01.06.2026

Justiits- ja digiministri määruse „Riikliku küberturvalisuse strateegia koostamise ulatus, tingimused ja elluviimise kord“ 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] Selle seletuskirja aluseks oleva eelnõu eesmärk on võtta üle ainult NIS2-direktiivi artikkel 7 osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega. Konkreetsemalt sätestatakse kavandatava määrusega riikliku küberturvalisuse strateegia koostamise ulatus, tingimused ja elluviimise kord ehk strateegia sisu ja koostamise nõuded.
Kuna ülevõtmisseadus suurendas halduskoormust (küberturvalisuse seaduse kohaldamisala täiendati uute subjektidega, kes peavad seaduse nõudeid täitma), tasakaalustati seda halduskoormuse tõusu Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega. Need muudatused jõustusid 1. oktoobril 2025. Kommenteeritav eelnõu ei näe ette halduskoormuse kasvu, see on seotud ennekõike Justiits- ja Digiministeeriumile antud ülesande sisustamise ja asjaomase 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 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.

Eelnõukohase määrusega võetakse üle Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta 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*), artikkel 7 osas, mida ei reguleerita küberturvalisuse seaduse ega muude õigusaktidega.

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

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[3] ELi direktiivide valdkonna all nimetatud ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Kuna ülevõtmisseadusega suurendati halduskoormust (küberturvalisuse seaduse kohaldamisala täiendati uute subjektidega, kes peavad seaduse nõudeid täitma), tasakaalustati seda halduskoormuse tõusu Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega. Need muudatused jõustusid 1. oktoobril 2025. Kommenteeritav eelnõu ei näe ette halduskoormuse kasvu, eelnõu on seotud ennekõike Justiits- ja Digiministeeriumile antud ülesande sisustamise ja asjaomase töökoormusega.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb viiest paragrahvist.

Paragrahv 1 sätestab määruse reguleerimisala ehk mis on määruse sisu. **Lõikes 1** sätestatakse, et määrus reguleerib NIS2-direktiivi artiklis 7 sätestatud küberturvalisuse strateegia (edaspidi *strateegia*) koostamist. **Lõikega 2** täpsustatakse eelnõukohase määruse sisu, sedastades, et selles sätestatakse strateegia sisu ja (§ 2, mis käsitleb strateegia põhisisu), koostamise kord (eelnõu §-d 4 ja 5, mis käsitlevad vastavalt strateegiast teavitamist ning strateegia hindamist ja uuendamist, kuid kaudselt ka eelnõu § 2) ning asjaomaste poliitikameetmete loetelu (eelnõu § 3, mis käsitleb strateegias kehtestatavaid poliitikameetmeid). Kommenteeritava lõike sõnastus on seotud eelnõukohase määruse volitusnormiga ehk küberturvalisuse seaduse § 5 lõikega 2 (*[r]iikliku küberturvalisuse strateegia ulatuse, tingimused ja elluviimise korra koos asjaomaste poliitikameetmete loeteluga kehtestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega).*
Eelnõukohase määruse ja kommenteeritava paragrahviga seoses vt ka ülevõtmisseaduse eelnõu seletuskirjas küberturvalisuse seaduse § 5 lõigete 1 ja 2 kohta esitatud selgitused, nii seal viidatud NIS2-direktiivi põhjendused 48–57, 60 ja 97 kui ka viited Euroopa Komisjoni suuniste NIS2-direktiivi artikli 4 lõigete 1 ja 2 kohaldamise kohta (2023/C 328/02)[4] asjakohastele punktidele ja osadele.

Paragrahvi 2 lõikega 1 võetakse üle NIS2-direktiivi artikli 7 lõike 1 sissejuhatava osa esimene lause (*[i]ga liikmesriik võtab vastu riikliku küberturvalisuse strateegia, milles määratakse kindlaks strateegilised eesmärgid, nende eesmärkide saavutamiseks vajalikud ressursid ning asjakohased poliitilised ja regulatiivsed meetmed, et saavutada ja säilitada kõrgel tasemel küberturvalisus.*).

[2] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[3] https://valitsus.ee/sites/default/files/documents/2023-05/VVTP%202023-2027_26.pdf
[4] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1751186614700

