

**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 pilyteenuse kasutamisel“ muutmise“ 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, kuid põhimõtteliselt ka avaliku sektori 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-c6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine/>.

korralduslikest turvalisuse tagamise meetmetest). Teenuseosutajale avaldub 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 käsitusala muudatus leevendada eelnõu mõju.

Kokkuvõtlikult sisaldab eelnõu ettevõtjatele nii halduskoormust suurendavaid kui ka vähendavaid muudatusi. Halduskoormus võib suureneeda 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 suurusel, tegevusvaldkonnast ja senisest turvatasemest. Halduskoormuse tasakaalustamise reeglil ei ole vaja rakendada.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@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://eelvoud.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 2023–2027⁵ 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 käsitusala muudatus halduskoormuse vähendamise lisameede, mis leevendab eelnõukohase määruse mõju.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast paragrahvist.

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

Paragrahvi 1 punktiga 1 muudetakse punkti 54¹, täiendades seda alapunktiga 1¹.

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/koalitsioonileppe-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 3¹.
<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 kolmeteistkümnest punktist.

Paragrahvi 2 punktiga 1 asendatakse määruses nr 121, välja arvatud § 4 lõikes 1¹, 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 1¹, 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 1¹ ja 1², lisades vastavalt terminid „andmekogu vastutav töötleja“ ja „andmekogu volitatud töötleja“ ja nende tähenduse. Andmekogu vastutav töötleja on andmekogu vastutav töötleja avaliku teabe seaduse § 43⁴ 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 § 43⁴ lõike 2 tähenduses. Selle lõike kohaselt võib andmekogu vastutav töötleja *volitada andmete töötlamise 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 täiendatakse määruse nr 121 § 3 lõikega 1¹.

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit tegi ülevõtmisseaduse menetluse käigus ettepaneku *lähutada 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 sätestatud. 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 § 5¹ ja sama määruse lisa ning ka eelnõu § 2 punkt 12).

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 4 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 käsitusala 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 rakendusala 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 5 muudetakse määruse nr 121 § 3 lõike 2¹ sissejuhatava lause sõnastust. Kõnesoleva eelnõuga lisatakse sellesse paragrahvi uus lõige (vt eelnõu § 2 punkt 3), mistõttu tuleb õigusselguse huvides kommenteeritava lõike sissejuhatavat lauset muuta. Muudatuse tulemusena ei kohaldata määruse nr 121 § 3 lõikeid 1, 1¹ ja 2 üksustele, keda on nimetatud sama paragrahvi lõikes 2¹.

Paragrahvi 2 punktiga 6 asendatakse määruse nr 121 § 3 lõike 2¹ punktis 1 sõna „määratlemise“ sõnaga „määratluse“. Tegemist on tehnilise muudatusega (parandatakse pealkirja sõnastust), kuna selles punktis viidatud Euroopa Komisjoni soovitus tegelik pealkiri on „Komisjoni soovitus, mis käsitleb mikro-, väikeste ja keskmise suurusega ettevõtjate määratlust“.⁷

Paragrahvi 2 punktiga 7 täiendatakse määruse nr 121 § 3 lõigetega 2² ja 2³.

Kuigi NIS2-direktiivi artikli 2 lõike 1 teine lõik võeti üle ülevõtmisseaduse kohase küberturvalisuse seaduse § 3 lõikega 6, siis kõnealuse muudatusega (lisanduv **lõige 2²**) 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 soovitus 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 soovitusel põhjendus 13:

(13) Vältimaks kunstlikku vahetegemist liikmesriigi erinevate avalik-õiguslike asutuste vahel ja arvestades vajadust õiguskindluse järele, peetakse vajalikuks kinnitada, et VKE ei ole ettevõtte, mille kapitalist või hääleõigustest 25% või enam kontrollib avalik-õiguslik asutus.

NIS2-direktiivi artikli 2 lõike 1 teine lõik täpsustab, et viidatud soovitusel 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 2¹ 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. Soovitusel 2003/361/EÜ ei ole mõeldud reguleerida seda, kuidas toimida kontrolli omavate avaliku sektori

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

organisatsioonidega, ja see ei sisalda selgeid reegleid selle teema kohta. Selle soovitusel 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 soovitusel 2003/361/EÜ kohta.

Lisanduva **lõikega 2³** 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 elutähtsateks⁸ või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovitusel 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 riigisiselt ei sätestata NIS2-direktiivis ette nähtud miinimumnõuetest rangemaid nõudeid, on lõikesse 2² 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- 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 8 täiendatakse määruse nr 121 § 5 lõikega 1¹.

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 sisu⁹.

⁸ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliseks üksuseks“.

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:

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. Termin „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. Termin „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 tsiviilkriisi ja riigikaitse seaduse eelnõu § 18 lõikes 1 on toimepidevus defineeritud kui *püsiva kriisiülesandega asutuse ja isiku, sealhulgas elutähtsa teenuse osutaja ja kohaliku omavalitsuse üksuse, 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 üksuste¹⁴ suhtes kohaldatavate nõuetega, mis on sätestatud NIS2-direktiivi artikli 21 lõike 5 alusel vastu võetud komisjoni rakendusmääruses (EL) 2024/2690,¹⁵ konkreetsemalt selle rakendusmääruse artiklis 2 ja rakendusmääruse lisa punktides 1 ja 2 ning mõlema punkti alapunktides.

Ülevõtmiseaduse vastuvõtmisele eelnenud menetluse käigus esitati kõnealuse sätte kohta järgmine kommentaar (vt ülevõtmiseaduse 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

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/tsiviilkriisi-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 registreerijad, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalseadusplatvormi pakkujad ja usaldusteenuse osutajad. Vt täpsemalt küberturvalisuse seaduse § 7 lõige 7 ja ülevõtmiseaduse 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](https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=PI_COM:Ares(2024)4640447&qid=1728309190768).

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 riskikäsitusmeetmed 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 soovitatav lisada ka rakendamise nõue. Seda viimast eriti olukorras, kus rakendusplaan riskikäsitusmeetmetega 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 12 ning selle selgitusi.

Paragrahvi 2 punktiga 9 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 § 5¹ (esmased turvameetmed) ja sellega seotud sama määruse lisas ette nähtud nõuete täitmiseks.

Paragrahvi 2 punktiga 10 muudetakse määruse nr 121 § 5¹ 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 tegevusalasid. Kõnealuse muudatusega sätestatakse, et määruses nr 121 ette nähtud esmased turvameetmed ongi needsamad alalisse kasutusse võetavad nõuded.

Paragrahvi 2 punktiga 11 muudetakse määruse nr 121 § 5¹ lõike 1 punkti 4, asendades sõnad „tarnijate, väliste teenuste osutajate ja partnerite haldus“ sõnadega „väliste partnerite haldus“. Tegemist on tehnilise muudatusega. Vt ka eelnõu § 2 punkti 12, konkreetsemalt seal märgitud määruse nr 121 lisa punkti 4 ja selle alapunkti selgitusi.

Paragrahvi 2 punktiga 12 asendatakse määruse nr 121 lisa (edaspidi *lisa*), mis on seotud määruse §-s 5¹ 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 3 ja 4 ning nende selgitused).

