06.01.2026

Justiits- ja digiministri määruse „Majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määruse nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ muutmine“ eelnõu
SELETUSKIRI

1. Sissejuhatus

1.1. Sisukokkuvõte

Küberturvalisuse 2. direktiiv ehk NIS2-direktiiv võetakse suuremas osas üle küberturvalisuse seaduse ja teiste seaduste muutmise seadusega (küberturvalisuse 2. direktiivi ülevõtmine, eelnõu 739 SE (edaspidi *739 SE*)). Siin kommenteeritava eelnõu kohaselt võetakse üle ainult NIS2-direktiivi artikli 10 lõiked 1, 3–5, 7 ja 8, artikli 11 lõiked 1 ja 3–5, artikli 12 lõige 1, artikli 14 lõige 3 ja artikli 16 lõige 2 osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega.
Eelnõu kohaselt sätestatakse, et Riigi Infosüsteemi Amet täidab küberturvalisuse seaduse § 5 tähenduses pädeva asutuse, ühtse kontaktpunkti, ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse, küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid ning koordineerib küberintsidentide käsitlemist. Sama amet osaleb ka oma pädevuse kohaselt NIS2-direktiivi artiklis 14 nimetatud koostöörühma tegevuses, artiklis 16 nimetatud Euroopa küberkriisiga tegelevate kontaktasutuste võrgustiku töös ja küberturvalisuse seaduse §-s 5 nimetatud küberintsidentide käsitlemise riiklike üksuste võrgustiku töös. Määrusega täpsustatakse ka ameti alla kuuluva küberintsidentide käsitlemise üksuse olemust ja ülesandeid.
Kuna 739 SE suurendas halduskoormust (küberturvalisuse seadust täiendati uute subjektidega, kes peavad seaduse nõudeid täitma), nähti halduskoormuse tasakaalustamine ette Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega. Need muudatused jõustusid 1. oktoobril 2025. Siin kommenteeritav eelnõu ei näe ette halduskoormuse kasvu, tehtavad muudatused on seotud ennekõike ühe ametiasutuse (Riigi Infosüsteemi Ameti) töökoormusega.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@justdigi.ee). Eelnõu on keeleliselt toimetanud Justiits- ja Digiministeeriumi õiguspoliitika osakonna õigusloome korralduse talituse toimetaja Inge Mehide (inge.mehide@justdigi.ee).

1.3. Märkused

Eelnõu on seotud küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõuga 739 SE.[1]

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

Eelnõukohase määrusega muudetakse majandus- ja kommunikatsiooniministri 25. aprilli 2011. a määrust nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ (edaspidi *määrus nr 28*) (RT I, 27.12.2024, 10).

Eelnõuga 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 10 lõiked 1, 3–5, 7 ja 8, artikli 11 lõiked 1 ja 3–5, artikli 12 lõige 1, artikli 14 lõige 3 ja artikli 16 lõige 2.

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“.[2] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027 ELi direktiivide valdkonna all olev ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Kuna 739 SE suurendas halduskoormust (küberturvalisuse seadust täiendati uute subjektidega, kes peavad seadusega kehtestatavaid nõudeid täitma), nähti halduskoormuse tasakaalustamine ette Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega, mis jõustusid 1. oktoobril 2025.

2. Eelnõu sisu ja võrdlev analüüs

Määruse nr 28 muutmise eelnõu koosneb seitsmest punktist.

Punktiga 1 muudetakse määruse nr 28 § 8 lõike 1 punkti 9. Kommenteeritava muudatusega võetakse üle NIS2-direktiivi artikli 11 lõike 1 teine lõik (lause *CSIRTid võivad osaleda rahvusvahelistes koostöövõrgustikes*). Selle kohta saab lugeda ka eelnõu punktis 6 viidatud NIS2-direktiivi põhjendusi. Muudatus tehakse eelmainitud paragrahvis, kuna selle sisu on kõige sarnasem sättega, mis tuleb NIS2-direktiivist üle võtta. Kuna sama ülesande sisu kohaldub praktikas ka muudele Riigi Infosüsteemi Ameti struktuuriüksustele[3], on võimalik teha see muudatus ameti põhiülesandeid sätestavas lõikes. Muudatuse tulemusena on kommenteeritava punkti uus sõnastus (allajoonitud osa on lisandunud tekstiosa) järgmine: „Amet täidab oma tegevusvaldkondades järgmiseid põhiülesandeid: .. rahvusvahelise koostöö arendamine ja korraldamine ning rahvusvahelisel suhtlemisel riigi esindamine ameti pädevuse piires, sealhulgas rahvusvahelistes koostöövõrgustikes.“ See täiendus tagab selguse, et punkti esimene pool hõlmab ka koostööd rahvusvahelistes koostöövõrgustikes.