Paragrahvi 2 lõikega 2 võetakse üle NIS2-direktiivi artikli 7 lõike 1 sissejuhatava osa teine lause (*[r]iiklik küberturvalisuse strateegia peab sisaldama järgmist*) koos sama lõike punktidega a–h.
Lõike 2 punktiga 1 võetakse üle NIS2-direktiivi artikli 7 lõike 1 punkt a (*liikmesriigi küberturvalisuse strateegia eesmärgid ja prioriteedid, mis hõlmavad eelkõige I ja II lisas osutatud sektoreid*). **Lõike 2 punktiga 2** võetakse üle artikli 7 lõike 1 punkt b (*juhtimisraamistik käesoleva lõike punktis a osutatud eesmärkide ja prioriteetide saavutamiseks, sealhulgas lõikes 2 osutatud poliitikameetmed*). **Lõike 2 punktiga 3** võetakse üle artikli 7 lõike 1 punkt c (*juhtimisraamistik, milles selgitatakse asjaomaste sidusrühmade rolli ja kohustusi riiklikul tasandil, mis toetavad [NIS2-direktiivi] kohaste pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide vahelist koostööd ja koordineerimist riiklikul tasandil, samuti nende organite ja valdkondlike liidu õigusaktide kohaste pädevate asutuste vahelist koordineerimist ja koostööd*). Küberturvalisuse seaduse § 5 lõigete 3 ja 4 kohaselt on pädevad asutused Riigi Infosüsteemi Amet ja julgeolekuasutused ning ühtse kontaktpunkti ja CSIRTi rolli täidab Riigi Infosüsteemi Amet. **Lõike 2 punktiga 4** võetakse üle artikli 7 lõike 1 punkt d (*mehhanism asjakohaste varade kindlaks tegemiseks ja kõnealuse liikmesriigi riskide hinnang*). **Lõike 2 punktiga 5** võetakse üle artikli 7 lõike 1 punkt e (*intsidentideks valmisoleku ja neile reageerimise meetmete ning seotud taastemeetmete, sealhulgas avaliku ja erasektori koostöö kirjeldus*). Eelnõus kasutatakse termini „intsident“ asemel terminit „küberintsident“, mis on defineeritud küberturvalisuse seaduse § 2 punktis 19. **Lõike 2 punktiga 6** võetakse üle artikli 7 lõike 1 punkt f (*riikliku küberturvalisuse strateegia rakendamisse kaasatavate asutuste ja sidusrühmade loetelu*). **Lõike 2 punktiga 7** võetakse üle artikli 7 lõike 1 punkt g (*poliitikaraamistik [NIS2-direktiivi] ning direktiivi (EL) 2022/2557 kohaste pädevate asutuste vahelise tegevuse tõhusaks koordineerimiseks küberriskide, -ohtude ja -intsidentide ning asjakohasel juhul muude kui küberriskide, -ohtude ja -intsidentide alase teabe jagamise ning järelevalveülesannete täitmise eesmärgil*). Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2557[5] kohaste pädevate asutuste all on mõeldud elutähtsa teenuse toimepidavust korraldavat asutust või tema poolt hädaolukorra seaduse § 37 lõike 5 alusel määratud asutust, Päästeametit ja Riigikantseleid. Kommenteeritava punktiga on seotud ka küberturvalisuse seaduse § 17[4] lõige 2, mille puhul vt ka ülevõtmisseaduse eelnõu seletuskirjast vastava lõike selgitusi. **Lõike 2 punktiga 8** võetakse üle artikli 7 lõike 1 punkt h (*kava, sealhulgas vajalikud meetmed kodanike küberturvalisuse alase teadlikkuse üldise taseme suurendamiseks*). Kommenteeritavas punktis on sõna „kodanike“ (NIS2-direktiivi ingliskeelses versioonis *citizen*) asemel kasutatud „elanike“, kuna need meetmed ei peaks piirduma ainult kodanikega, vaid ka muude inimestega, kes Eestis elavad.

Paragrahviga 3 võetakse üle NIS2-direktiivi artikli 7 lõike 2 sissejuhatav lauseosa (*[r]iikliku küberturvalisuse strateegia osana võtavad liikmesriigid vastu eelkõige poliitikameetmed*) koos punktidega a–j. Sõna „poliitikameetmed“ vaste NIS2-direktiivi ingliskeelses versioonis on „*policies*“, saksakeelses „*Konzepte*“ ja prantsuskeelses versioonis „*politiques*“.
Lõike 1 punktiga 1 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt a (*mis käsitlevad üksuste teenuste osutamiseks kasutatavate IKT-toodete ja IKT-teenuste tarneahela küberturvalisust*). Termini „üksus“ kohta vt küberturvalisuse seaduse § 2 punkt 39, terminite „IKT-toode“ ja „IKT-teenus“ kohta vt Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881[6] artikli 2 punktid 12 ja 13.

[5] Konsolideeritud tekst: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02022L2557-20221227.
[6] Konsolideeritud tekst: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02019R0881-20250204.