Algselt kaaluti kõnesoleva eelnõu puhul eraldi paragrahvi loomist, mis võtaks üle NIS2-direktiivi artikli 21 lõigete 2 ja 3 sisu (alalisel 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 tole 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 alalisel 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 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 elutähtsatel¹⁷ 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 elutähtis¹⁸ 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

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

¹⁷ Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulistel üksustel“.

¹⁸ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluline üksus“.

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 elutähtsad¹⁹ 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 elutähtsate²⁰ ja oluliste üksuste poolt, või liikmesriigid võivad üksustelt nõuda, et nad kasutaksid sertifitseeritud IKT-tooteid, IKT-teenuseid ja IKT-protsesse.

(81) Et vältida elutähtsate²¹ ja oluliste üksuste 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 elutähtsa²² või olulise üksuse riskidele avatuse määraga ning intsidendi ühiskondliku ja majandusliku mõjuga. Elutähtsatele²³ ja oluliste üksuste kohandatud küberturvalisuse riskijuhtimismeetmete kehtestamisel tuleks igakülgsest arvesse võtta elutähtsate²⁴ 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) Elutähtsad²⁵ ja olulised üksused peaksid tagama oma tegevuses kasutatavate võrgu- ja infosüsteemide turvalisuse. Nende puhul on eelkõige tegemist privaatsete võrgu- ja infosüsteemidega, mida haldavad kas elutähtsa²⁶ või olulise üksuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. [NIS2-direktiivis] sätestatud küberturvalisuse riskijuhtimismeetmeid ning teatamiskohustust tuleks kohaldada asjaomaste elutähtsate²⁷ ja oluliste üksuste suhtes olenemata sellest, kas kõnealused üksused hooldavad oma võrgu- ja infosüsteeme ise või tellivad selleks hooldusteenuse väljast.

¹⁹ Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.

²⁰ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

²¹ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

²² Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuse“.

²³ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

²⁴ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

²⁵ Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.

²⁶ Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulise üksuse“.

²⁷ Ülevõtmisseaduse kohases küberturvalisuse seaduses „ülioluliste üksuste“.

(84) Võttes arvesse nende piiriülest olemust, tuleks domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite²⁸, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate²⁹, hallatud teenuse osutajate³⁰, turbetarnijate³¹, internetipõhise kauplemiskohtade³², internetipõhiste otsingumootorite³³, sotsiaalturvalisusteenuse platvormi pakkujate³⁴ 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 tarneaahelast 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 elutähtsad³⁵ ja olulised üksused hindama ja arvesse võtma toodete ja teenuste üldist kvaliteeti ja vastupidavust, nendesse integreeritud küberturvalisuse riskijuhtimismeetmeid, samuti oma tarnijate ja teenuseosutajate³⁶ küberturvalisuse tavaid, sealhulgas nende turvalise arenduse menetlusi. Elutähtsaid³⁷ 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 turbetarnijatel³⁸ sellistes teenusevaldkondades nagu intsidentide lahendamine, läbistustestimine, turvaaudit ja konsultatsioonid. Turbetarnijad³⁹ on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on üksuste tegevusse tihedalt lõimitud, kaasneb nendega eriline risk. Seega peaksid elutähtsad⁴⁰ ja olulised üksused olema turbetarnija⁴¹ valimisel iseäranis hoolikad.

(88) Elutähtsad⁴² 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 tavaid ja eelkõige intellektuaalomandi

²⁸ Ülevõtmiseaduse kohases küberturvalisuse seaduses „tippdomeeninimede registrite pidajad“.

²⁹ Ülevõtmiseaduse kohases küberturvalisuse seaduses „sisulevivõrguteenuse osutajate“.

³⁰ Ülevõtmiseaduse kohases küberturvalisuse seaduses „haldusteenuse osutajate“.

³¹ Ülevõtmiseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajate“.

³² Ülevõtmiseaduse kohases küberturvalisuse seaduses „internetipõhiste kauplemiskohtade pidajate“.

³³ Ülevõtmiseaduse kohases küberturvalisuse seaduses „veebipõhise otsingumootori pakkujate“.

³⁴ Ülevõtmiseaduse kohases küberturvalisuse seaduses „sotsiaalmeeiaplatvormi pakkujate“.

³⁵ Ülevõtmiseaduse kohases küberturvalisuse seaduses „üliloolulised üksused“.

³⁶ Siin ei ole pigem mõeldud ülevõtmiseaduse 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 ülevõtmiseaduse järgse küberturvalisuse seaduse kohased haldusteenuse osutajad või infoturbeteenuse osutajad. See märkus käib ka käesoleva tekstilõigu kahe järgmise lause kohta.

³⁷ Ülevõtmiseaduse kohases küberturvalisuse seaduses „üliloolulisi üksusi“.

³⁸ Ülevõtmiseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajatel“.

³⁹ Ülevõtmiseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutajad“.

⁴⁰ Ülevõtmiseaduse kohases küberturvalisuse seaduses „üliloolulised üksused“.

⁴¹ Ülevõtmiseaduse kohases küberturvalisuse seaduses „infoturbeteenuse osutaja“.

⁴² Ülevõtmiseaduse kohases küberturvalisuse seaduses „üliloolulised üksused“.

kaitsega seotud tavad. Võttes arvesse andmete olulisust ja väärtust elutähtsate⁴³ ja oluliste üksuste tegevuse jaoks, peaksid kõnealused üksused kolmandate isikute poolt osutatavatele andmete teisendamise ja analüüsi teenustele tuginedes võtma kõik asjakohased küberturvalisuse riskijuhtimismeetmed.

(89) Elutähtsad⁴⁴ 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 tarneahelariiske ning aidata asjakohaselt juhtida [NIS2-direktiivi] kohaldamisalasse kuuluvates sektorites tegutsevatel elutähtsatel⁴⁵ 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 soovitusel (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, nõrkuste⁴⁶ ja muude riskide vastu, mis on seotud tarneahelaga, ning uurida, kuidas saaks elutähtsaid⁴⁷ 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 nõrkusi⁴⁸ 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 tehnilisi tegureid, sealhulgas neid, mis on kindlaks määratud soovitusel (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 elutähtsad⁴⁹ 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 olulusringi 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

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“.

⁴⁹ Ülevõtmisseaduse kohases küberturvalisuse seaduses „üliolulised üksused“.

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 [NIS2-direktiivi] 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 intsidentist, 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 intsidentideadetega juba omandatud. ENISA võib koostada üldkasutatavate elektroonilise side võrkude pakkujate⁵⁰ 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.

(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 laieneses 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

⁵⁰ Ülevõttmiseseaduse kohases küberturvalisuse seaduses „üldkasutatava elektroonilise side võrgu teenuse osutajate“.

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 elutähtsate⁵¹ ja oluliste üksuste teenused sõltuvad interneti kaudu pakutavatest teenustest. Et tagada elutähtsate⁵² ja oluliste üksuste pakutavate teenuste sujuv osutamine, on oluline, et kõikidel üldkasutatavate elektroonilise side võrkude pakkujatel⁵³ oleksid asjakohased küberturvalisuse riskijuhtimismeetmed ja et nendega seotud olulistest intsidentidest teatataks. 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 pakkujatele⁵⁴ 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 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 osutajaid⁵⁵, innustada võtma vastu domeeninimede süsteemi teisendamise mitmekesistamise strateegia. Ühtlasi peaksid liikmesriigid innustama avaliku ja turvalise Euroopa domeeninimede süsteemi teisendamise teenuse väljatöötamist ja kasutamist.

