25.02.2026

Justiits- ja digiministri määruse „Küberintsidendist teavitamisel esitatavad andmed ja teavitamise 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 739 SE (edaspidi *739 SE*)).[1] Selle seletuskirja aluseks oleva eelnõu eesmärk on võtta üle ainult NIS2-direktiivi artikli 23 lõige 4 osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega. Konkreetsemalt sätestatakse kavandatava määrusega, mis on küberintsidendist teavitamisel esitatavate teadete sisu (st teave). Nendeks teadeteks on esmane teade, intsidenditeade, vahearuanne ja lõppraport.
Kuna nii 739 SE kui ka kavandatava määruse eelnõu kohaselt – viimase puhul väga vähesel määral – halduskoormus kasvab (küberturvalisuse seadust täiendatakse uute subjektidega, kes peavad täitma seaduses, sh ka määruses ette nähtavaid nõudeid), nähti halduskoormuse tasakaalustamine ette Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega.[2] Nimetatud määruse kohaselt lihtsustati eelkõige mikro- ja väikeettevõtjate küberturvalisuse tagamise nõudeid, nähes ettevõtjatele ette vaid esmaste turvameetmete täitmise kohustuse standardi järgimise asemel. Need muudatused jõustusid 1. oktoobril 2025.

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.

Eelnõu kohaselt 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*), artikkel 23 lõige 4 osas, mida ei reguleerita küberturvalisuse seaduse ega muude õigusaktidega.

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

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“.[3] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027[4] ELi direktiivide valdkonna all olev ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Kuna nii 739 SE kui ka kavandatava määruse eelnõu kohaselt – viimase puhul väga vähesel määral – halduskoormus kasvab (küberturvalisuse seadust täiendatakse uute subjektidega, kes peavad täitma seaduses, sh ka määruses ette nähtavaid nõudeid), nähti halduskoormuse tasakaalustamine ette Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatustega.[5] Nimetatud määruse kohaselt lihtsustati eelkõige mikro- ja väikeettevõtjate küberturvalisuse tagamise nõudeid, nähes ettevõtjatele standardi järgimise asemel ette vaid esmaste turvameetmete täitmise kohustuse. Need muudatused jõustusid 1. oktoobril 2025.

Küberturvalisuse seaduse § 8 lõige 8^1 näeb ette järgmist: „Kui Euroopa Komisjoni võtab vastu Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 23 lõikes 11 nimetatud rakendusakti, milles täpsustatakse küberintsidendi, sealhulgas olulise mõjuga küberintsidendi kohta esitatava teate või raporti vorm ja selle esitamise kord, lähtutakse nimetatud rakendusaktis sätestatud nõuetest.“ Euroopa Komisjon on viidatud artikli lõike (teise lõike) alusel vastu võtnud rakendusmääruse[6] (EL) 2024/2690, kuid see rakendusakt sisaldab volitusnormi aluseks oleva artikliga seoses ainult neid juhtusid, mille korral tuleks intsidenti pidada oluliseks NIS2-direktiivi artikli 23 lõike 3 tähenduses. Rakendusmäärus (EL) 2024/2690 ei sätesta vastavat vormi ega täpsusta küberintsidendi, sh olulise mõjuga küberintsidendi kohta teate või raporti esitamise korda (vt selle lõike esimest lõiget). Seega ei ole veel olemas rakendusakti, mis näeb ette teate või raporti vormi ja selle esitamise korra. Kui selline rakendusakt tulevikus vastu võetakse, lähtuvad rakendusaktis nimetatud teenuseosutajad selles rakendusaktis kehtestatud nõuetest. Ülejäänud küberturvalisuse seaduse kohased teenuseosutajad järgivad siinse eelnõuga kavandatavat määrust. Euroopa Komisjon on digitaalse koondmääruse ettepanekus[7] selgitanud, et eelviidatud komisjoni rakendusakt (artikli 23 lõike 11 esimene lõige) võetakse vastu, sealhulgas ühtlustatakse selle ettepaneku käigus ka eri õigusaktide alusel ette nähtud teavituste vorme. See siiski ei tähenda, et rakendusmäärust (EL) 2024/2690 ja selles olevaid nõudeid ei pea juba praegu järgima need üksused, kes on selles nimetatud.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb kahest paragrahvist.