Lõike 1 punktiga 2 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt b (*mis käsitlevad IKT-toodete ja IKT-teenuste küberturvalisusega seotud nõuete ja vastavate spetsifikatsioonide lisamist riigihankemenetlusse, sealhulgas seoses küberturvalisuse sertifitseerimise, krüpteerimisnõuete ning avatud lähtekoodiga küberturvalisuse toodete kasutamisega*). Avatud lähtekoodi kohta vt ka kommenteeritava lõike punkti 5 selgitus.
Lõike 1 punktiga 3 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt c (*nõrkuste haldamiseks, mis hõlmab kohase nõrkuste koordineeritud avalikustamise edendamist ja hõlbustamist artikli 12 lõikele 1 kohaselt*). Eelnõus kasutatakse termini „nõrkus" asemel terminit „turvahaavatavus", mis on defineeritud küberturvalisuse seaduse § 2 punktis 31. Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 60:
(60) Liikmesriigid peaksid võtma koostöös ENISAga[7] meetmeid, et nõrkuste[8] koordineeritud avalikustamist hõlbustada, kehtestades selleks asjakohase riikliku poliitika. Oma riikliku poliitika raames peaksid liikmesriigid kooskõlas oma õigusega püüdma võimalikult suures ulatuses lahendada probleeme, millega puutuvad kokku nõrkuste valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega. Võttes arvesse, et mõnes liikmesriigis võib nõrkuste valdkonnas uuringuid läbi viivate füüsiliste ja juriidiliste isikute suhtes kohaldada kriminaal- ja tsiviilvastutust, soovitatakse liikmesriikidel võtta vastu suunised, mis käsitlevad infoturbeuurijate nende tegevuse eest vastutusele võtmisest loobumist ja tsiviilvastutusest vabastamist.
Lõike 1 punktiga 4 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt d (*mis on seotud avatud interneti avaliku tuuma üldise kättesaadavuse, usaldusväärsuse ja konfidentsiaalsuse säilitamisega, sealhulgas vajaduse korral merealuste sidekaablite küberturvalisusega*). Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 97:
(97) Siseturg sõltub interneti toimimisest rohkem kui kunagi varem. Peaaegu kõigi elutähtsate[9] ja oluliste üksuste teenused sõltuvad interneti kaudu pakutavatest teenustest. Et tagada elutähtsate ja oluliste üksuste pakutavate teenuste sujuv osutamine, on oluline, et kõikidel üldkasutatavate elektroonilise side võrkude pakkujatel[10] oleksid asjakohased küberturvalisuse riskijuhtimismeetmed ja et nendega seotud olulistest intsidentidest[11] teataks. Liikmesriigid peaksid tagama üldkasutatavate elektroonilise side võrkude turvalisuse säilimise ning oma eluliste julgeolekuhuvide kaitse sabotaaži ja spionaaži eest. Kuna rahvusvaheline ühenduvus edendab ja kiirendab liidu ja selle majanduse konkurentsipõhist digitaliseerimist, tuleks merealuseid sidekaableid mõjutavatest intsidentidest teavitada CSIRTi või, kui see on kohaldatav, pädevat asutust. Kui see on asjakohane, tuleks merealuste sidekaablite küberturvalisust riiklikus küberturvalisuse strateegias arvesse võtta ning see peaks hõlmama võimalike küberturvalisuse riskide kaardistamist ja leevendusmeetmeid, et tagada nende kaitse kõrgeimal tasemel.
Lõike 1 punktiga 5 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt e (*mis edendavad selliste asjakohaste kõrgetasemeliste tehnoloogiate väljatöötamist ja integreerimist, mille eesmärk on rakendada tipptasemel küberturvalisuse riskijuhtimismeetmeid*). Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendused 51 ja 52:
(51) Liikmesriigid peaksid ergutama uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamist, mis võiks parandada küberrünnete avastamist ja ennetamist ning ressursse küberrünnete vastu paremini suunata. Seepärast peaksid liikmesriigid sellise tehnoloogia

[7] ENISA on Euroopa Liidu Küberturvalisuse Ameti rahvusvaheline lühend.
[8] Eelnõus kasutatakse termini „nõrkus" asemel terminit „turvahaavatavus", mis on defineeritud küberturvalisuse seaduse § 2 punktis 31.
[9] Küberturvalisuse seaduses on termini „elutähtis üksus" asemel kasutatud terminit „ülioluline üksus".
[10] Küberturvalisuse seaduses on termini „üldkasutatava elektroonilise side võrgu pakkuja" asemel kasutatud terminit „üldkasutatava elektroonilise side võrgu teenuse osutaja".
[11] Küberturvalisuse seaduses nimetatakse neid „olulise mõjuga küberintsidentideks".

kasutamise hõlbustamiseks soodustama oma riiklikes küberturvalisuse strateegiates teadus- ja arendustegevust, eelkõige seoses küberturvalisuse automatiseeritud või poolautomaatsete vahenditega, ning, kui see on kohane, jagama sellise tehnoloogia kasutajate koolitamiseks ja tehnoloogia täiustamiseks vajalikke andmeid. Uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamine peaks olema kooskõlas liidu andmekaitseõigusega, sealhulgas andmekaitsepõhimõtetega, nagu andmete täpsus, võimalikult väheste andmete kogumine, õiglus ja läbipaistvus ning andmeturve, näiteks tipptasemel krüpteerimine. Määruses (EL) 2016/679 sätestatud lõimitud ja vaikimisi andmekaitse nõuetest tuleb täielikult kinni pidada.

(52) Tänu avatud lähtekoodiga küberturbevahenditele ja -rakendustele võib tõusta avatuse tase ja need võivad mõjuda soodsalt tööstusinnovatsiooni tõhususele. Avatud standardid soodustavad turbevahendite koostalitlusvõimet, mis on kasulik tööstusvaldkonna sidusrühmade turvalisuse seisukohast. Avatud lähtekoodiga küberturbevahendid ja -rakendused võivad võimendada laiemat arendajate kogukonda, võimaldades tarnijate mitmekesistamist. Avatud lähtekoodiga võib kaasneda küberturvalisusega seotud vahendite kontrolliprotsessi suurem läbipaistvus ning kogukonna juhitav nõrkuste[12] tuvastamise protsess. Seetõttu peaks liikmesriikidel olema võimalik edendada avatud lähtekoodiga tarkvara ja avatud standardite kasutuselevõttu, järgides poliitikat, mis on seotud avatud andmete ja avatud lähtekoodi kasutamisega läbipaistvusel põhineva turvalisuse osana. Avatud lähtekoodiga küberturbevahendite kasutuselevõttu ja kestlikku kasutamist edendavad tegevuskavad, on eriti olulised väikeste ja keskmise suurusega ettevõtjate jaoks, kellel on märkimisväärsed rakenduskulud, mida saaks vähendada, kui vajadust spetsiifiliste rakenduste või vahendite järele vähendataks.