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“.

⁵⁵ Ülevõtmisseaduse kohases küberturvalisuse seaduses „veebipõhise otsingumootori pakkujaid“.

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 iseloomust 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 riskianalüüsist ja arvestama ühiskonnas ja küberruumis toimuvat oma meetmete uuendamisel, soovitavalt lähtuma Riigi Infosüsteemi Ameti soovitudest ja

⁵⁶ Kättesaadav ettevõtlus- ja infotehnoloogiainistri 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/>.

				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, SYS, IND, NET, INF	CON, OPS, DER, APP, SYS, IND, NET, INF	Protseduurilised teemad valdavalt CONi ja OPSi moodulites, muudes moodulites täpsustused; DER lisab nõrkuse halduse, mis kajastub ka varapõhistes moodulites	Põhiosa 4.2 A5.7, A5.8, A5.23, A7.11, A7.12, A7.13, A7.14, A8.1, A8.6, 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 kasutuskohadest	A8.1, A8.24
Punkt i	ISMS, ORP, CON, OPS, APP, SYS, SYS, IND, NET, INF	ORP, CON, OPS, APP, SYS, IND, NET, INF	Pääsuhaldus katab pea kõiki moduleid, 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 kasutuskohades 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 2¹ 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. Seda illustreerib tabel 2. Tabeli vastavuste esitamisel on võetud eeskuju ka NIS2-direktiivi artikli 21 lõike 5 alusel kehtestatud Euroopa Komisjoni rakendusmääruse (EL) 2024/2690⁵⁷ lisa esitatud tehniliste ja meetodiliste nõuete loetelust. Viidatud rakendusmäärus kohaldub ainult teatud teenuseosutajatele,⁵⁸ sh on selle rakendusmäärusega seoses kehtestatud küberturvalisuse seaduse § 7 lõige 7 (vt ka selle lõike selgitused ülevõtmisseaduse eelnõu seletuskirjas).

Tabel 2. NIS2-direktiivi artikli 21 lõigete 1–3 võrdlus määruse nr 121 lisa sätestatud esmaste turvameetmetega

Art 21 lõige 1	Lisas sätestatud esmaste turvameetmete punkt või punktid	Kommentaar
Terve lõige	Sissejuhatava osa kolmas lõik	Seos on proportsionaalsuse kontekstis ehk see jätab võimaluse rakendada meetet, mis on kõige asjakohasem
Art 21 lõige 2	Lisas sätestatud esmaste turvameetmete punkt või punktid	Kommentaar
Punkt a	Punkt 1 tervikuna	
Punkt b	Punkt 5 tervikuna, kuid seotud on ka punktid 7.8–7.11	
Punkt c	Punkt 1.4, kuid seotud on ka punktid 3.1, 3.6, 5.3 ja 7.6	

⁵⁷ <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1769430711987>

⁵⁸ Ülevõtmisseaduse kohase küberturvalisuse seaduse termineid kasutades on nendeks üksusteks: domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registreerijad, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbetaenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalmeediaplatformi pakkujad ja usaldusteenuse osutajad.

Punkt d	Punkt 4 tervikuna, kuid seotud on ka punkt 1.3	
Punkt e	Punkt 1.5, kuid seotud on ka punktid 6.1, 7.1–7.3 ja 7.12–7.14	
Punkt f	Punkt 1.3, kuid seotud on ka punktid 3.1, 4.1, 4.2, 6.6 ja 7.14	
Punkt g	Punkt 2 tervikuna, kuid seotud on ka punktid 5.1 ja 6.1–6.5	
Punkt h	Punktid 3.3, 3.4 ja 7.7, kuid seotud on ka punktid 2.6, 7.12, 7.13	
Punkt i	Punktid 1.1, 1.6, 2.3, 2.4, 2.6, 3.2, 3.5, 3.7, 6.2, 6.6, 7.3, 7.5 ning punktid 8 ja 9 tervikuna, kuid seotud on ka punktid 6.3, 7.10 ja 7.11	Personalile tasutakontrolli tegemine on ametnike puhul ette nähtud avaliku teenistuse seadusega ning kui keegi personalist peab saama riigisaladuse loa, siis toimub taustakontroll riigisaladuse ja salastatud välisteabe seaduses ette nähtud taustakontrolli menetluse raames
Punkt j	Punkt 2.5 ja 5.3, kuid seotud on ka punktid 1.4 ja 6.4	
Art 21 lõige 3	Lisas oleva esmaste turvameetmete punkt või punktid	Kommentaar
Terve lõige	Punktid 4.1 ja 4.2	

Eelnõu koostamisel otsustati asendada määruse nr 121 kehtiv lisa tervikuna, et tagada lisa kui terviku kompleksus. 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 järgnevatl selgitatud muudatustele ka muid tehnilisi muudatusi (**lisa punktid 1.6, 6.6 ja 7.3**), mille eesmärk on järgida õigusaktide normitehnika sõnastuse põhimõtteid ja tagada lausete sõnastuste selgus.

Lisa sissejuhatuses tehakse kaks muudatust. Sissejuhatuse esimesse punkti lisatakse sõna „alaliselt“, et see vastaks määruse nr 121 § 51 lõike 1 sissejuhatavale lausele (vt ka eelnõu § 2

punkt 10 ja selle selgitus). Teise muudatusena koondatakse sissejuhatuse kolmanda ja neljanda punkti sisu ühte punkti. See muudatus ei too kaasa sisulist muudatust teenuseosutaja jaoks.

Lisa punkti 1.1 lisatakse tekstiosa „küberturvalisuse seaduse §-s 6¹ nimetatud juhatuse liikme ja“. See tekstiosa lisatakse, et luua otsene seos viidatud seaduse sättes kehtestatud kohustusega. Kõnesolevas lisas viidatakse tervele paragrahvile, et see hõlmaks nii lõigetes 1 ja 4 nimetatud isikuid, st nii neid juriidilisi isikuid, kellel on juhatuse liikmed, kui ka neid, kellel juhatuse liikmeid oma tegevusvormi tõttu pole. Viidatud seaduse paragrahvi sisu ja olemust on selgitatud ülevõtmisseaduse eelnõu seletuskirjas. Kommenteeritavas punktis mainitud juhatuse liige ja infoturbe eest vastutav isik võivad praktikas olla sama isik (nt kui teenuseosutaja tegevusvormi tõttu), kuid need võivad olla ka erinevad isikud.

Lisa punktis 1.2 asendatakse sõna „infoturbepõhimõtted“ sõnadega „infoturbe- ja riskijuhtimispõhimõtted“, et viia sõnastus rohkem vastavusse NIS2-direktiivi artikli 21 lõike 2 punktiga 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*). Selle muudatusega võetakse üle ka NIS2-direktiivi artikli 21 lõike 2 punkti i sõnastus (*[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: .. i) personali turvalisust, juurdepääsukontrolli põhimõtteid ja varade haldust*), s.o selles kasutatud sõnad „personali turvalisus“, st kommenteeritav muudatus hõlmab ka personali turvalisust. Praktikas seisnevad personali turvalisus ja sellega seotud protseduurid näiteks nii personali (ametnike ja töötajate) tausta kontrollimises kui ka meetmetes, millega tagatakse nende füüsiline turvalisus.