Punktiga 2 muudetakse määruse nr 28 § 8 lõike 4 punkti 3.
Muudetud punktis sätestatakse, et Riigi Infosüsteemi Amet täidab küberturvalisuse valdkonnas küberturvalisuse seaduse § 5 tähenduses pädeva asutuse, ühtse kontaktpunkti, ulatuslike küberintsidentide ja kriiside ohjamise eest vastutava pädeva asutuse, küberintsidentide

[2] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[3] Määruse nr 28 § 10 lõige 1: „Ameti struktuuriüksused on küberturvalisuse keskus, riigi infosüsteemi teenistus ja peadirektorile vahetult alluvad osakonnad. Lisaks võivad ameti struktuuri kuuluda teenistujad, kes ei ole ühegi struktuuriüksuse koosseisus ning kes alluvad vahetult peadirektorile või peadirektori määratud teenistujale.“

käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid ning koordineerib küberintsidentide käsitlemist. Need ülesanded anti 739 SE kohase küberturvalisuse seaduse § 5 lõike 3 järgi Riigi Infosüsteemi Ametile, kuid siin kommenteeritava muudatusega täpsustatakse nende ülesannete täitmise jaotust ameti sees.

Punktiga 3 täiendatakse määruse nr 28 § 8 lõiget 4 punktiga 3^1.
Tehtav muudatus on seotud NIS2-direktiivi artikli 14 lõike 3 esimese lause (lause *Koostöörühma moodustavad liikmesriikide, komisjoni ja ENISA esindajad.*) ning artikli 16 lõike 2 esimese lõike (lauseosa *EU-CyCLONe-sse kuuluvad liikmesriikide küberkriisi ohjamise asutuste esindajad ..*) ülevõtmisega.
Osa NIS2-direktiivis kasutatud termineid võetakse 739 SE kohaselt küberturvalisuse seadusesse või siin kommenteeritavasse määrusesse üle teises sõnastuses. Näiteks on NIS2-direktiivi artikli 9 lõikes 1 kasutatud terminit „küberkriisi ohjamise asutus“ termini „ulatuslike küberintsidentide ja kriiside ohjamise eest vastutav pädev asutus“ kohta. Viimati nimetatud sõnastust kasutatakse ka Eesti õiguses.
Kommenteeritava punktiga on kavas anda asjaomased volitused Riigi Infosüsteemi Ametile, 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 antakse ka Justiits- ja Digiministeeriumile, lisades sarnase esindusvolituse ministeeriumi põhimäärusesse teise eelnõuga.
Riigi Infosüsteemi Ametile anti 739 SE kohaselt küberintsidentide käsitlemise riiklike üksuste võrgustikus osalemise ülesanne (vt eelnõukohase küberturvalisuse seaduse § 5 lõike 3 punkti 5), kuid siin kommenteeritava muudatusega täpsustatakse nii selle kui ka siinses punktis nimetatud muude ülesannete täitmise jaotust ameti sees.

Punktiga 4 täiendatakse määruse nr 28 teist peatükki §-ga 9^1. Selle paragrahvi lisamine on seotud NIS2-direktiivi artikli 10 lõike 1 punktide a–f ja artikli 11 lõike 1 esimese lõigu ülevõtmisega. Selle kohta saab ka lugeda eelnõu § 1 punktis 6 viidatud NIS2-direktiivi põhjendusi.
Eelnõu koostades oli esialgu kavas luua järgnevad sätted ainult küberintsidentide käsitlemise üksuse kohta, kuid töö käigus otsustati kehtestada asjaomased kohustused laiemalt, st panna need ka teistele Riigi Infosüsteemi Ameti struktuuriüksustele[4]. Need on oma sisult sellised kohustused, mida on võimalik panna ka ameti teistele struktuuriüksustele. Seetõttu loodi kõnealused sätted eraldi paragrahvina määruse nr 28 teises peatükis, mis reguleerib ameti tegevusvaldkonda ja põhiülesandeid.
Kommenteeritava paragrahvi **punktiga 1** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkti a esimene lause (lause *CSIRTid peavad tagama oma sidekanalite laialdase kättesaadavuse, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad neil teistega ja teistel nendega igal ajal ühendust võtta*). Kommenteeritavas punktis hõlmavad sõnad „sidekanalite laialdane ja pidev kättesaadavus“ ja „mitmesuguseid töökindlaid vahendeid“ ka olukorda, kus on vaja vältida nõrku lülisid (ingl *single point of failure*). Kommenteeritava paragrahvi **punktiga 2** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkti a teine lause (lause *CSIRTid määravad selgelt kindlaks sidekanalid ning teevad need oma sihtrühmadele ja koostööpartneritele teatavaks*). Kommenteeritava paragrahvi **punktiga 3** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punktid b (lause *CSIRTide ametiruumid ja nende tööd toetavad infosüsteemid peavad asuma turvalises kohas*) ja f (lause *CSIRTidel peavad olema varusüsteemid ja varutööruumid, et tagada oma teenuste toimepidevus*). Kommenteeritava

[4] Vt eelmist allviidet.

paragrahvi **punktiga 4** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkt c (lause *CSIRTidel peab olema päringute haldamiseks ja suunamiseks sobiv süsteem, ennekõike selleks, et tõhustada üleandmisi*). Kommenteeritava paragrahvi **punktiga 5** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkt d (lause *CSIRTid peavad tagama oma tegevuse konfidentsiaalsuse ja usaldusväärsuse*). Kommenteeritava paragrahvi **punktiga 6** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkt e (lauseosa *CSIRTidel peab olema piisavalt töötajaid, et tagada nende teenuste alaline kättesaadavus ..*). Kommenteeritava paragrahvi **punktiga 7** võetakse üle NIS2-direktiivi artikli 11 lõike 1 punkt e (lauseosa *[CSIRTid] .. peavad tagama oma töötajatele asjakohase väljaõppe*).