Lõike 1 punktiga 6 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt f (*mille abil edendatakse ja arendatakse küberturvalisuse alast haridust ja koolitust, küberturvalisuse alaseid oskusi, teadlikkust, teadus- ja arendusalgatusi ning suuniseid heade küberhügieenitavade ja -kontrolli kohta kodanikele, sidusrühmadele ja üksustele*). Eelnõu § 2 lõike 2 punkti 8 selgitustes on selgitatud, miks kasutatakse sõna „kodanike“ asemel sõna „elanike“, see selgitus käib ka kõnesoleva punkti kohta. Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendused 49 ja 50:

(49) Võrgu- ja infosüsteemide taristu, riistvara, tarkvara ja veebipõhiste rakenduste turvalisuse ning selliste ettevõtjate või lõppkasutajate andmete kaitsmiseks, millest üksused sõltuvad, luuakse alus küberhügieeni poliitikameetmetega. Küberhügieeni poliitikameetmed, mis koosnevad ühistest alustavadest, sealhulgas tarkvara ja riistvara uuendamine, salasõnade muutmine, uute paigalduste haldamine, administraatori õigustega juurdepääsukontode piiramine ja andmete varundamine, võimaldavad luua intsidentide[13] või küberohtude puhuks valmisoleku ning üldise turvalisuse ja julgeoleku ennetava raamistiku. Liikmesriikide küberhügieeni poliitikameetmeid peaks jälgima ja analüüsima ENISA[14].

(50) Küberturvalisuse alane teadlikkus ja küberhügieen on liidu küberturvalisuse taseme tõstmiseks üliolulised, eelkõige seetõttu, et ühendatud seadmete arv kasvab pidevalt ja neid võetakse küberrünnete puhul üha enam sihtmärgiks. Tuleks teha pingutusi, et suurendada üldist teadlikkust selliste seadmetega seotud riskidest, samal ajal kui liidu tasandil tehtavad hindamised võiksid aidata tagada ühtse arusaama sellistest riskidest siseturul.

Lõike 1 punktiga 7 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt g (*millega toetatakse akadeemilisi ja teadusasutusi küberturvalisuse vahendite ja turvalise võrgutaristu*

[12] Eelnõus kasutatakse termini „nõrkus“ asemel terminit „turvahaavatavus“, mis on defineeritud küberturvalisuse seaduse § 2 punktis 31.

[13] Eelnõus kasutatakse termini „intsident“ asemel terminit „küberintsident“, mis on defineeritud küberturvalisuse seaduse § 2 punktis 19.

[14] ENISA on Euroopa Liidu Küberturvalisuse Ameti rahvusvaheline lühend.

väljatöötamisel, täiustamisel ja kasutuselevõtmise edendamisel). Eelnõus kasutatud termin „teadusasutus“ on defineeritud küberturvalisuse seaduse § 2 punktis 29.

Lõike 1 punktiga 8 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt h (*sealhulgas asjakohane menetluskord ja sobivad teabevahetuslahendused, millega toetatakse vabatahtlikku küberturvalisuse alase teabe vahetamist üksuste vahel kooskõlas liidu õigusega*). Kommenteeritava punktiga seoses vt ka eelnõu § 3 lõige 2.

Lõike 1 punktiga 9 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt i (*mis tugevdavad väikeste ja keskmise suurusega ettevõtjate, eelkõige nende, kes on [NIS2-direktiivi] kohaldamisalast välja jäetud, kübervastupidavusvõimet ja küberhügieeni lähtetaset, pakkudes nende erivajaduste rahuldamiseks kergesti kättesaadavaid suuniseid ja tuge*). Eelnõus on kasutatud sõna „kübervastupidavusvõime“ (ingl *resilience*) asemel sõna „küberkerksus“, lähtudes Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2847[15] sõnastusest. Samuti on sõna „lähtetase“ asemel kasutatud sõna „baastase“. Sõna „erivajaduste“ asemel on kasutatud sõnastust „spetsiifiliste vajaduste“, kuna viimane on sobilikum, kui arvestada NIS2-direktiivi ingliskeelses versioonis olevat sõnastust „*specific needs*“. Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 56:

(56) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates käsitlema väikeste ja keskmise suurusega ettevõtjate küberturvalisuse vajadusi. Liidus on väikeste ja keskmise suurusega ettevõtjate osakaal tööstus- ja äriturul suur ning neil on sageli raske kohaneda uute äritavadega üha rohkem ühendatud maailmas ja digitaalses keskkonnas, kus töötajad on kodutööl ja äritegevus toimub järjest rohkem interneti kaudu. Mõnedel väikestel ja keskmise suurusega ettevõtjatel on küberturvalisusega seoses sellised probleemid nagu vähene küberteadlikkus, kaugtöösüsteemide IT-turvalisuse puudumine, küberturvalisuse tagamiseks kasutatavate lahenduste suured kulud ja kõrgem ohutase, näiteks lunavaraga seoses, mille lahendamiseks nad peaksid saama suuniseid ja tuge. Väikestest ja keskmise suurusega ettevõtjatest on üha enam saamas tarneahela rünnete sihtmärk, sest nende küberturvalisuse riskijuhtimismeetmed ja ründehaldamine ei ole nii ranged ning asjaolu tõttu, et neil on piiratud turberessursid. Sellised tarneahela ründed ei mõjuta üksnes väikeseid ja keskmise suurusega ettevõtjaid ja nende tegevust, vaid võivad avaldada astmelist mõju ka üksustele, kellele nad tarnivad, põhjustades ulatuslikuma ründe. Liikmesriigid peaksid oma riiklike küberturvalisuse strateegiate kaudu aitama väikestel ja keskmise suurusega ettevõtjatel tarneahelates esinevaid probleeme lahendada. Liikmesriikidel peaks olema väikeste ja keskmise suurusega ettevõtjate jaoks riiklikul või piirkondlikul tasandil kontaktpunkt, mis kas annab väikestele ja keskmise suurusega ettevõtjatele suuniseid ja abi või suunab nad küberturvalisuse küsimustes suuniste ja abi saamiseks asjakohaste asutuste juurde. Liikmesriike julgustatakse osutama ka selliseid teenuseid nagu veebisaidi konfigureerimine ja logimise võimaldamine mikroettevõtjatele ja väikestele ettevõtjatele, kellel see võimekus puudub.

Lõike 1 punktiga 10 võetakse üle NIS2-direktiivi artikli 7 lõike 2 punkt j (*mis edendavad aktiivset küberkaitset*). Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 57:

(57) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates laiema kaitsestrateegia osana võtma kasutusele aktiivse küberkaitse edendamise poliitika. Selle asemel et tegutseda reageerivalt, tähendab aktiivne küberkaitse võrguturbe rikkumise aktiivset ennetamist, avastamist, seiret, analüüsimist ja tagajärgede leevendamist, milleks kasutatakse nii ohvri võrgus kui ka sellest väljaspool olevaid võimalusi. See võiks hõlmata liikmesriike, kes pakuvad teatavatele üksustele tasuta teenuseid või vahendeid, sealhulgas iseteeninduskontrolle, avastamisvahendeid ja kõrvaldamisteenuseid. Võime ohuteavet ja -analüüse, kübertegevuse hoiatusi ja reageerimismeetmeid kiiresti ja automaatselt jagada ning mõista on ülioluline, et teha ühtseid pingutusi võrgu- ja infosüsteemide vastu suunatud rünnete tulemuslikuks

[15] Konsolideeritud tekst: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02024R2847-20241120.

ennetamiseks, avastamiseks ja vastumeetmete võtmiseks. Aktiivne küberkaitse põhineb kaitsestrateegial, millega välistatakse ründemeetmed.

Lõige 2 sätestab, et lisaks eelmainitud poliitikameetmetele võib strateegia sisaldada ka muid poliitikameetmeid. Sellega tagatakse, et strateegia võib sisaldada ka muid teemasid, mis on välja toodud NIS2-direktiivi põhjendustes, mis ei ole strateegia kohustuslik sisu direktiivi artiklis 7. Kommenteeritava lõikega on seotud NIS2-direktiivi põhjendused 53–55:
(53) Kommunaalettevõtted on üha enam ühendatud linnade digivõrkudega, et parandada linnatranspordivõrke, ajakohastada veevarustust ja jäätmekäitlust ning suurendada valgustuse ja hoonete kütmise tõhusust. Need digitaliseeritud kommunaalettevõtted on küberrünnete vastu vähe kaitstud ja edukas küberrünne võib kodanikke nende ettevõtete omavahelise seotuse tõttu ulatuslikult kahjustada. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse selliste ühendatud või arukate linnade arendamist ja nende võimalikku mõju ühiskonnale.
(54) Viimastel aastatel on liit seisnud silmitsi lunavararünnete hüppelise kasvuga, mille puhul pahavara krüpteerib andmeid ja süsteeme ning nõuab vabastamiseks lunaraha maksmist. Lunavararünnete sagenemist ja tõsidust võivad mõjutada mitmed tegurid, nagu erinevad ründemustrid, nagu lunavara kui teenusega seotud kuritegelikud ärimudelid ja krüptoraha, lunaraha nõudmised ja tarneahela rünnete sagenemine. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse lunavararünnete sagenemist.
(55) Sobiva raamistiku kõigi sidusrühmade vahel teadmiste vahetamiseks, parimate tavade jagamiseks ja vastastikuse mõistmise ühise taseme loomiseks võib pakkuda küberturvalisuse valdkonna avaliku ja erasektori partnerlus. Liikmesriigid peaksid edendama poliitikat, millega toetatakse küberturvalisuse valdkonna avaliku ja erasektori partnerluse loomist. Niisuguses poliitikas tuleks muu hulgas täpsustada, millised on avaliku ja erasektori partnerluse ulatus ja kaasatud sidusrühmad, juhtimismudel, olemasolevad rahastamisvõimalused ja osalevate sidusrühmade koostoime. Avaliku ja erasektori partnerluse raames saab võimendavalt kasutada erasektori üksuste eksperditeadmisi, et abistada pädevaid asutusi tänapäevaste teenuste ja protsesside arendamisel, sealhulgas teabevahetus, varajane hoiatamine, küberohtude ja intsidentidega[16] seotud õppused, kriisiohje ning vastupanuvõime kavandamine.