AKITi kohaselt on infoturbe (ingl *information security*) riskihalduslik tegevus teabe turvalisuse säilitamiseks, sealhulgas andmekaitse tagamiseks. AKIT esitab selle termini juures ka seose rahvusvahelise standardiga ISO/IEC 27000, milles on selle termini tähendust selgitatud teabe konfidentsiaalsuse, tervikluse ja käideldavuse säilitamisena. Teiseks selgitab AKIT, et tegemist on distsipliiniga, mis käsitleb teabe turvalisust.⁵⁹ AKITis on infoturbe (ingl *cybersecurity*) olemuse selgitamise juures viidatud standardile CNSSI 4009-2015, mille kohaselt on tegemist arvutite, elektronsidesüsteemide, elektronsideteenuste, traatside ja elektronside, sealhulgas neis sisalduva teabe kahjustuste vältimise, kaitse ja taaste nende käideldavuse, tervikluse, autentsuse, konfidentsiaalsuse ja salgamatuse tagamiseks.⁶⁰ Sõna „infoturbe“ selgitab Eesti Keele Instituudi ühendsõnastik kui infovarade (andmed, riistvara, tarkvara, side, infrastruktuur, personal) turvalisuse tagamist.⁶¹

Eelmainitud sõnaga „infoturbe“ on praktikas seotud ka sõnad „infoturvapoliitika“ või „üleorganisatsiooniline infoturvapoliitika“. AKITi kohaselt on infoturvapoliitika (ingl *information security policy*) organisatsiooni turvapoliitika osa, määratleb nõuded teabe turvalisusele, infoturbe üldeesmärgid, infoturbe halduse süsteemi struktuuri ja on infoturbe esmane alusdokument. AKIT toob sama sõna puhul ka seose rahvusvahelise standardiga ISO/IEC 29110-4-3, mille kohaselt on see dokument, mis teatab kirjalikult, kuidas organisatsioon kavatseb kaitsta oma füüsilisi ja infotehnoloogilisi varasid. Sarnane selgitus on ka standardis CNSSI 4009-2015.⁶² AKIT annab ka selgituse üleorganisatsioonilisele infoturvapoliitikale (ingl *corporate information security policy*), mille puhul on toodud seos

⁵⁹ <https://akit.cyber.ee/term/513-infoturbe-1>

⁶⁰ <https://akit.cyber.ee/term/6911-kuberturve-3-infoturbe-2>

⁶¹ <https://sonaveeb.ee/search/unif/dlall/dsall/infoturbe/1/est>

⁶² <https://akit.cyber.ee/term/799-infoturvapoliitika>

rahvusvahelise standardi ISO/IEC 27033 selgitusega ehk tegemist on dokumendiga, mis kirjeldab juhtkonna suunitlust ja toetust teabe turvalisuse alal vastavalt ärinõuetele ning kohaldatavaile õigusaktidele ja eeskirjadele, samuti kõige üldisemaid infoturbenõudeid, mida tuleb järgida kogu organisatsioonis.⁶³

Eelnõus on kasutatud terminit „riskijuhtimispõhimõtted“, nagu küberturvalisuse seaduses – vt seaduse § 2 punkt 11 (termini „infoturbeteenuse osutaja“ tähenduse selgitus) ja § 6¹ lõige 2 (teenuseosutaja asjakohane juhatuse liige peab läbima koolitusi, mis hõlmavad ka riskide juhtimise viise). Selle all mõistetakse samu tegevusi, mille kohta õigusaktides (vt nt küberturvalisuse seaduse § 7 lõike 1 punkt 1) või ka muus küberturvalisuse tagamise valdkonna tekstides kasutatakse terminit „riskide haldamine“. Selleks et kasutada lisas terminit „riskide haldamine“, tuleks muuta ka küberturvalisuse seadust, mida kõnesoleva eelnõu ajaraami arvestades pole võimalik teha.

Lisa uue punktiga 1.4 (kehtiva lisa punktid 1.4 ja 1.5 on edaspidi vastavalt punktid 1.6 ja 1.7) nähakse ette, et infoturbe korralduse valdkonnas peab teenuseosutaja *tagama oma tegevusega seotud kriisihalduse ja toimepidevuse, sealhulgas varundus- ja taasteprotseduuride toimimise*. Selle punkti lisamine on seotud NIS2-direktiivi artikli 21 lõike 2 punkti c ülevõtmisega (*[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: .. c) talituspidevust, näiteks varundushaldus ja avariitaaste, ning kriisiohjet*).

AKITi kohaselt on kriisihaldust (ingl *crisis management*) rahvusvahelistes standardites ISO 22300 ja 28002 selgitatud kui terviklikku halduse protsessi, mis tuvastab võimalikud organisatsiooni ähvardavad toimed ja loob karkassi, millele rajada elastsus, mis on võimeline toimivalt reageerima organisatsiooni kesksete huvipoolte, maine, kaubamärgi ja väärtusi loovate tegevuste kaitseks ning toimivalt taastama teovõime. AKIT viitab ka teisele rahvusvahelisele standardile ISO/IEC/IEEE 24765, mille kohaselt on tegemist toimingutega, juhaks kui tekkinud probleemi ei lahendata ootamatuseplaaniga (ingl *contingency plan*).⁶⁴ Sõna „kriisihaldus“ selgitab Eesti Keele Instituudi ühendsõnastik kui meetmete süsteemi, mis hõlmab kriisiks valmistumist, kriisi ennetamist ja lahendamist.⁶⁵

Sõna „toimepidevus“ puhul saab teatavat paralleeli tuua hädaolukorra seaduse § 2 lõikes 5 sätestatud elutähtsa teenuse toimepidevusega, milleks on elutähtsa teenuse osutaja järjepideva toimimise suutlikkus ja järjepideva toimimise taastamise võime pärast elutähtsa teenuse katkestust. Riigikogus arutlusele oleva tsiviilkriisi ja riigikaitse seaduse eelnõu § 18 lõikes 1 on toimepidevus defineeritud kui püsiva kriisiülesandega asutuse ja isiku, sealhulgas elutähtsa teenuse osutaja ja kohaliku omavalitsuse üksuse, ning põhiseadusliku institutsiooni suutlikkus ja valmidus järjepidevalt toimida ning igal ajal oma ülesandeid täita ja teenuseid osutada.⁶⁶ Sõna „toimepidevus“ selgitab Eesti Keele Instituudi ühendsõnastik kui võimelisust, suutlikkust toimida edaspidi, jätkata alustatud tegevust.⁶⁷

AKITi kohaselt on varunduse (ingl *backup*) olemuseks varukomponentide (näiteks andmete varukoopiate) rakendamine ennetava turvameetmena, tervikluse ja käideldavuse tagamiseks. AKITis on toodud näitena rahvusvaheline standard ISO/IEC/IEEE 24765, mille kohaselt see on asendaja loomine või määramine süsteemile, komponendile, failile, protseduurile, isikule.⁶⁸