Punktiga 5 muudetakse määruse nr 28 § 13 lõike 1 punkti 1. Muudatuse tulemusena on selle punkti sõnastus (alla joonitud osa on lisanduv tekstiosa) järgmine: „Küberturvalisuse keskuse ülesanded on: .. Eesti riigi tasemel CERT (Computer Emergency Response Team), küberintsidentide käsitlemise üksuse ja turvahaavatavuse koordineeritult avaldamise koordinaatori ülesannete täitmine, sealhulgas Eesti arvutivõrkudes toimuvate turvaintsidentide käsitlemine.“ Muudatuse tulemusena on selge, et nii küberintsidentide käsitlemise üksuse kui ka turvahaavatavuse koordineeritult avaldamise koordinaatori ülesanded on ennekõike küberturvalisuse keskuse ülesannete hulgas. Samuti tekib parem seos ja selgus ka muudatustega, mis tehakse eelnõu punkti 6 kohaselt.
Termin „küberintsidentide käsitlemise üksus“ defineeritakse 739 SE kohaselt küberturvalisuse seaduse § 2 punktis 20 kui „ekspertide grupp, kelle ülesanne on teha küberintsidendi käsitlemist toetavaid toiminguid“. Küberintsidendi käsitlemine on sama paragrahvi kohaselt „toimingud ja menetlused, mille eesmärk on küberintsidenti ennetada, tuvastada, analüüsida, ohjata või lahendada ja sellest taastuda“.

Punktiga 6 täiendatakse määruse nr 28 § 13 lõigetega 1^1–1^4. Nende lõigete lisandumine on seotud NIS2-direktiivi artikli 10 lõigete 1, 3–5, 7 ja 8, artikli 11 lõigete 1 ja 3–5 ning artikli 12 lõike 1 ülevõtmisega. Kommenteeritava lõikega on seotud ka NIS2-direktiivi põhjendused 41–47:
(41) Liikmesriigid peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et ennetada, vältida ja avastada intsidente ja riske ning neile reageerida ja nende mõju leevendada. Seepärast peaksid liikmesriigid [NIS2-direktiivi] alusel looma või määrama ühe või mitu CSIRTi ning tagama, et neil on piisavad vahendid ja tehniline võimekus. CSIRTid peaksid vastama [NIS2-direktiivis] sätestatud nõuetele, et tagada tulemuslik ja ühilduv võimekus tulla toime intsidentide ja riskidega ning tagada liidu tasandil tõhus koostöö. Liikmesriigid peaksid saama CSIRTideks määrata ka olemasolevaid infoturbeintsidentidega tegelevaid rühmi (CERTe). Et tugevdada üksuste ja CSIRTide vahelist usalduslikku suhet olukorras, kus CSIRT on pädeva asutuse osa, peaks liikmesriikidel olema võimalik kaaluda CSIRTide operatiivülesannete funktsionaalset eraldamist, eelkõige seoses sellega, mis puudutab teabevahetust ja üksuste toetamist ning pädevate asutuste järelevalvetegevust.
(42) CSIRTide ülesandeks on intsidentide käsitlemine. See hõlmab suure hulga mõnikord tundlike andmete töötlemist. Liikmesriigid peaksid tagama, et CSIRTidel on teabevahetuse ja töötlemise taristu, samuti hästi varustatud töötajad, mis tagab nende tegevuse konfidentsiaalsuse ja usaldusväärsuse. CSIRTid võiksid sellega seoses vastu võtta ka tegevusjuhendid.
(43) Mis puutub isikuandmetesse, siis peaks CSIRTidel olema võimalik kooskõlas määrusega (EL) 2016/679 teha elutähtsa või olulise üksuse taotlusel üksuse teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide ennetavat kontrolli. Kui see on kohaldatav, peaksid liikmesriigid püüdma tagada kõikide valdkondlike CSIRTide tehnilise võimekuse võrdse taseme. Liikmesriikidel peaks olema võimalik paluda oma CSIRTide arendamisel ENISA abi.