Lisaks eeltoodule osutab kommenteeritav lõige kaudselt ka Euroopa Komisjoni suunistele [NIS2-direktiivi] artikli 4 lõigete 1 ja 2 kohaldamise kohta (2023/C 328/02)[17]. Need suunised on praktikas seotud ennekõike küberturvalisuse seaduse § 1 lõike 4 rakendamisega, kuid neis on selgitatud ka riikliku küberturvalisuse strateegiat. Nende suuniste liites on Euroopa Parlamendi ja nõukogu määruse[18] (EL) 2022/2554 kohta käivate selgituste punktis 2 sätestatud, et *[l]iikmesriigid peaksid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiatesse.*

Paragrahviga 4 võetakse üle NIS2-direktiivi artikli 7 lõige 3 (*[l]iikmesriigid teavitavad komisjoni oma riiklikust küberturvalisuse strateegiast kolme kuu jooksul pärast selle vastuvõtmist. Liikmesriigid võivad jätta sellistest teadetest välja teabe, mis on seotud nende riikliku julgeolekuga*) ning määratletakse strateegia koostamise nõuded.

[16] Eelnõus kasutatakse termini „intsident“ asemel terminit „küberintsident“, mis on defineeritud küberturvalisuse seaduse § 2 punktis 19.
[17] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1751186614700
[18] Konsolideeritud tekst: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02022R2554-20221227.

Lõikega 1 nähakse ette, et strateegia viiakse ellu valdkonna arengukava programmiga riigieelarve seaduse § 19 tähenduses ning lähtuvalt valdkonna arengukava ja programmi koostamise, elluviimise, aruandluse, hindamise ja muutmise korrast, kui eelnõukohane määrus ei sätesta teisiti.
Riigieelarve seaduse § 19 (strateegilised arengudokumendid) lõiked 3 ja 4 määratlevad valdkonna arengukava ja programmi sisud:

- Valdkonna arengukava on arengudokument, milles määratakse terviklikult ühe või mitme poliitikavaldkonna üldeesmärk, alaeesmärgid ja nende mõõtmist võimaldavad mõõdikud ning poliitikainstrumendid, mille kaudu seatud eesmärke plaanitakse saavutada.
- Programm on arengudokument, milles määratakse tulemusvaldkonna alaeesmärgi saavutamisele suunatud meetmed, mõõdikud, tegevused ja rahastamiskava. Mõõdikud peavad olema otseselt seotud programmi eesmärkidega ja olema perioodiliselt mõõdetavad, et hinnata riigieelarve vahendite kasutamise efektiivsust ning tulemuslikkust.

Sama seaduse § 20 (strateegiliste arengudokumentide koostamine, elluviimine ja muutmine) lõiked 2, 4 ja 5 näevad ette:

- Valdkonna arengukava koostatakse vähemalt eelarvestrateegia perioodiks. Valdkonna arengukava kinnitab Vabariigi Valitsus, kui seadusest ei tulene teisiti. Valdkonna arengukava esitatakse enne kinnitamist Riigikogule arutamiseks.
- Programm koostatakse kooskõlas eelarvestrateegia perioodiga. Programmi kinnitab minister. Kui programmi eesmärgi saavutamisse panustavad mitu ministeeriumi, kinnitavad ministrid kogu programmi või jaotatakse programm osadeks, mille ministrid kinnitavad.
- Valdkonna arengukava ja programmi koostamise, elluviimise, aruandluse, hindamise ja muutmise korra kehtestab Vabariigi Valitsus määrusega[19].

Eelviidatud Vabariigi Valitsuse määruse nõuetest lähtutakse nii valdkonna arengukava kui ka selle ellu viimisega seotud programmi(de) koostamisel ja muutmisel. Tolle määruse §-id 2, 4, 7 ja 9 näevad ette järgmist:

- Valdkonna arengukava koostatakse üldjuhul seitsmeks kuni kümneks aastaks.
- Valdkonna arengukava elluviimist hinnatakse vähemalt üks kord hiljemalt kolm aastat enne kestuse lõppu.
- Programm koostatakse ja seda muudetakse eelarvestrateegia ja riigieelarve koostamise raames.
- Programmi aruandlus toimub tulemusaruandluse raames riigieelarveseaduse § 33^1 lõike 5 alusel kehtestatud määruse[20] kohaselt, sh selle määruse 5. peatükk sisustab tulemusaruande sisu kui ka selle koostamise sageduse (seda tehakse sisuliselt kord aastas, st lõppenud eelarveaasta kohta).