⁶³ <https://akit.cyber.ee/term/2675-uleorganisatsiooniline-infoturvapoliitika>

⁶⁴ <https://akit.cyber.ee/term/3887-kriisihaldus>

⁶⁵ <https://sonaveeb.ee/search/unif/dlall/dsall/kriisihaldus/1/est>

⁶⁶ <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/679eccc7-62b9-4817-a660-745e6642a8d9/tsiviilkriisi-ja-riigikaitse-seadus/>

⁶⁷ <https://sonaveeb.ee/search/unif/dlall/dsall/toimepidevus/1/est>

⁶⁸ <https://akit.cyber.ee/term/33-varundus>

Teise alternatiivina viidatakse AKITis selle sõna selgituses rahvusvahelisele standardile ISO/IEC 2382, mille kohaselt on varundus kadunud või hävinenud andmeid taastada või süsteemi töövõimet säilitada aitav (protseduur, meetod, riistvara).⁶⁹ Sõna „andmevarundus“ selgitab Eesti Keele Instituudi ühendsõnastik kui andmete koopia loomise ja säilitamise protsessi, mis võimaldab taastada andmeid juhul, kui esialgsed andmed on kadunud, rikutud või kättesaamatud.⁷⁰

Lisa uue punktiga 1.5 (kehtiva lisa punktid 1.4 ja 1.5 on edaspidi vastavalt punktid 1.6 ja 1.7) nähakse ette, et infoturbe korralduse valdkonnas peab teenuseosutaja *tagama võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisuse, sealhulgas turvahaavatavuste käsitlemise ja avaldamise*. Selle punkti lisamine on seotud NIS2-direktiivi artikli 21 lõike 2 punkti e ülevõtmisega (*[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: .. e) võrgu- ja infosüsteemide hankimise, arendamise ja hooldamise turvalisust, sealhulgas nõrkuste käsitlemine ja avalikustamine*).

Termini „turvahaavatavus“ (mida kasutatakse sõna „nõrkus“ asemel) kohta vt ülevõtmisseaduse kohase küberturvalisuse seaduse § 2 punkti 31. Turvahaavatavuse käsitlemise ja avaldamise kohta vt ka NIS2-direktiivi artikli 14 alusel asutatud võrgu- ja infoturbe koostöörühma koostatud asjakohaseid suuniseid.⁷¹

Ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati lisa kavandatud punkti sisu kohta järgmine kommentaar (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), Välisministeeriumi kommentaar nr 10.1): *Sellises sõnastuses võib sätet mõista kui kohustust avalikustada süsteemi nõrkused, mis viib olukorrani, kus on avalikustatud teave, mis võimaldab teostada asutuse vastu edukat küberrünnet. Palume muuta sätte sõnastust selliselt, et teabe avalikustamise kohustus ei tekitaks või lisaks juurde otsest ohtu teenuse osutaja süsteemidele. Pakume välja järgmise sõnastuse: „7) tagama süsteemi hankimise, arendamise ja hooldamise turvalisuse, sh nõrkuste käsitlemise ning avalikustamise selliselt, et ei lisandu juurde uusi ohtusid;“.*

Lisaks on Eesti Infotehnoloogia ja Telekommunikatsiooni Liit esitanud järgmise kommentaari (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), kommentaar nr 24.15):

Eelnõu § 1 punktidega 25-28 muudetakse [küberturvalisuse seaduse] §-i 7. Antud muudatusega laiendatakse subjektide kohustusi. Üldise loogika järgi peavad olema turvameetmed kaetud, kui standard on rakendatud. Eelnõud lugesid aga selgub, et peab järgima lisaks standardile ka eelnõus toodud meetmeid. Kusjuures need meetmed on põhjalikult avatud eelnõu seletuskirjas. Oluline probleem on see, et selle sätte lõikega 2 laiendatakse NIS2 direktiivi sõnastust. Käände muutmisega [küberturvalisuse seaduses] on muudetud NIS2 direktiivi artikkel 21 lõike 2 punktide a)-j) sisu.

Jääb ebaselgeks, kas see on tahtlik või mitte. Oleme seisukohal, et kui NIS2 direktiiv jätab võimaluse subjektidel midagi teha, siis ei tohi seda Eesti õiguses kohustuseks muuta.

Seetõttu tekib olukord, kus NIS2 direktiivi artikkel 21 lõike 2 punkt e) sätestab muuhulgas: „meetmed hõlmavad sh. nõrkuste käsitlemist ja avalikustamist“. [Küberturvalisuse seaduse] § 7 lg [2] punktis 7 näiteks on aga kohustuseks „tagama sh. nõrkuste käsitlemise ja avalikustamise“. Kui NIS2 direktiiv ütleb, et avalikustamise protseduur/ulatus peab meetmetes kirjas olema, siis eelnõus on sellest saanud kohustus avalikustada. ..

⁶⁹ <https://akit.cyber.ee/term/10207-varu-2-varundus>

⁷⁰ <https://sonaveeb.ee/search/unif/dlall/dsall/andmevarundus/1/est>

⁷¹ Guidelines on Implementing National Coordinated Vulnerability Disclosure Policies – kättesaadav: <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>.

Esitatud kommentaari ei võetud kõnealuse sätte sõnastamisel arvesse, kuna eelnõu tulemusel katab teenuseosutaja, kes peab rakendama kas Eesti infoturbestandardit või selle alternatiiviks olevat standardit, ühe standardi järgimisega ka ära VV määruses nr 121 ette nähtud esmased turvameetmed. Kommenteeritava lisa punkti 1.5 puhul on lähtutud NIS2-direktiivi artikli 21 lõike 2 punkti e sisust ja eesmärgist, st siinkohal ei ole mindud ulatuslikuma reguleerimise teed.

Lisa punktis 4 ja selle alapunktides tehtavad muudatused on seotud nii eelnõu § 2 punktiga 11 tehtava muudatusega kui ka NIS2-direktiivi artikli 21 lõike 2 punkti d ülevõtmisega (*[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: .. d) tarneahela turvalisust, sealhulgas sellised turvalisusesse puutuvad aspektid, mis on seotud iga üksuse ja tema otsese tarnijate või teenuseosutajate vaheliste suhetega*)a. Lisaks võetakse ühe alapunktiga üle ka NIS2-direktiivi artikli 21 lõige 3 (*[l]iikmesriigid tagavad, et käesoleva artikli lõike 2 punktis d osutatud meetmete asjakohasust kaaludes võtavad üksused arvesse igale otsesele tarnijale ja teenuseosutajale eriomaseid nõrkusi ning nende tarnijate ja teenuseosutajate toodete üldist kvaliteeti ja küberturvalisuse tavaid, sealhulgas nende turvalise arenduse korda. Liikmesriigid tagavad samuti, et nimetatud punktis osutatud meetmete asjakohasust kaaludes võtavad üksused arvesse artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamiste tulemusi*).