(44) CSIRTidel peaks üksuse taotluse alusel olema võimalik elutähtsa[5] või olulise üksuse kõiki internetiühendusega varasid pidevalt jälgida, nii siseruumides kui ka väljaspool, et tuvastada, mõista ja hallata üksuse üldisi organisatsioonilisi riske seoses hiljuti tuvastatud tarneahela kahjustuste ja kriitilisel tasemel nõrkustega[6]. Üksust tuleks julgustada CSIRTile teatama, kas tal on privilegeeritud juhtimisliides, kuna see võib mõjutada leevendusmeetmete võtmise kiirust.
(45) Arvestades küberturvalisuse alase rahvusvahelise koostöö tähtsust, peaks CSIRTidel olema võimalik lisaks [NIS2-direktiivi] kohaselt loodud CSIRTide võrgustikule osaleda ka rahvusvaheliste koostöövõrgustike töös. Seepärast peaks CSIRTidel ja pädevatel asutustel olema oma ülesannete täitmiseks võimalik vahetada teavet, sealhulgas isikuandmeid, kolmandate riikide riiklike küberturbe intsidentide lahendamise üksuste või pädevate asutustega, kui on täidetud liidu andmekaitseõiguses sätestatud tingimused isikuandmete edastamiseks kolmandatele riikidele, muu hulgas määruse (EL) 2016/679 artiklis 49 sätestatud tingimused.
(46) Oluline on tagada piisavad vahendid [NIS2-direktiivi] eesmärkide saavutamiseks ning võimaldada pädevatel asutustel ja CSIRTidel täita selles sätestatud kohustusi. Liikmesriigid võivad riiklikul tasandil kehtestada rahastamismehhanismi, et katta [NIS2-direktiivi] kohaselt liikmesriigis küberturvalisuse eest vastutavate avaliku sektori asutuste ülesannete täitmisega seotud vajalikud kulud. Selline mehhanism peaks olema kooskõlas liidu õigusega, proportsionaalne ja mittediskrimineeriv ning võtma arvesse erinevaid lähenemisviise turvaliste teenuste pakkumisele.
(47) CSIRTide võrgustik peaks jätkuvalt aitama suurendada kindlustunnet ja usaldust ning edendama kiiret ja tõhusat operatiivkoostööd liikmesriikide vahel. Et tõhustada operatiivkoostööd liidu tasandil, peaks CSIRTide võrgustik kaaluma võimalust kutsuda oma töös osalema küberturvalisuse poliitika kujundamisega seotud asjaomased liidu asutused ja ametid, näiteks Europoli.

Eelnõukohase määruse nr 28 § 13 **lõige 1[1]** on seotud NIS2-direktiivi artikli 10 lõigete 1 (kolmas lause), 3–5, 7 ja 8, artikli 11 lõike 1 (teine lõik), lõike 3 (esimese lõigu punktid a–h ja teine lõik) ning lõigete 4 ja 5 ülevõtmisega.
Osa NIS2-direktiivis kasutatud termineid võetakse 739 SE kohaselt küberturvalisuse seadusesse või siin kommenteeritavasse määrusesse üle teises sõnastuses. Näiteks mõeldakse NIS2-direktiivi termini „riiklike küberturbe intsidentide lahendamise üksus“ ehk lühendi CSIRT all Eesti õiguses „küberintsidentide käsitlemise üksust“; termin „elutähtis üksus“ on Eesti õiguses edaspidi „ülioluline üksus“; „nõrkus“ on Eesti õiguses edaspidi „turvahaavatavus“; „intsident“ on Eesti õiguses edaspidi „küberintsident“; „kohtuekspertiisiandmed“ on Eesti õiguses edaspidi „digitaalkriminalistika andmed“; „nõrkuste koordineeritud avalikustamise protsessi koordinaator“ on Eesti õiguses edaspidi „turvahaavatavuse koordineeritult avaldamise koordinaator“; „nõrkuste koordineeritud avalikustamine“ on Eesti õiguses edaspidi „turvahaavatavuse koordineeritult avaldamine“. Neid aspekte tuleb siin kommenteeritava eelnõu selgituste kontekstis arvestada.
Kommenteeritava lõike punktides olevaid ülesandeid täidab NIS2-direktiivi kohaselt ennekõike küberintsidentide käsitlemise üksus. 739 SE ja siin kommenteeritavate muudatuste kohaselt on vastava rolli täitja Riigi Infosüsteemi Amet, sh täpsustatakse eelnõu eelmises punktis tehtava muudatusega, et neid ülesandeid täidab ameti struktuuriüksuseks olev küberturvalisuse keskus. Sellest lähtudes on sõnastatud ka kommenteeritava lõike sissejuhatav lause.
Kommenteeritava lõike **punktiga 1** võetakse üle NIS2-direktiivi artikli 10 lõike 1 kolmas lause (lauseosa *CSIRTid peavad .. hõlmama vähemalt I ja II lisas osutatud sektoreid, allsektoreid või*

[5] 739 SE järgi küberturvalisuse seaduses „üliolulise üksuse“.
[6] 739 SE järgi küberturvalisuse seaduses „turvahaavatavustega“.