Kommenteeritavas lõikes on kasutatud sõnastust „kui käesolev määrus ei sätesta teisiti“, kuna eelnõukohane § 5 määratleb, et strateegia hindamine ja uuendamine peab toimuma vähemalt iga viie aasta tagant (vt ka selle paragrahvi selgitust).

Lõikega 2 võetakse üle NIS2-direktiivi artikli 7 lõike 3 esimene lause ning sellega nähakse ette, et Justiits- ja Digiministeerium teatab Euroopa Komisjonile strateegia vastuvõtmisest kolme kuu jooksul pärast selle vastuvõtmist. See ülesanne antakse ministeeriumile, kuna küberturvalisuse seaduse § 5 lõike 1 teine lause näeb ette, et strateegia koostamist koordineerib

[19] https://www.riigiteataja.ee/akt/123122019005
[20] https://www.riigiteataja.ee/akt/123122023013

riikliku küberturvalisuse valdkonna eest vastutav minister. **Lõikega 3** võetakse üle eelviidatud direktiivi lõike 3 teine lause.

Paragrahviga 5 võetakse üle NIS2-direktiivi artikli 7 lõike 4 esimene lause (*[l]iikmesriigid hindavad oma riiklikke küberturvalisuse strateegiaid peamiste tulemusnäitajate põhjal korrapäraselt ja vähemalt iga viie aasta järel ja vajaduse korral ajakohastavad neid*). Eelnõus on sõna „korrapäraselt" asemel kasutatud „regulaarselt". Siin vt ka eelnõukohase määruse § 4 lõike 1 selgitust.

Määrusele lisatakse normitehniline märkus NIS2-direktiivi kohta.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu vastab NIS2-direktiivile ning kuna direktiiv võeti ennekõike üle ülevõtmisseadusega, on seaduseelnõu materjalide hulgas ka NIS2-direktiivi ja ülevõtmisseaduse vastavustabel. Siinkohal esitatakse need NIS2-direktiivi artikli 7 sätted, mis on seotud kõnesoleva eelnõuga:
1) lõike 1 esimene lause = eelnõu § 2 lõige 1 ja see on seotud ka § 1 lõikega 2;
2) lõike 1 teine lause = eelnõu § 2 lõike 2 sissejuhatav lauseosa;
3) lõike 1 punkt a = eelnõu § 2 lõike 2 punkt 1;
4) lõike 1 punkt b = eelnõu § 2 lõike 2 punkt 2;
5) lõike 1 punkt c = eelnõu § 2 lõike 2 punkt 3;
6) lõike 1 punkt d = eelnõu § 2 lõike 2 punkt 4;
7) lõike 1 punkt e = eelnõu § 2 lõike 2 punkt 5;
8) lõike 1 punkt f = eelnõu § 2 lõike 2 punkt 6;
9) lõike 1 punkt g = eelnõu § 2 lõike 2 punkt 7;
10) lõike 1 punkt h = eelnõu § 2 lõike 2 punkt 8;
11) lõike 2 sissejuhatav lauseosa = eelnõu § 3 lõike 1 sissejuhatav lauseosa ja see on seotud ka lõikega 2;
12) lõike 2 punkt a = eelnõu § 3 lõike 1 punkt 1;
13) lõike 2 punkt b = eelnõu § 3 lõike 1 punkt 2;
14) lõike 2 punkt c = eelnõu § 3 lõike 1 punkt 3;
15) lõike 2 punkt d = eelnõu § 3 lõike 1 punkt 4;
16) lõike 2 punkt e = eelnõu § 3 lõike 1 punkt 5;
17) lõike 2 punkt f = eelnõu § 3 lõike 1 punkt 6;
18) lõike 2 punkt g = eelnõu § 3 lõike 1 punkt 7;
19) lõike 2 punkt h = eelnõu § 3 lõike 1 punkt 8;
20) lõike 2 punkt i = eelnõu § 3 lõike 1 punkt 9;
21) lõike 2 punkt j = eelnõu § 3 lõike 1 punkt 10;
22) lõike 3 esimene lause = eelnõu § 4 lõige 2;
23) lõike 3 teine lause = eelnõu § 4 lõige 3;
24) lõike 4 esimene lause = eelnõu § 5.
Iga muudatuse juures on võrreldud muudetava sätte vastavust Euroopa Liidu õigusele, vajaduse korral on toodud ka võimalikud sõnastusalternatiivid.
Sätete puhul, mis sõnastatakse teisiti kui NIS2-direktiiv, 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 reguleerib riikliku küberturvalisuse strateegia koostamist, mille koordineerimise ülesanne on riikliku küberturvalisuse valdkonna eest vastutaval ministril. See tähendab, et eelnõu mõjutab ennekõike Justiits- ja Digiministeeriumi, kelle teenistujad (konkreetsemalt riikliku küberturvalisuse talituse ametnikud) strateegiat ette valmistavad. Määrusekohase strateegia koostamise ülesanne on põhimõtteliselt sama kui see, mille mõju on tervikuna hinnatud ülevõtmisseaduse seletuskirjas[21] (vt seletuskirja punkt 6.5), mistõttu selle tulemusi siin ei korrata.
Eelnõu mõjutab ennekõike riigiasutuste korraldust. Muudes valdkondades eelnõu olulist mõju ei avalda, mistõttu pole mõju sihtrühmade kaupa käsitletud.