Paragrahviga 1 määratakse teavitamise sisu ja kord. Tegemist on NIS2-direktiivi artikli 23 lõike 4 ülevõtmisega. Küberturvalisuse seaduse § 8 määrab nii nende teavituste esitamise

[3] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027
[4] https://valitsus.ee/sites/default/files/documents/2023-05/VVTP%202023-2027_26.pdf
[5] https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6
[6] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1769430711987
[7] https://digital-strategy.ec.europa.eu/et/library/digital-omnibus-regulation-proposal

ajavälbad kui ka muud üldisemad nõuded, kuid kõnealuses paragrahvis sätestatakse, mis andmeid esmases teates, intsidenditeates, vahearuandes ja lõppraportis esitatakse.

Lõige 1 näeb ette, et esmases teates esitatakse järgmine teave, kui see on teate esitamise hetkel teada:
1) teave olulise mõjuga küberintsidendi sisu ja põhjuse kohta, sealhulgas asjakohasel juhul teave turvarikkemärgi kohta koos selgitusega, kas olulise mõjuga küberintsidendi eeldatavaks põhjuseks on ebaseaduslik või pahatahtlik tegevus;
2) hinnang olulise mõjuga küberintsidendile, sealhulgas selle raskusastmele ja mõjule;
3) teave olulise mõjuga küberintsidendi piiriülese mõju kohta;
4) teave olulise mõjuga küberintsidendi lahendamiseks ettevõetavate tegevuste kohta;
5) selle kontaktisiku andmed, kellega toimub edasine suhtlus seoses küberintsidendi lahendamisega.
Esmase teate (NIS2-direktiivis sõnastuses „varajane hoiatus“) sisuga seoses on asjakohased NIS2-direktiivi põhjenduse 102 laused 5 ja 6: *Varajane hoiatus peaks sisaldama üksnes teavet, mis on vajalik CSIRTi või, kui see on kohaldatav, pädeva asutuse olulisest intsidendist teavitamiseks ja võimaldama asjaomasel üksusel vajaduse korral abi otsida. Selline varajane hoiatus, kui see on kohaldatav, peaks näitama, kas on kahtlus, et olulise intsidendi põhjuseks on ebaseaduslik või pahatahtlik tegevus, ning kas sellel on tõenäoliselt piiriülene mõju.*
Termin „küberintsident“ on defineeritud küberturvalisuse seaduse § 2 punktis 19. Olulise mõjuga küberintsidendi kohta saab lugeda küberturvalisuse seaduse § 8 lõigetest 1 ja 2, sh ka § 8 lõikesse 2 lisanduvast punktist 6, mis omakorda viitab Euroopa Komisjoni asjakohasele rakendusaktile[8] ja selles kirjeldatud olukordadele, millal küberintsident on käsitletav olulise mõjuga küberintsidendina küberturvalisuse seaduse tähenduses. Turvarikkemärk on rikkumisele viitav asjaolu (igasugune tunnus, mis viitab rikkumise toimumisele).
739 SE koostamise käigus hinnati korduvalt, mis on NIS2-direktiivi artikli 23 lõike 4 punkti a minimaalne ülevõetav osa (st mis on esmase teate sisu) ning kuivõrd on direktiiviga ette nähtud sõnastusliku miinimumiga võimalik täita pädevale asutusele, ennekõike Riigi Infosüsteemi Ametile seatud ülesannet ja ootust, et asutus saaks anda teavituse esitajale abi ja tagasisidet selle teabe põhjal, mis on esitatud esmase teatega. Sõnastusliku miinimumiga on siin mõeldud, et olulise mõjuga küberintsidendi korral tuleb teada anda, kas 1) selle eeldatavaks põhjuseks on ebaseaduslik või pahatahtlik tegevus ning kas 2) sellel on Eesti riigipiiri ületav mõju. Lõpptulemusena jõuti järeldusele, et on otstarbekas sõnastada esmase teate sisu nii, nagu on kõnealuses paragrahvis. Esmase teatega esitatakse see teave, mis on teate esitamise hetkel teada või olemas, sest praktikas võib esineda ka olukord, et mingi asjaolu ei ole veel teada (nt intsidendi piiriülene mõju või hinnang olulise mõjuga küberintsidendi tõsiduse ja mõju kohta vms). Seetõttu on kommenteeritavas lõikes kasutatud sõnastust „kui see on teate esitamise hetkel teada“. See tekitab tasakaalu nii küberintsidendist teavitamise kohustuse kui ka küberintsidendi käsitlemise vaatest. See on ka põhjus, miks kommenteeritava lõike sisu hõlmab elemente, mis on NIS2-direktiivi artikli 23 lõikes 4 ette nähtud nii varajasele hoiatusele (eelnõu tähenduses „esmane teade“), intsidenditeatele (eelnõus samuti „intsidenditeade“), vahearuandele (eelnõus samuti „vahearuanne“) kui ka lõpparuandele (eelnõus „lõppraport“). See võimaldab ka vältida, et tekib kuni neli erinevat vormi, mida tuleb ühe küberintsidendi puhul täita – selle asemel on võimalik kasutusele võtta üks vorm, mida saab vajaduse korral täiendada või parandada.