üksuste liike ning vastutama intsidentide käsitlemise eest kindla menetluse kohaselt). Kommenteeritava lõike **punktiga 2** võetakse üle NIS2-direktiivi artikli 10 lõige 5 (lause *CSIRTid osalevad artikli 19 kohaselt korraldatud vastastikuses hindamises*). Kommenteeritava lõike **punktiga 3** võetakse üle NIS2-direktiivi artikli 10 lõige 4 (lauseosa *CSIRTid teevad koostööd*). Kommenteeritava lõike **punktiga 4** võetakse üle NIS2-direktiivi artikli 10 lõiked 7 (laused 1 ja 2 ehk *CSIRTid võivad luua koostöösuhteid kolmandate riikide riiklike küberturbe intsidentide lahendamise üksustega. Selliste koostöösuhete osana hõlbustavad liikmesriigid tõhusat, tulemuslikku ja turvalist teabevahetust nende kolmandate riikide riiklike küberturbeintsidentide lahendamise üksustega, kasutades asjakohaseid teabevahetuse protokolle, sealhulgas fooriprotokolli)* ja 8 (*CSIRTid võivad teha kolmandate riikide riiklike küberturbeintsidentide lahendamise üksustega või samaväärsete kolmandate riikide asutustega koostööd, eelkõige selleks, et anda neile küberturvalisuse alast abi*). Kommenteeritava lõike **punktiga 5** võetakse üle NIS2-direktiivi artikli 10 lõige 4 (lause *CSIRTid teevad koostööd ning, kui see on kohane, vahetavad kooskõlas artikliga 29 asjakohast teavet elutähtsate ja oluliste üksuste sektoripõhiste või -vaheliste kogukondadega*). Kommenteeritava lõike **punktiga 6** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt a (lauseosa *korraldada küberohtude, nõrkuste ja intsidentide seiret ja analüüsi riiklikul tasandil*). Kommenteeritava lõike **punktiga 7** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt a (lauseosa *taotluse korral osutada abi asjaomastele elutähtsatele ja olulistele üksustele seoses nende võrgu- ja infosüsteemide reaalajas või reaalajalähedase seirega*). Kommenteeritava lõike **punktiga 8** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt b (lause *tagada küberohtude, nõrkuste ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadete edastamine ning teabe levitamine asjaomastele elutähtsatele ja olulistele üksustele ning pädevatele asutustele ning muudele asjaomastele sidusrühmadele, võimaluse korral reaalajalähedaselt*). Kommenteeritava lõike **punktiga 9** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt c (lauseosa *lahendada intsidente ning, kui see on kohaldatav, abistada asjaomaseid elutähtsaid ja olulisi üksusi*).

Kommenteeritava lõike **punktiga 10** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt d (lauseosa *koguda ja analüüsida kohtuekspertiisiandmeid ning analüüsida järjepidevalt riske ja intsidente ning tagada küberturvalisuse alane olukorrateadlikkus*). Kommenteeritavas punktis on mainitud ka „kohtuekspertiisiandmeid“ ehk inglise keeles *forensic data*. Üldreeglina on digitaalne kohtuekspertiis üks osa kohtuekspertiisist, mis on suunatud tõendite tuvastamiseks, saamiseks, töötlemiseks, analüüsimiseks ja raporteerimiseks ning on talletatud infosüsteemi digiseadmele või teistele andmekandjatele – seda kõike selleks, et see teave oleks kohtus vastuvõetav. Tõendite kogumine on ka osa küberturvalisuse valdkonnaga seotud rahvusvahelistest standarditest. Näiteks rahvusvahelise standardi ISO/IEC 27001:2002 lisa A 5.28 kohaselt peaksid organisatsioonid tuvastama, koguma, saama ja säilitama tõendeid, mis on seotud infoturbeintsidentidega. NIS2-direktiivi kontekstis tuleb „kohtuekspertiisiandmeid“ käsitada mitte ainult kriminaalõiguse valdkonnaga seotud kohtuekspertiisiandmetena, vaid pigem laiemalt ehk nende andmete kogumine ja analüüs võib aidata kasutada tõendeid ka teistes olukordades – näiteks selleks, et teha intsidendi tuumpõhjuse analüüsi või tegeleda vastavuskontrolliga. Tuleb arvestada asjaoluga, et NIS2-direktiiv ei anna küberintsidentide käsitlemise üksustele õiguskaitseasutuste ülesandeid ehk need ei tegele kriminaalmenetlusega. Sel puhul tehakse pigem koostööd õiguskaitseasutustega, näiteks selleks, et pakkuda õiguskaitseasutustele tuge nende algatatud kriminaalmenetlustes.