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

Eelnõukohase määrusega seotud tegevusi ja kulusid on üldistatult hinnatud ülevõtmisseaduse eelnõu seletuskirjas[22] (vt seletuskirja punkt 7, täpsemalt p 7.1), mistõttu selle tulemusi siin ei korrata.
Kõnesoleva eelnõuga on seotud NIS2-direktiivi põhjendus 48:
(48) Küberturvalisuse kõrge taseme saavutamiseks ja säilitamiseks peaksid [NIS2-direktiiviga] nõutavad riiklikud küberturvalisuse strateegiad koosnema sidusatest raamistikest, milles on esitatud strateegilised eesmärgid ja prioriteedid küberturvalisuse valdkonnas ning nende saavutamiseks vajalik juhtimine. Need strateegiad võivad koosneda ühest või mitmest seadusandlikust või muust kui seadusandlikust aktist.
Eestis ei koostata strateegiaid eraldi dokumendina, vaid osana laiemast strateegilisest raamistikust ehk konkreetse valdkonna arengukavast.[23] Arvestades eelviidatud NIS2-direktiivi põhjenduse 48 teist lauset, võib kõnesoleva määruse kohane strateegia olla mõne muu dokumendi osa. Praktikas on Vabariigi Valitsuse kinnitatud digiühiskonna arengukavas käsitletud ka küberturvalisuse valdkonda. Seega on kõnesoleva määruse kohane strateegia üks osa digiühiskonna arengukavast ja Vabariigi Valitsuse vastu võetud (vt küberturvalisuse seaduse § 5 lõike 1 esimene lause: *Vabariigi Valitsus võtab vastu Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artiklis 7 nimetatud riikliku küberturvalisuse strateegia, mis võib olla koostatud muu õigusakti kohase dokumendi osana*). Justiits- ja Digiministeerium on ette valmistanud digiühiskonna arengukava, millega seatakse Eesti digiarengu sihid kuni aastani 2035, mis hõlmab ka küberturvalisuse valdkonda. Vabariigi Valitsus saatis 19. veebruaril 2026 Riigikogule arutamiseks digiühiskonna arengukava. Pärast arutelusid Riigikogus esitatakse arengukava kinnitamiseks Vabariigi Valitsusele.[24]
Lisaks eeltoodule tuleb selgitada kõnesoleva määruse kohase strateegia koostamise tausta. Vabariigi Valitsuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu nr 505 SE kohase seadusega läksid digiühiskonna poliitika, avalike e-teenuste, digiarengu ja küberturvalisuse, riigi infosüsteemide, kesksete võrgu- ja infosüsteemide ning side ja telekommunikatsiooniga seotud ülesanded 1. jaanuaril 2025 Majandus- ja Kommunikatsiooniministeeriumilt üle Justiits- ja Digiministeeriumile. Kõnesoleva määruse kohast strateegiat[25] hakati koostama siis, kui küberturvalisuse valdkonna koordineerimise ülesanne oli Majandus- ja Kommunikatsiooniministeeriumil. Uue digiühiskonna arengukava

[21] Vt allviide 1.
[22] Vt allviide 1.
[23] https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/strateegilised-arengudokumendid
[24] Vt https://valitsus.ee/uudised/valitsus-saadab-riigikogule-digiuhiskonna-uue-arengukava ja eelnõude infosüsteemi toimik 25-1360. https://eelnoud.valitsus.ee/main/mount/docList/9d05decd-60e7-4680-bc7c-3e3ad5d52566
[25] Küberturvalisuse strateegia 2024-2030. https://www.justdigi.ee/digi-side-ja-kuber/riigi-kuberturvalisuse-tagamine

vastuvõtmisel peab Justiits- ja Digiministeerium koostatud küberturvalisuse strateegia 2024–2030 üle vaatama ning seda vajaduse korral uuendama.

6. Määruse jõustumine

Algselt oli kavas lisada jõustumiskuupäevaks konkreetne kuupäev, mis jätaks piisavalt aega eelnõu avalikuks kooskõlastamiseks ning määruse kehtestamiseks ja avaldamiseks Riigi Teatajas. Määruse koostamise käigus otsustati seda lähenemist muuta, kuna määruse sisu arvestades on võimalik määrust jõustada ka üldises korras. Lisaks ei tähenda üldises korras jõustumine seda, et määruse kehtima hakkamise kuupäevaks tuleb küberturvalisuse strateegia 2024–2030 üle vaadata.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Enne eelnõu koostamist toimusid kaasamised seoses NIS2-direktiivi ülevõtmisega. Nende käigus sai anda tagasisidet muu hulgas ka kommenteeritava määruse eelnõuga kavandatavate nõuete kohta. Asjaomase tagasiside leiab ülevõtmisseaduse eelnõu dokumentide juurest.

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

Eelnõu saadetakse arvamuse avaldamiseks Eesti Pangale, Eesti Interneti Sihtasutusele, Finantsinspektsioonile ja Riigi Infosüsteemi Ametile.