Kommenteeritava punkti põhisisu on seotud tarneahela ja selle turvalisuse tagamisega. AKITi kohaselt on tarneahel (ingl *supply chain*) ressursside, protsesside ja nende sooritajate jada toorme hankimisest valmiskauba toimetamiseni individuaalsele või kollektiivsele lõpptarbijale; ahela komponendid on materjalivoog, rahavoog, teabevoog. Rahvusvahelise standardi ISO 22300 kohaselt on tarneahel tegevustes osalevate ning toodete või teenuste väljastuse teel materjalide allikaks olemisega väärtust loovate organisatsioonide, inimeste, protsesside, logistika, teabe, tehnoloogia ja ressursside kahepoolne seos; tarneahelasse võivad kuuluda turustajad, alltöövõtjad, valmistusvahendid, logistikatarnijad, sisemised jaotuskeskused, jaemüüjad, hulgimüüjad ja muud olemid, mis viivad lõppkasutajani. Rahvusvahelise standardi ISO/IEC 27036-1 kohaselt on tarneahel kogum organisatsioone koos kaasnevate ressursside ja protsessidega, igaüks neist tegutsemas hankija ja/või tarnijana, moodustades järjestikku tarnesuhted, mis luuakse tellimuse andmisega, leppega, muu formaalse soetamiskokkuleppega.⁷² Sõna „tarneahel“ selgitab Eesti Keele Instituudi ühendsõnastik kui protsesside, inimeste, tegevuste, info ja ressursside süsteemi, mida on vaja mingi toote või teenuse jõudmiseks tootjast tarbijani.⁷³

Kommenteeritava punkti aluseks olevas NIS2-direktiivi punktis (NIS2-direktiivi artikli 21 lõike 2 punkt d) on kasutatud väljendit *üksuse ja tema otsese tarnijate või teenuseosutajate*, mida kõnesolevas eelnõus tähistavad sõnad „välised partnerid. Eelnõu selles punktis ei olnud võimalik kasutada sõna „teenuseosutaja“ (nagu NIS2-direktiivi viidatud sättes), kuna sellele sõnale on küberturvalisuse seaduses antud teine tähendus (vt selle seaduse § 3 lõige 1).

Ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati kõnealuse sätte kohta mitmesuguseid kommentaare – toona oli plaanis vastavad nõuded sätestada küberturvalisuse seaduse § 7 lõike 2 eri punktidenä (sh praegune lõige 2 oleks olnud sellele järgnenud lõigete hulgas). Eesti Haiglate Liit esitas järgmise kommentaari (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), kommentaar nr 23.1):

Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 (edaspidi NIS2) artikkel 21 lõige 2 (d) käsitleb küberturvalisuse riskijuhtimise meetmeid, mida elutähtsad ja olulised üksused peavad rakendama. NIS2 kohustab elutähtsaid ja olulisi üksuseid rakendama kõiki ohte

⁷² <https://akit.cyber.ee/term/3928-tarneahel>

⁷³ <https://sonaveeb.ee/search/unif/dlall/dsall/tarneahel/1/est>

hõlmaval lähenemisviisil asjakohaseid ja proportsionaalselt tehnilisi, tegevuslikke ja korralduslikke meetmeid, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust, et ennetada või minimeerida intsidentide mõju nende teenuste saajatele ja muudele teenustele.

NIS2 rõhutab riskide juhtimist ja proportsionaalsust, samas kui küberturvalisuse seaduse eelnõu § 7 lõige 2 punkt 6 kehtestab turvameetmete rakendamisel üldise kohustuse “Tagama süsteemi tarneahela turvalisuse”.

Meie hinnangul võib nõue olla ebarealistlik, sest teenuse osutajal ei pruugi olla alati täielikku kontrolli kogu tarneahela üle, eriti kui tegemist on suuremahuliste ja keerukate tarneahelatega. Tarnijate ja koostööpartnerite regulaarne hindamine suurendab ka teenuseosutajate halduskoormust ja võib põhjustada tarnekatkestusi, kui tarnijad ei vasta kehtestatud turbenõuetele.

Teeme ettepaneku muuta eelnõu [küberturvalisuse seaduse] § 7 lõige 2 punkte 1 ja 6 alljärgnevalt:

(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud:

1) koostama ja kehtestama infoturvariskide kaalutlemise metoodika ja protseduurid (sh rakendama proportsionaalseid riskijuhtimise meetmeid süsteemi tarneahela turvalisuse tagamiseks);

6) tagama koostööpartnerite vahelistes lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise;

Ettepanekus välja toodud täpsustus “proportsionaalsed riskijuhtimise meetmed” muudab nõude paindlikumaks ja võimaldab teenuse osutajatel kohandada riskijuhtimise meetmeid vastavalt oma suurusele, riskitasemele ja ressurssidele. Samuti vähendab muudatus ebarealistlike ootusi, mille kohaselt peab teenuse osutaja turvameetmete rakendamisel “tagama süsteemi tarneahela turvalisuse”. Lisaks suurendab muudatus vastavust NIS2 direktiivi artikli 21 nõuetega, mis rõhutavad proportsionaalsust ja riskipõhist lähenemist.

Eelnõu [küberturvalisuse seaduse] § 7 lõike 2 punkti 6 täpsustus keskendub konkreetsele tegevusele ja vähendab üldistust ning suunab tegevust paremini.

Eesti Haiglate Liidu kommentaari ei võetud kõnealuse punkti sõnastamisel arvesse, kuna proportsionaalsuse ja riskipõhise lähenemise nõuded on sätestatud küberturvalisuse seaduse § 7 lõike 2 punktides 4 ja 5. Seetõttu ei ole seda aspekti vaja määruses nr 121 korrata.

Eesti Ravimihulgitajate Liit esitas järgmise kommentaari (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), kommentaar nr 31.6):

Eelnõus tuleks täpsemalt ja direktiivile vastavalt ka kitsamalt piiritleda teenuse osutaja kohustus „tagada süsteemi tarneahela turvalisus“.

Erinevalt eelnõus pakutud [küberturvalisuse seaduse] § 7 lg [2] p 6 sõnastusega rõhutab ja toob NIS2 direktiiv tarneahela turvalisuse osas ennekõike esile üksuse ja tema otseste tarnijate või teenuseosutajate vahelised suhted.

Seega on direktiivi põhirõhk suunatud just eelnimetatud kitsamalt piiritletud suhetele, mitte sama sügavus- ja rõhuasetusega kogu tarneahelale. Sama põhimõtte peaks selgelt väljenduma ka eelnõus.