Kommenteeritava lõike **punktiga 11** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt e (lauseosa *kontrollida elutähtsa või olulise üksuse taotlusel ennetavalt selle üksuse võrgu- ja infosüsteeme, et teha kindlaks potentsiaalselt olulise mõjuga nõrkused*). Kommenteeritava lõike **punktiga 12** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt f (lauseosa *osaleda CSIRTide võrgustikus ning osutada teistele võrgustiku liikmetele*

nende taotluse korral oma võimekusele ja pädevusele vastavat vastastikust abi). Kommenteeritava lõike **punktiga 13** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt g (lauseosa *kui see on kohaldatav, tegutseda artikli 12 lõikes 1 osutatud nõrkuste koordineeritud avalikustamise protsessi koordinaatorina*). Kommenteeritava lõike **punktiga 14** võetakse üle NIS2-direktiivi artikli 11 lõike 3 esimese lõike punkt h (lauseosa *panustada artikli 10 lõike 3 kohaste turvaliste teabejagamisvahendite kasutuselevõtmisse*). Kommenteeritava lõike **punktiga 15** võetakse üle NIS2-direktiivi artikli 11 lõike 3 teine lõige (laused *CSIRTid võivad elutähtsate ja oluliste üksuste üldkasutatavaid võrgu- ja infosüsteeme ennetavalt väliselt kontrollida. Selline kontrollimine toimub nõrkade või ebaturvaliselt konfigureeritud võrgu- ja infosüsteemide tuvastamiseks ning asjaomaste üksuste teavitamiseks. Sellisel kontrollimisel ei tohi olla negatiivset mõju üksuste teenuste toimimisele*). Kommenteeritava lõike **punktiga 16** võetakse üle NIS2-direktiivi artikli 11 lõiked 4 (lause *CSIRTid loovad koostöösuhteid erasektori asjaomaste sidusrühmadega, et saavutada [NIS2-direktiivi] eesmärgid*) ja 5 (lause *Lõikes 4 osutatud koostöö hõlbustamiseks toetavad CSIRTid ühtsete või standardsete tavade, liigitamissüsteemide ja taksonoomiate kasutuselevõttu seoses järgmisega: a) intsidentide käsitlemise menetlused; b) kriisiohje ning c) artikli 12 lõike 1 kohane nõrkuste koordineeritud avalikustamine.*).

Eelnõukohase määruse nr 28 § 13 **lõikega 1[2]** võetakse üle NIS2-direktiivi artikli 11 lõike 3 kolmas lõige (lause *Esimeses lõigus osutatud ülesannete täitmisel võivad CSIRTid riskipõhise lähenemisviisi alusel teatavaid ülesandeid prioriseerida.).* „Esimese lõigu“ all ongi mõeldud kommenteeritava lõike punktides 6–14 sätestatud ülesandeid. Sarnast triaaži teeb Riigi Infosüsteemi Amet ka korrakaitseseaduse § 24 kohaselt tehtava ohuprognoosi alusel, kuid kuna korrakaitseseaduse kohaselt tehtav ohuprognoos on kohaldatav ainult erasektori ehk halduseväliste isikute suhtes ja NIS2-direktiiv on mõeldud kohalduma ka avaliku sektori suhtes, tuleb volitus küberintsidentide käsitlemise üksusele anda laiemalt, kui on ette nähtud korrakaitseseaduses. Siiski on kommenteeritavas lõikes märgitud ka ohuprognoos, et oleks üheselt selge, et see on üks lähenemisviis, millest lähtudes küberintsidentide käsitlemise üksus enda tööd planeerib.

Eelnõukohase määruse nr 28 § 13 **lõikega 1[3]** võetakse üle NIS2-direktiivi artikli 12 lõige 1.
NIS2-direktiiv näeb ette, et küberintsidentide käsitlemise üksus täidab turvahaavatavuse koordineeritult avaldamise koordinaatori ülesandeid. 739 SE ja siin kommenteeritavate muudatuste kohaselt täidab sellise koordinaatori rolli Riigi Infosüsteemi Amet, sh täpsustab eelnõu punktis 5 tehtav muudatus, et neid ülesandeid täidab ameti struktuuriüksuseks olev küberturvalisuse keskus. Sellest lähtudes on sõnastatud ka kommenteeritava lõike sissejuhatav lause.
Kommenteeritava lõike **punktiga 1** võetakse üle NIS2-direktiivi artikli 12 lõike 1 esimese lõigu teine lause (lause *Koordinaatoriks määratud CSIRT tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral suhtlust nõrkusest teavitava füüsilise või juriidilise isiku ning potentsiaalse nõrkusega IKT-toodete tootja või IKT-teenuste osutaja vahel, tegutsedes ükskõik kumma poole taotlusel*). Kommenteeritava lõike **punktiga 2** võetakse üle NIS2-direktiivi artikli 12 lõike 1 esimese lõigu punkt a (lause *Koordinaatoriks määratud CSIRTi ülesandeks on: a) teha kindlaks asjaomased üksused ja võtta nendega ühendust*). Selle punkti puhul on lisatud sõnad „teavitatud potentsiaalse turvahaavatavuse või turvahaavatavuse“, et tagada suurem selgus selles, mida peetakse sätte kontekstis silmas „asjaomase üksuse“ all. Sama selgitus kohaldub ka sama lõike punktidele 3 ja 7. Kommenteeritava lõike **punktiga 3** võetakse üle NIS2-direktiivi artikli 12 lõike 1 esimese lõigu punkt b (lauseosa *Koordinaatoriks määratud CSIRTi ülesandeks on: .. b) abistada nõrkusest teavitavaid füüsilisi ja juriidilisi isikuid ning ..*).
Kommenteeritava lõike **punktiga 4** võetakse üle NIS2-direktiivi artikli 12 lõike 1 esimese lõigu