[8] Rakendusakt jõustus 7. novembril 2024 ja on kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1730728447038. Lisainfo: 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.

Lõike 1 punkt 1 on seotud NIS2-direktiivi artikli 23 lõike 4 punkti a (lauseosa *märgitakse (kui see on kohaldatav), kas olulise intsidendi põhjuseks on eeldatavasti ebaseaduslik või pahatahtlik tegevus*), punkti b (lauseosa *antakse esialgne hinnang olulisele intsidendile, sealhulgas .. võimaluse korral ka rikkeindikaatoritele*) ning punkti d alapunktide i (*intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus*) ja ii (*ohu liik või lähtepõhjus, mis intsidendi tõenäoliselt põhjustas*) ülevõtmisega. Sõnad „oluline intsident" on määruse eelnõu tähenduses „olulise mõjuga küberintsident". Sõna „intsident" on eelnõu tähenduses „küberintsident". Sõna „rikkeindikaator" on eelnõu tähenduses „turvarikkemärk". Turvarikkemärk on rikkumisele viitav asjaolu ehk igasugune tunnus, mis viitab rikkumise toimumisele. Sõna „turvarikkemärk" kasutatakse ka küberturvalisuse seaduses, mistõttu ei ole võimalik selle sisu eelnõukohases määruses terminina defineerida ning kui seda teha, siis kasutaks kõrgemaastme õigusakt (seadus) alama astme õigusakti (määruse) definitsiooni, mis ei ole õigusloomes kohane.

Lõike 1 punkt 2 on seotud NIS2-direktiivi artikli 23 lõike 4 punkti b (lauseosa *antakse esialgne hinnang olulisele intsidendile, sealhulgas selle tõsidusele ja mõjule*) ülevõtmisega. Sõna „tõsidus" asemel on eelnõus kasutatud sõna „raskusaste". Raskusaste on seotud võrgu- ja infosüsteemi turvalisust ja selle toimepidevust mõjutavate ning küberintsidendi tekkimist põhjustavate riskide loetelu koostamisega, mille käigus määratakse riskide realiseerumise tagajärgede raskusaste ja kirjeldatakse riskijuhtimismeetmeid. Riskianalüüsi koostamise kohustus on ette nähtud Vabariigi Valitsuse 9. detsembri 2022. a määruse[9] nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" § 5 lõikega 1, selle sisu täpsustatakse Vabariigi Valitsuse määrusi muutva eelnõuga. Varem oli vastav nõue ette nähtud enne NIS2-direktiivi vastuvõtmist kehtinud küberturvalisuse seaduses, konkreetsemalt selle § 7 lõike 2 punkti 1 kuni 31.12.2025 kehtinud sõnastuses. Seega pole riskianalüüsi koostamine, sh selle „raskusaste", uus tegevus ega käsitlus. Sarnaselt sõnaga „turvarikkemärk" ei ole ka eelnõukohases määruses võimalik terminina defineerida sõna „raskusaste" (vt eelmise punkti selgitust).

Lõike 1 punkt 3 on seotud nii NIS2-direktiivi artikli 23 lõike 4 punkti a (lauseosa *milles märgitakse (kui see on kohaldatav), kas [olulisel intsidendil] .. võib olla piiriülene mõju*) kui ka punkti d alapunkti iv (*kui see on kohaldatav, intsidendi piiriülene mõju*) ülevõtmisega. Iga piiriülene intsident ei ole automaatselt piiriülese mõjuga. Piiriülese mõju all mõeldakse, et küberintsidendi mõju avaldub lisaks Eesti Vabariigi territooriumil oleva(te)le võrgu- ja infosüsteemi(de)le ka mõne muu riigi võrgu- ja infosüsteemi(de)le. Muu riigi all mõeldakse nii mõnda teist Euroopa Liidu liikmesriiki kui ka mõnda kolmandat riiki. Seda põhjusel, et näiteks ulatusliku küberintsidendi[10] korral eeldatakse, et taoline intsident on seotud rohkem kui ühe Euroopa Liidu liikmesriigiga.