Punktis 4.1 on otseselt mainitud „otseseid tarnijaid“, st need on hõlmatud terminiga „välised partnerid“, st „väliste partnerite“ all mõeldakse ka otseseid tarnijaid. Ka kommenteeritava lisa kehtiv punkt 4 hõlmab juba oma mõttelt „otseseid tarnijaid“, kuid kõnesoleva muudatusega soovitakse taolised üksused eraldi välja tuua, et tekiks selgem seos NIS2-direktiivi artikli 21 lõike 2 punktiga d. Punktis 4.1 tehtav muudatus siiski ei tähenda, et teenuseosutaja ei võiks teha enda väliste osapoolte tarneahelas põhjalikumat (tausta)kontrolli, kui vastav vajadus ilmneb näiteks riskihinnangust, millele on omakorda andnud tõuke teenuseosutaja enda kohustused, vajadused või kahtlused. Siinkohal peab ka arvestama asjaolu, et tarneahela suhtes (tausta)kontrolli tegemise kohustus on sisuliselt ette nähtud ka isikuandmete kaitse valdkonnas

ning see ei ole seotud ainult „otsese tarnija“ olukorraga –vt isikuandmete kaitse üldmääruse⁷⁴ artikli 28 lõiked 2 ja 4:

2. *Volitatud töötleja ei kaasa teist volitatud töötlejat ilma vastutava töötleja eelneva konkreetse või üldise kirjaliku loata. Üldise kirjaliku loa korral teavitab volitatud töötleja vastutavat töötlejat kõigist kavandatavatest muudatustest, mis puudutavad teiste volitatud töötlejate lisamist või asendamist, andes seeläbi vastutavale töötlejale võimaluse esitada selliste muudatuste suhtes vastuväiteid.*

4. *Kui volitatud töötleja kaasab vastutava töötleja nimel konkreetsete isikuandmete töötlemise toimingute tegemiseks teise volitatud töötleja, nähakse lepingus või muus liidu või liikmesriigi õiguse kohases õigusaktis asjaomase teise volitatud töötleja suhtes ette samad andmekaitsekohustused, mis on sätestatud lõikes 3 osutatud vastutava töötleja ja volitatud töötleja vahelises lepingus või muus õigusaktis; eelkõige annab see piisava tagatise, et rakendatakse asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine vastaks käesoleva määruse nõuetele. Kui see teine volitatud töötleja ei täida oma andmekaitsekohustusi, jääb algne volitatud töötleja vastutava töötleja ees täielikult vastutavaks kõnealuse teise volitatud töötleja kohustuste täitmise eest.*

Eesti Vee-ettevõtete Liit esitas järgmise kommentaari (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), kommentaar nr 32.3):

Eelnõu punktis 26, millega muudetakse küberturvalisuse seaduse §-i 7 lg 2 p-i 6 kohustub teenuse osutaja tagama süsteemi tarneahela turvalisuse, sh teenuse osutaja ja tema koostööpartnerite vahelistes lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise.

Palume täpsustada eelnõus või vähemalt selgitada seletuskirjas, millised on need turvameetmed, mida teenuse osutaja peaks koostööpartneri lepingus sätestama? Kas piisab üldisest viitest, et tellija on teenuse osutajaks [küberturvalisuse seaduse] tähenduses ning seega kohustub koostööpartner arvestama [küberturvalisuse seadusest] tulenevaga, järgima vähemalt keskmist küberturbe taset ning teavitama tellijat puudutavatest intsidentidest [küberturvalisuse seaduses] toodud tähtjajooksul? Kui sellest ei piisa, siis palume täpsustada, mida konkreetselt oodatakse?

Lisaks palume täpsustada, mida tähendab regulaarne ülevaatus ja ajakohastamine? Milline on regulaarsus või kas teenuse osutaja määrab selle ise? Kuidas toimub turvameetmete ajakohastamine olukorras, kus koostöölepingu muutmine toimub vaid poolte kokkuleppel (ja sageli teenuse osutajate puhul veel ka riigihanke tulemusel ehk muutmisele kehtivad veel eraldiseisvad reeglid)?

NIS2-direktiiv ei näe ette konkreetsemaid meetmeid, mida teenuseosutaja peaks koostööpartneriga sõlmitavas lepingus sätestama. Seetõttu seda määruse kõnesoleva sättega ei täpsustata. Samas on näiteks E-ITSi puhul esitatud kommentaariga seotud väljast tellimise moodul OPS.2.3. ja ka moodul OPS.3.2. Sarnaseid nõudeid peab rakendama ka teenuseosutaja, kes rakendab E-ITSi asemel alternatiivset standardit. Kokkulepete muutmise regulaarsuse määrab teenuseosutaja ise. Kui mõnest õigusaktist tulenevalt on tekkinud uued kohustused, siis selle alusel saabki osapoolte kokkuleppel lepingut muuta. Kui üldine ohupilt muutub, siis tuleb samuti lepingut ajakohastada. Kui välise partneri turvatase pole piisav, tuleb teenuseosutajal endal rakendada piisavaid lisameetmeid võimalike riskide vähendamiseks. Nõue tagada lepingute muutmise võimalus on tingitud just sellest, et ka pikaajaliste partneritega saaks aeg-ajalt küberturvalisuse teemad omavahel uuesti kokku leppida.

Kommenteeritava punktiga seotud meetmete puhul on võimalik tuua paralleeli ka rakendusmääruse (EL) 2024/2690 artikli 2 ja rakendusmääruse lisa punktiga 1.3 ning punktiga 5 koos selle alapunktidega. Näiteks ei sätesta NIS2-direktiiv, milline võiks olla

⁷⁴ Algteksti leiab aadressil: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>; konsolideeritud teksti aadressil: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02016R0679-20160504>.

kommenteeritava punktiga seotud regulaarse ülevaatuse intervall. Mainitud rakendusmääruse lisa punktis 5.1.6 on seda selgitatud järgmiselt: *Asjaomased üksused vaatavad tarneahela turvalisuse põhimõtted läbi ning jälgivad ja hindavad tarnijate ja teenuseosutajate küberturvalisuse tavade muutumist ning vajaduse korral tegutsevad selle põhjal plaaniliste ajavahemike järel ja siis, kui aset leiavad olulised muutused tegevuses või riskides või olulised intsidendid, mis on seotud IKT-teenuste osutamisega või mis mõjutavad tarnijatelt või teenuseosutajatelt pärit IKT-toodete turvalisust. Selle punkti puhul on rakendusmääruse punktis 5.1.7 ette nähtud, et selle nõude kohaldamiseks teevad asjaomased üksused järgmist: a) jälgivad regulaarselt teenusetasemelepete rakendamist käsitlevaid aruandeid, kui see on asjakohane; b) vaatavad läbi tarnijatelt ja teenuseosutajatelt pärit IKT-toodete ja IKT-teenustega seotud intsidendid; c) hindavad plaanivälise läbivaatamise vajalikkust ja dokumenteerivad oma tähelepanekud arusaadaval viisil; d) analüüsivad tarnijatelt ja teenuseosutajatelt pärit IKT-toodete ja IKT-teenustega seotud muutustega kaasnevaid riske ja võtavad vajaduse korral õigeaegselt leevendavaid meetmeid.*

Lisa uue punktiga 4.2 (kehtiva lisa punkt 4.2 on edaspidi punkt 4.3) nähakse ette, et teenuseosutaja peab väliste partnerite halduse valdkonnas võtma turvameetmete asjakohasust kaaludes arvesse välistele osapooltele eriomaseid turvahaavatavusi, nende toote üldist kvaliteeti ja küberturvalisusega seotud tavadid, sealhulgas toote turvalise arendamise korda ning NIS2-direktiivi artikli 22 lõike 1 kohaselt korraldatud kriitilise tähtsusega tarneahelate turvariskide koordineeritud hindamise tulemusi. Sellega võetakse üle NIS2-direktiivi artikli 21 lõige 3.

Termini „turvahaavatavus“ definitsiooni ja selgituste kohta vt ülevõtmisseaduse kohase küberturvalisuse seaduse § 2 punkt 31 ja selle selgitus.