punkt c (lauseosa *Koordinaatoriks määratud CSIRTi ülesandeks on: .. c) pidada läbirääkimisi avalikustamise tähtaegade üle ..*). Kuigi eelviidatud NIS2-direktiivi säte ei sõnasta otsesõnu, et tegemist on avalikkuse teavitamisega turvahaavatavusest, on eelnõus tehtud sellekohane täpsustus, et oleks konkreetsemalt aru saada, mis laadi avalikustamisega on tegemist. Kommenteeritava lõike **punktiga 5** võetakse üle NIS2-direktiivi artikli 12 lõike 1 esimese lõigu punkt c (lauseosa *Koordinaatoriks määratud CSIRTi ülesandeks on: .. c) .. hallata mitut üksust mõjutavaid nõrkusi*). Kommenteeritava lõike **punktiga 6** võetakse üle NIS2-direktiivi artikli 12 lõike 1 teise lõigu teine lause (lauseosa *Koordinaatoriks määratud CSIRT tagab, et teatatud nõrkusega seoses võetakse hoolikaid järelmeetmeid ..*). Kommenteeritava lõike **punktiga 7** võetakse üle NIS2-direktiivi artikli 12 lõike 1 teise lõigu teine lause (lauseosa *Koordinaatoriks määratud CSIRT .. tagab nõrkusest teatava füüsilise või juriidilise isiku anonüümsuse*). Kommenteeritav punkt on seotud ennekõike turvahaavatavusest teatava isiku anonüümsuse tagamisega teiste osapoolte kui küberintsidentide käsitlemise üksuse liikmete suhtes. Kui sätestada anonüümsuse tagamine ka selle üksuse ees, ei saa üksus täita kommenteeritava lõike punktis 1 olevat usaldusväärse vahendaja ülesannet ehk vajaduse korral küsida teatajalt lisainfot, mis aitab potentsiaalse või reaalse turvahaavatavuse olemust ning algpõhjuseid välja selgitada. Kommenteeritava lõike **punktiga 8** võetakse üle NIS2-direktiivi artikli 12 lõike 1 teise lõigu kolmas lause (lause *Kui teates osutatud nõrkus võib oluliselt mõjutada üksusi rohkem kui ühes liikmesriigis, teeb iga asjaomase liikmesriigi poolt koordinaatoriks määratud CSIRT asjakohasel juhul teiste koordinaatoriks määratud CSIRTidega CSIRTide võrgustikus koostööd*).

Eelnõukohase määruse nr 28 § 13 **lõike 1[4]** kohaselt tehakse Riigi Infosüsteemi Ameti peadirektorile volitus, millega ta võib lõike 1 punktis 4 ning lõigetes 1^1 ja 1^3 sätestatud ülesande või ülesanded anda sama määruse § 15 punkti 2 alusel üle ameti muule struktuuriüksusele, sätestades ülesande või ülesanded struktuuriüksuse põhimääruses. Määruse nr 28 § 15 punkti 2 kohaselt kinnitab ameti peadirektor osakondade ja teiste struktuuriüksuste põhimäärused, ameti asjaajamiskorra, töökorralduse reeglid ja muud töökorralduslikud dokumendid, ametnike ja töötajate töötasu ning ametijuhendid vastavuses õigusaktidega. Kommenteeritava muudatusega antakse ameti peadirektorile paindlikkus anda üks või mitu eelnõukohase määruse nr 28 § 13 asjakohastes lõigetes toodud ülesannet üle teisele struktuuriüksusele kui küberturvalisuse keskus. Kommenteeritava lõike puhul tähendab sõna „ülesanne“ nii ainsust kui ka mitmust. Määruse nr 28 § 10 lõige 1 sätestab: „Ameti struktuuriüksused on küberturvalisuse keskus, riigi infosüsteemi teenistus ja peadirektorile vahetult alluvad osakonnad. Lisaks võivad ameti struktuuri kuuluda teenistujad, kes ei ole ühegi struktuuriüksuse koosseisus ning kes alluvad vahetult peadirektorile või peadirektori määratud teenistujale.“
Näiteks on juba praegu ameti peadirektor sätestanud juhtimiskeskuse osakonna põhiülesandeks seire tagamise ja tegemise, mis on käsitatav eelnõukohase määruse nr 28 § 13 lõike 1^1 punktis 7 toodud ülesandena. Vastav ülesanne on leitav juhtimiskeskuse osakonna põhimäärusest.[7] Tegemist on sarnase ülesandega, mis on sätestatud ka määruse nr 28 § 13 lõike 1 punktis 4, mistõttu tehakse ka tolle ülesande puhul asjakohane volitus.

Punktiga 7 täiendatakse määrust nr 28 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 koostades.