Lõike 1 punkt 4 on seotud NIS2-direktiivi artikli 23 lõike 4 punkti d alapunkti iii (*juba kohaldatud ja kohaldamisel olevad leevendusmeetmed*) ülevõtmisega. Leevendusmeetmete all mõeldaksegi ettevõetavaid tegevusi ehk neid meetmeid, mis on kasutusele võetud, sh asjakohasel juhul ka tulevikus (näiteks kui üksus teeb rakendatud meetme üle mingi aja pärast ise sisemist kontrolli).

[9] https://www.riigiteataja.ee/akt/127092025002

[10] Küberturvalisuse seaduse (RT I, 30.12.2025, 15) § 2 punkt 34: ulatuslik küberintsident – küberintsident, mille põhjustatud häired on niivõrd laialdased, et üks Euroopa Liidu liikmesriik ei suuda nendega toime tulla, või millel on märkimisväärne mõju vähemalt kahele Euroopa Liidu liikmesriigile.

Lõike 1 punkt 5 on ajendatud Riigi Infosüsteemi Ameti tagasisidest eelnõule. Ameti ettepaneku sisu oli järgmine: „Teeme ettepaneku: .. 2) eelnõu § 1 lg 1 täiendada punktiga: „5) kontaktisik, kellega toimub edasine suhtlus seoses intsidendiga.“ Ettepaneku eesmärk on tagada suhtluse operatiivsus. Teavitusi ei tehta alati isiku poolt, kes peaks olema edasine kontaktisik. Vastava teabe esitamise kohustus tagaks kiirema kontakti intsidendiga tegeleva isikuga.“ Praktikas võib teate esitajaks olla kommenteeritavas punktis mõeldud kontaktisik, kuid kui see nii ei ole, siis esitatakse ka siinne teave. Kontaktisiku andmete all on mõeldud ennekõike füüsilise isiku ees- ja perekonnanime, telefoninumbrit ning e-posti aadressi. Need andmed kantakse küberturvalisuse seaduse § 13 lõike 1 alusel asutatud küberintsidentide registrisse. Eraldi eelnõuga täiendatakse registri põhimääruse[11] § 5 lõiget 2, et viidatud lõige sisaldaks ka kontaktisiku andmeid.

Lõige 2 on seotud samade NIS2-direktiivi sätete ülevõtmisega, mis on viidatud siinse paragrahvi lõike 1 asjakohastes punktides, sh on seotud NIS2-direktiivi artikli 23 lõike 4 punkti b (lauseosa *millega, kui see on kohaldatav, ajakohastatakse punktis a osutatud teavet ning antakse esialgne hinnang olulisele intsidendile, sealhulgas selle tõsidusele ja mõjule ning võimaluse korral ka rikkeindikaatoritele*) ülevõtmisega. Kommenteeritav lõige näeb ette, et kui tegemist on intsidenditeatega, siis esitatakse lõikes 1 nimetatud teave. Kui esmase teate puhul esitatakse see teave, mis on esitamise hetkel olemas, siis intsidenditeate puhul esitatakse kogu teave, mis on lõikes 1 välja toodud. Intsidenditeate esitamisega uuendatakse ka esmases teates esitatud andmeid ehk intsidenditeate esitamise mõte ei ole esitada uuesti neid andmeid, mis olid esmase teate esitamise hetkel olemas. Eesmärk on anda intsidenditeate esitamise hetkel olev ülevaade konkreetsest küberintsidendist ja selle lahendamisest. Kui intsidenditeate puhul ei ole jätkuvalt mõne asjaolu kohta teavet, mis tuleb esitada (näiteks ei ole veel teada, et tegemist on piiriülese mõjuga), saab vastavas osas selgitada, et see info puudub või pole sel hetkel asjakohane (vt ka eelnõu § 1 lõiget 5).