NIS2-direktiivi artikli 22 lõike 1 kohaselt võib NIS2-direktiivi artikli 14 kohane koostöörühm koostöös Euroopa Komisjoni ja Euroopa Liidu Küberturvalisuse Ametiga teha kindlate kriitilise tähtsusega IKT-teenuste, IKT-süsteemide või IKT-toodete tarneahelate turberiski koordineeritud hindamisi, võttes arvesse tehnilisi ja asjakohasel juhul ka muid kui tehnilisi riskitegureid. Üheks selliseks hindamiseks on näiteks ELi küberturvalisuse riski hindamine ja stsenaariumid telekommunikatsiooni ja energeetika sektorites.⁷⁵

Ülevõtmisseaduse vastuvõtmisele eelnenud menetluse käigus esitati ka kõnesolevate sätete kohta järgmine kommentaar (vt ülevõtmisseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), Riigi Infosüsteemi Ameti kommentaar nr 17.43):

Teeme ettepaneku sõnastada eelnõu [küberturvalisuse seaduse] § 7 lg 2² p 1 järgmiselt:

„(2²) Käesoleva paragrahvi lõike 2 punktis 6 nimetatud tarneahela turvalisusega seotud turvameetmete asjakohasust kaaludes võtab teenuse osutaja arvesse:

1) koostööpartnerile eriomaseid nõrkusi, koostööpartneri toote üldist kvaliteeti, elutsüklihaldust ja küberturvalisuse tavadid, sealhulgas toote turvalise arenduse korda;“.

Selgitame, et ettepanek lisada sõna "elutsüklihalduse" annaks arusaamise taakvara tekke riskidest juba toote kasutamise plaanimise etapis.

Esitatud kommentaari ei arvestatud, kuna eesmärk on NIS2-direktiivi minimaalse ülevõtmise huvides lähtuda artikli 21 lõike 3 sõnastusest ja seda mitte laiendada.

Lisa uue punktiga 5.4 nähakse ette, et teenuseosutaja peab küberintsidentide halduse valdkonnas võtma kasutusele abinõud intsidentide mõju vähendamiseks ja leviku piiramiseks. Sellega võetakse üle NIS2-direktiivi artikli 21 lõike 2 punkt b (*[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: .. b) intsidentide käsitlemist*). Nende meetmete puhul on võimalik tuua paralleeli ka

⁷⁵ EU cybersecurity risk evaluation and scenarios for the telecommunications and electricity sectors, <https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>

rakendusmääruse (EL) 2024/2690 artikli 2 ja rakendusmääruse lisa punktiga 3 koos selle alapunktidega.

Ülevõtmiseaduse vastuvõtmisele eelnenud menetluse käigus esitati kõnesoleva sätte kohta järgmine kommentaar (vt ülevõtmiseaduse eelnõu seletuskirja lisa 3 (märkuste tabel), Riigi Infosüsteemi Ameti kommentaar nr 17.39): *Teeme ettepaneku sõnastada eelnõu [küberturvalisuse seaduse] § 7 lg 2 p 1-3 ja 9-14 järgmiselt: „(2) Teenuse osutaja on turvameetmete rakendamisel kohustatud: .. 3) tagama küberintsidentide avastamise ja halduse protseduuride toimimise; ..* Kommenteeritav alapunkt on üks osa küberintsidentide avastamise ja haldamise protseduuri nõuetest, mis on ette nähtud ennekõike kommenteeritava lisa punkti 5 teistes alapunktides. Seega on eeltoodud kommentaariga arvestatud punkti 5 puhul tervikuna.

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 mitteleidv. 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 rakendada ei pea. Tegelikult on tole punkti puhul algusest saadik mõeldud, et tarkvara eemaldamiseks on alus, kui korraga kehtib vähemalt üks kahest nimetatud tingimusest. Seetõttu on tole 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 13 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 ülevõtmiseadusest, 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 töötaja, 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.

Paragrahviga 4 nähakse ette määruse jõustumise aeg, milleks on 1. aprill 2026 (vt käesoleva seletuskirja punkt 6).

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu järgib NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiivi võttis ennekoike 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 54¹ alapunkt 1¹;
- 2) artikli 16 lõige 2 = määrusega nr 319 kinnitatud „Justiits- ja digiministeeriumi põhimääruse” punkti 54¹ alapunkt 1¹;
- 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 punkt 1.4 kuid seotud on ka 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 punkt 1.5, kuid seotud on ka 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, 1.6, 2.3, 2.4, 2.6, 3.2, 3.5, 3.7, 6.2, 6.6, 7.3, 7.5 ning punktid 8 ja 9 tervikuna, kuid seotud on ka punktid 6.3, 7.10 ja 7.11;
- 12) artikli 21 lõike 2 punkt j = määruse nr 121 lisa punkt 2.5 ja 5.3, kuid seotud on ka punktid 1.4 ja 6.4;

13) artikli 21 lõige 3 = määruse nr 121 lisa punktid 4.1 ja 4.2.

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 konkreetset 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 (st ennekõike selle lisa asendamine) on teatav mõju. Selle mõju laadi ja ulatust on hinnatud ülevõtmisseaduse eelnõu seletuskirjas (vt ülevõtmisseaduse eelnõu seletuskirja⁷⁶ punkt 6.1.), mistõttu mõjuhindamist siin ei korrata. Lisaks leevendatakse eelnõuga nende teenuseosutajate (ennekõike erasektori, kuid sisuliselt ka avaliku sektori 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. Seeläbi on eelnõuga kavandatud Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitusala 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.

⁷⁶ Vt altviidet nr 1.

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

Eelnõukohase määruse rakendamisega ei prognoosita tulusid.

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 seletuskirja⁷⁷ 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,⁷⁸ 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, kuid sisuliselt ka avaliku sektori 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. Seega on eelnõukohase määrusega tehtav Eesti infoturbestandardi või selle alternatiivina kasutatava standardi käsitusala muudatus halduskoormuse vähendamise lisameede, mis leevendab eelnõukohase määruse mõju.

Määruses nr 1 tehtavad muudatused ei too kaasa riigi ja kohaliku omavalitsuse tegevusi ega kulusid.

6. Määruse jõustumine

Määrus jõustub 1. aprillil 2026. Jõustumisaja määramisel on lähtutud kuupäevast, mis ajaks on võimalik läbida eelnõu avalik koostööst ning tagada eelnõukohase määruse vastuvõtmine Vabariigi Valitsuses.

7. Eelnõu koostööstamine, huvirühmade kaasamine ja avalik konsultatsioon

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.

⁷⁷ Vt altviidet nr 1.

⁷⁸ <https://eits.ria.ee/et/abimaterjalid/tugirakendus>

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

Eelnõu saadeti arvamuse avaldamiseks Riigikogu Kantseleile, Riigikontrollile, Vabariigi Presidendi Kantseleile, Õiguskantsleri Kantseleile, Andmekaitse Inspektsioonile, Eesti Pangale, Riigi Infosüsteemi Ametile, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusele, Registrate ja Infosüsteemide Keskusele, Riigiside Sihtasutusele, Eesti Interneti 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, Eesti Kaubandus-Tööstuskojale, Eesti Põllumajandus-Kaubanduskojale, Eesti Toiduainetööstuse Liidule ja Eesti Kaupmeeste Liidule.