse kontrolli ning annaks kontrollivale asutusele õiguse töödelda ja pääseda juurde selleks vajalikule teabele.	**Antud selgitus** Vabariigi Valitsuse 09.12.2022 määrusega nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ sätestatud esmased turvameetmed kohalduvad nii era- kui ka avaliku sektorile. Esmaste turvameetmete järgmisel eeldatakse, et küberturvalisuse seaduse subjekt hindab, milline on tema jaoks potentsiaalse tarnija (koostööpartneri) usaldusväärus, sh kas partneri pakutav teenus sobib võrgu- ja infosüsteemi turvameetmetega või võimekusega osutada nõuetekohast teenust. Esmaste turvameetmete juures ei peeta silmas potentsiaalse tarnija töötajate tausta uurimist. Hindamisel võib arvesse võtta teada olevat ja kättesaadavat teavet, sealhulgas ka kättesaadavaid erinevate riikide regulaatorite avaldatud hinnanguid. Potentsiaalse tarnija hindamise sügavuse ei ole piiritletav, sõltub kättesaadavat teabest ja küberturvalisuse seaduse subjekti enda poolsest riskide aktsepteerimisest.
2.	Teeme ettepaneku lisada võrgu- ja infosüsteemide küberturvalisuse nõuetesse läbiva krüpteerimise põhimõte. See tähendab, kui	**Antud selgitus**

	andmeside ühendus võimaldab krüpteerimisprotokollide kasutamist, siis tuleb seda ka teha. Praegu on lisa punktides 7.7 ja 8.4 nõutud üksnes kõvaketaste ja traadita võrgu andmeside krüpteerimine, mis ei ole Välisministeeriumi hinnangul piisav.	Vabariigi Valitsuse 09.12.2022 määrusega nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ sätestatud esmased turvameetmed kohalduvad kõigile küberturvalisuse seaduse subjektidele sõltumata suuruses. Ettevõtjate turvameetmete, sealhulgas krüpteerimise vajadus võib olla erinev lähtuval ettevõtja võrgu- ja infosüsteemides ning seal töödeldavast teabest. Seega ei ole absoluutne krüpteerimise nõude kehtestamine asjakohane.
Riigi Info- ja Kommunikatsioonitehnoloogia Keskus 02.04.2026 nr 1-5/26-93-2		
	Võrgu- ja infosüsteemi turvameetmete nõuded Toetame eelnõu eesmärki viia võrgu- ja infosüsteemide küberturvalisuse nõuded kooskõlla NIS2 direktiiviga ning vähendada põhjendamatut halduskoormust seal, kus see ei anna täiendavat turvaväärtust. Soovitame täpsustada kesksete teenuseosutajate rolli ja vastutuse ulatust, sh eristada selgelt, millised kohustused lasuvad teenusepakkujal ning millised klientasutusel. Samuti peame oluliseks ühtsete standardite ja juhiste kehtestamist (nt riskihindamine, auditid, intsidentide käsitlus), et tagada teenuste ülene kooskõla. Täiendavalt tuleks arvestada vajadusega tagada piisavad ressursid ja realistlikud rakendustähtajad, arvestades nõuete märkimisväärset laienemist.	**Antud selgitus** Vabariigi Valitsuse 09.12.2022 määrusega nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ ei laiene isikutele, kes ei ole küberturvalisuse seaduse subjektid. Samuti puudub seaduses volitus välistele isikutele otseste kohustuse kehtestamiseks. Väliste isikutega peab saavutama teenuse osas kokkuleppe küberturvalisuse seaduse subjekt ise.
	RIT peab oluliseks, et E-ITS-i ja muude tunnustatud standardite vaheline vastavusloogika oleks praktiliselt rakendatav, sh arvestaks olemasolevaid sertifikaate ja auditeid kogu teenuse ulatuses, mitte killustatult.	**Antud selgitus** NIS2-direktiiv näeb ette, et turvameetmete rakendamise kohustus on üksuse (küberturvalisuse seaduse subjekt) ülene, senise teenuse põhise lähenemise osas (mis kehtis kuni 31.12.2025. a). Eelnõuga nähakse ette, et üksus ei pea ühesuguseid meetmeid rakendama üksuse üleselt vaid saab endiselt järgida teenusepõhist lähemist. Selline lähenemine võimaldab üksusel tegevusvaldkondades,