Lõige 3 on seotud samade NIS2-direktiivi sätete ülevõtmisega, mis on viidatud siinse paragrahvi lõike 1 asjakohastes punktides, sh nii NIS2-direktiivi artikli 23 lõike 4 punkti c (*CSIRTi või, kui see on kohaldatav, pädeva asutuse taotlusel vahearuande vaatlusaluste asjade seisu kohta*) kui ka kaudselt punkti d ülevõtmisega. Nende punktide põhisisu võeti üle 739 SE kohase seadusega, kuid seaduseelnõuga küberturvalisuse seaduses tehtavad muudatused ei määra kindlaks, mis on lõpparuande (eelnõus lõppraporti) või vahearuande sisu. Kavandatavas lõikes määratakse vahearuande sisu kindlaks: tegemist on olemuselt sama teabega, mis on nimetatud sama paragrahvi lõikes 1. Selle käigus uuendatakse ka intsidenditeatega esitatud andmeid ehk vahearuande mõte ei ole esitada uuesti neid andmeid, mis olid intsidenditeate esitamise hetkel olemas. Eesmärk on anda vahearuande esitamise hetkel olev ülevaade konkreetsest küberintsidendist ja selle lahendamisest.
Vahearuandega tuleb esitada ka see teave, mida Riigi Infosüsteemi Amet küsib vahearuande esitajalt – seda siis, kui amet soovib mingi asjaolu kohta lisateavet saada. Lisateabe küsimine toimub ennekõike esmases teates või intsidenditeates esitatud teabe põhjal. Ametil pole kohustust lisateavet küsida, kuid kui ta seda teeb, peab teavituse tegija küsitud teabe esitama.
Eelnõuga ei saa täpsustada, mitu vahearuannet tuleb esitada, kuna see sõltub konkreetset intsidendi asjaoludest ja selle lahendamisest. Teatav erisus on siis, kui lõppraportit käsitatakse vahearuandena (vt küberturvalisuse seaduse § 8 lõike 7 teist lauset), mille puhul on mitme sätte koosmõju tõttu ette näha, et tuleb esitada vähemalt üks vahearuanne. Ametile kohalduvad ka haldusmenetluse seaduses ette nähtud nõuded ja põhimõtted (vt nt § 3–6), millest lähtudes peab amet hindama, kas ja kui tihti ta vahearuannet või selles olevaid lisaandmeid küsib.

[11] https://www.riigiteataja.ee/akt/124082023003

Lõige 4 on seotud NIS2-direktiivi artikli 23 lõike 4 punkti d ülevõtmisega. Selles punktis on määratud kindlaks lõpparuande (eelnõus lõppraporti) sisu. Lõppraporti tegemise vajadus on seotud ennekõike konkreetse teenuseosutaja ülesandega analüüsida ja vajaduse korral rakendada süsteemiseid muudatusi küberintsidendi kordumise vältimiseks. Vastav nõue on ette nähtud teiste õigusaktidega – vt Vabariigi Valitsuse 09.12.2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 6 punkti 1 ning ka sama määruse § 5^1 ja seotud lisa punkti 1.3. Sarnane nõue on ette nähtud ka Eesti infoturbestandardis, – vt ettevõtlus- ja infotehnoloogiaministri 16.12.2022. a määruse[12] nr 101 „Eesti infoturbestandard“ lisa 1 punkti 10.1 ja selle alapunkte.
Lõike 4 punkt 1 on seotud NIS2-direktiivi artikli 23 lõike 4 punkti d alapunkti ii (*ohu liik või lähtepõhjus, mis intsidendi tõenäoliselt põhjustas*) ülevõtmisega. **Lõike 4 punkt 2** on seotud NIS2-direktiivi artikli 23 lõike 4 punkti d alapunkti iii (*juba kohaldatud ja kohaldamisel olevad leevendusmeetmed*) ülevõtmisega. **Lõike 4 punkt 3** on seotud NIS2-direktiivi artikli 23 lõike 4 punkti d alapunktide i (*intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus*) ja iv *(kui see on kohaldatav, intsidendi piiriülene mõju*) ülevõtmisega.