[7] https://ria.ee/sites/default/files/vp_contacts/files/RIA-juhtimiskeskuse-osakonna-pohimaarus-juuni2025.pdf

Normitehniline märkus lisatakse määrusesse nr 28, kuna muudesse õigusaktidesse pole kavandatud NIS2-direktiivi kõiki artikli 10 lõikeid 1, 3–5, 7 ja 8, artikli 11 lõikeid 1 ja 3–5, artikli 12 lõiget 1, artikli 14 lõiget 3 ning artikli 16 lõiget 2 üle võtvaid sätted, mis on seotud Riigi Infosüsteemi Ametiga.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu järgib õigusnormide loomisel NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiiv võeti ennekõike üle 739 SEga, on selle seaduseelnõu materjalide juures ka NIS2-direktiivi vastavustabel. Seletuskirja siinses osas esitatakse need väljavõtted, mis on seotud siin kommenteeritava eelnõuga:
1) artikli 10 lõige 1 = määruse nr 28 § 13 lg 1^1 p 1;
2) artikli 10 lõige 3 = määruse nr 28 § 9 p 1 ja lg 1^1 p 14;
3) artikli 10 lõige 4 = määruse nr 28 § 13 lg 1^1 p 3 ja 5;
4) artikli 10 lõige 5 = määruse nr 28 § 13 lg 1^1 p 2;
5) artikli 10 lõige 7 = määruse nr 28 § 13 lg 1^1 p 4;
6) artikli 10 lõige 8 = määruse nr 28 § 13 lg 1^1 p 4;
7) artikli 11 lõige 1 = määruse nr 28 § 8 lg 1 p 9 ja § 9^1;
8) artikli 11 lõige 3 = määruse nr 28 § 13 lg 1^1 p-d 6–15 ja lg 1^2;
9) artikli 11 lõige 4 = määruse nr 28 § 13 lg 1^1 p 16;
10) artikli 11 lõige 5 = määruse nr 28 § 13 lg 1^1 p 16;
11) artikli 12 lõige 1 = määruse nr 28 § 13 lg 1^3;
12) artikli 14 lõige 3 = määruse nr 28 § 8 lg 4 p 3^1;
13) artikli 16 lõige 2 = määruse nr 28 § 8 lg 4 p 3^1.
Iga tehtava 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

Eelnõukohane määrus mõjutab ainult Riigi Infosüsteemi Ametit ja selle töökorraldust. Ameti põhimääruses tehtavad muudatused on põhimõttelised samad muudatused, mida on tervikuna hinnatud 739 SE seletuskirjas (vt 739 SE seletuskirja punkti 6.5), mistõttu nende mõjude hindamist siin ei korrata.

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

Eelnõuga tulu ei prognoosita.

Riigi Infosüsteemi Ameti põhimäärusega seotud muudatustega seotud tegevused ja kulude aspektid on hinnatud 739 SE seletuskirjas (vt 739 SE seletuskirja punkti 7, täpsemalt p 7.2), mistõttu hindamist siin ei korrata.

6. Määruse jõustumine

Eelnõu koostades kaaluti jõustumiskuupäevana konkreetset kuupäeva – ennekõike 1. jaanuari 2026, mis oleks ka 739 SEga tehtavate muudatuste jõustumise kuupäev. Sellest variandist loobuti, kuna kooskõlastamine Justiits- ja Digiministeeriumis kestaks enam-vähem sama ajani, ning vältimaks olukorda, et sisemine kooskõlastamine võtab rohkem aega ja eelnõukohane määrus 1. jaanuaril ei jõustu, otsustati jõustada see üldkorras. Seega jõustuvad eelnõuga tehtavad muudatused kolmandal päeval pärast Riigi Teatajas avaldamist.

Määruse sisu on seotud ainult Riigi Infosüsteemi Ametiga. Siinse eelnõuga seotud põhilisemad mõjud on hinnatud 739SE muudatuste käigus (vt 739 SE seletuskirja punkti 7, täpsemalt p 7.2). Amet täidab sisuliselt enamikke ülesandeid, mis siinse määruse tulemusena lisanduvad. Amet on tegelenud ettevalmistustega, et neid ülesandeid täita, mistõttu puudub vajadus täiendava üleminekuaja sätestamiseks.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

7.1. Enne eelnõu koostamist toimusid kaasamised seoses NIS2-direktiivi ülevõtmisega. Nende käigus sai anda tagasisidet muu hulgas ka siin kommenteeritava eelnõuga sätestatavate nõuete kohta. Sellekohane tagasiside ja nendega seotud vastused on leitavad 739 SE dokumentide juurest. Samuti on seletuskirjas asjakohasel juhul selgitatud märkusi, mis saabusid 739 SE kohta enne selle esitamist Riigikogule.

7.2. Kuna eelnõu puudutab Justiits- ja Digiministeeriumi valitsemisala asutuse (Riigi Infosüsteemi Ameti) põhimääruse muutmist, ei edastata eelnõu ministeeriumitele, Riigikantseleile ja muudele osapooltele avalikuks kooskõlastamiseks eelnõude infosüsteemi kaudu. Enne eelnõukohase määruse kehtestamist arutati eelnõu sisu Riigi Infosüsteemi Ametiga.