		millega ei kvalifitseeru küberturvalisuse seaduse subjektiks, rakendada teistsuguseid turvameetmeid kui valdkonnas, mille osutamise tulemina nad muutusid seaduse subjektiks. Seega näiteks NIS2-direktiivi artikli 21 lõike 5 alusel kehtestatud rakendusmäärusega ettenähtud tegevusvaldkonnas rakendatakse rakendusmäärusest tulenevaid meetmeid, kuid küberturvalisuse seaduses nimetamata valdkondades esmaseid turvameetmeid.
	Arvestades, et mitmetes valdkondades kasutatakse väliseid partnereid, soovitame kaaluda, eelkõige peatükis 4, ühtsete ja täpsemate nõuete kehtestamist välistele partneritele, selle asemel et jätta vastavate meetmete määratlemine suures ulatuses iga kasutaja otsustada. Samuti peame oluliseks sätestada kohustus määrata kogu teabele säilitustähtaeg, et välistada põhjendamatu nn tähtajatu säilitamine, mitte üksnes käsitleda andmete säilitamist seadmete utiliseerimise kontekstis.	**Antud selgitus** Väliste partnerite kaasatuse ulatus sõltub igast üksusest enesest ning riigi poolt välistele partneritele nõuete kehtestamine ei ole otstarbekas ega ka seadusega kooskõlas. Teabe säilitamise tähtajad sõltuvad siiski üksuse enda tööprotsessidest ja vajadustes. Isikuandmete säilitamisel on olemas isikuandmete kaitse üldmäärusest tulenev regulatsioon. Justiits- ja Digiministeerium ei pea siin vajalikuks täiendavate kesksete tähtaegade ettenägemist.
	Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel Toetame eelnõu eesmärki suurendada pilvteenuste turvalist kasutamist ning tuua selgust vastutuse jaotusesse. RIT-i kui keskse teenuseosutaja vaates on oluline, et regulatsioon võimaldaks pakkuda standardiseeritud pilvelahendusi mitmele asutusele ilma liigse halduskoormuseta. Liialt detailne või asutusepõhine nõuete rakendamine võib takistada ühtsete teenuste arendamist ja vähendada oluliselt kuluefektiivsust.	**Võetud teadmiseks**
	Soovitame täpsustada kesksete teenusepakkujate rolli ning võimaldada turvameetmete rakendamist teenusepõhiselt, mitte iga	**Võetud teadmiseks**

	klientasutuse lõikes eraldi. Samuti on oluline, et aktsepteeritaks rahvusvahelisi standardeid ja pilveteenuse pakkujate sertifikaate (nt ISO) ilma dubleerivate auditikohustusteta. Täiendavalt võiks selgemalt määratleda, millised nõuded jäävad pilveteenuse pakkuja ning millised teenuse tarbija vastutusalasse, et vältida vastutuse hajumist.	Märkus ei ole seotud eelnõu skoobiga.
	Oluline on, et NIS2 nõuete ja EITS-i täitmine ei oleks dubleerivad kohustused. Kui EITS-i nõuded on täidetud, siis peaks sellega olema täidetud ka NIS2 nõuded, mistõttu on praktikas vajalik ühtse vastavustabeli vms loomine, mis lihtsustab vastavuskontrolli teostamist.	**Antud selgitus** Eesti infoturbestandard (E-ITS) on kooskõlas NIS2-direktiivi artikliga 21 ja eraldi nõuete täitmise kinnitamise kohustus üksustel puudub. Siin vt ka eelnõu § 2 punkti 13 selgitust (st ennekõike sealset tabelit), mis nõuetele vastavust selgitab.