Lõige 5 näeb ette, et kui mingeid andmeid ei ole võimalik esmase teatega, intsidenditeatega või vahearuandega esitada, lisatakse sellekohane selgitus samasse teatesse või aruandesse.
Eelnõu sai avalikult kooskõlastuselt tagasisidet, et eelnõu ei sisalda kohustust puuduvat infot põhjendada. Kaitseministeeriumi tagasisides on märgitud järgnev*:* „Eelnõu § 1 lõige 1 sätestab küberintsidentidest teavitamisel esmases teates esitatava teabe. Sätte kohaselt tuleb esmases teates esitada teave võimaluse korral, kuid ei täpsusta .., kas ja kuidas tuleb põhjendada info puudumist. Seletuskiri selgitab „võimaluse korral“ kasutamist, aga ei sätesta normis endas kohustust puudumist põhjendada. Info esitamata jätmine peab olema põhjendatud ja ajutine ning need alused peavad tulema selgelt õigusaktist. Määruses sätestamata jätmine võib anda kohustatud isikutele väga laia tõlgendusruumi.“ Samuti oli Eesti Perearstide Seltsi tagasisides märgitud järgnevat: „Hindame ning palume rõhutada paindlikkust esmase teate esitamisel, kuna selles etapis peaks prioriteet olema teabe esitamise operatiivsus, mitte detailsus ja analüüs. Seda peaksid arvestama ka vormid ning teabe menetlejad, võttes muuhulgas arvesse NIS2-st tulenevaid varajase hoiatuse eesmärke. Vormil või juhises võiks olla olemas ka indikatsioon, et varases etapis on aktsepteeritav vastata “hindamisel / info puudub”. Varases etapis detailse teabe esitamise nõue vähendaks esmaste teavituste operatiivsust ning ei pruugiks olla otstarbekas ressursikasutus ajal, mil fookus on intsidendi lahendamisel ja/või teenuse taastamisel. Palume eelnõu § 1 lg 1 osas seletuskirjas selgemalt välja tuua, et esmase teavituse etapis ei eeldata informatsiooni detailsust ega juurpõhjuse tasemel analüüsi, vaid piisab teadaoleva esmase info edastamisest.“
Eeltoodu tõttu nähakse ette kommenteeritav lõige. See tekitab oodatud paindlikkust (ehk kui mingit teavet pole, siis ei saa seda kohustuslikus korras esitada) ja ka täpsustab teate esitamisel ette nähtud andmete puudumise põhjendamist (näiteks selgitatakse esmases teates, et küberintsidendi tuumik ehk põhjus on alles välja selgitamisel, mistõttu selle aspekti kohta ei ole võimalik tõsikindlat infot veel anda).
Kommenteeritavas lõikes ei ole märgitud lõppraportit, kuna lõppraporti koostamise hetkeks peaks olema küberintsidendist selgem arusaam ja ülevaade ehk mis juhtus, miks juhtus ja mida võeti ette, et see tulevikus uuesti ei juhtuks.

Paragrahvis 2 nähakse ette määruse jõustumise aeg, milleks on 1. aprill 2026 (vt seletuskirja punkti 6).

[12] https://www.riigiteataja.ee/akt/128082025012

Määrusele lisatakse normitehniline märkus NIS2-direktiivi kohta.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõus järgitakse õigusnormide loomisel NIS2-direktiivi. Eelnõu vastab NIS2-direktiivile ning kuna direktiiv võeti ennekõike üle 739 SE kohase seadusega, on seaduseelnõu materjalide juures ka NIS2-direktiivi vastavustabel. Seletuskirja siinses osas tuuakse välja need väljavõtted NIS2-direktiivi artikli 23 lõike 4 esimesest lõigust, mis on seotud siinse eelnõuga:
1) punkt a = määruse § 1 lg 1 p-d 1 ja 3 ning kaudselt ka lg 5;
2) punkt b = määruse § 1 lg 1 p-d 1–3 ning kaudselt ka lg 2 ja 5;
3) punkt c = määruse § 1 lg 3 ning kaudselt ka lg 1;
4) punkti d alapunkt i = määruse § 1 lg 1 p 1 ja lg 4 p 3;
5) punkti d alapunkt ii = määruse § 1 lg 1 p 1 ja lg 4 p 1;
6) punkti d alapunkt iii = määruse § 1 lg 1 p 4 ja lg 4 p 2;
7) punkti d alapunkt iv = määruse § 1 lg 1 p 3 ja lg 4 p 3;
8) punkt e = määruse § 1 lg 3 ning kaudselt ka lg 1 ja 2.
Iga tehtava muudatuse juures on võrreldud muudetava sätte vastavust Euroopa Liidu õigusele, vajaduse korral on toodud ka võimalikud sõnastusalternatiivid.
Sätete puhul, mis lahendatakse teisiti, kui on sõnastatud 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 mõjutab neid üksusi, kes esitavad olulise mõjuga küberintsidendi kohta teateid Riigi Infosüsteemi Ametile. Need üksused on nii avaliku kui ka erasektori taustaga. 739 SE seletuskirjas on hinnatud, kui palju üksusi see muudatus mõjutab. Muudatuse mõju on seotud asjaoluga, mis teavet edaspidi küberintsidendist teavitamise korral esitatakse.
Määrusega tehtaval muudatusel ei ole neile üksustele olulist mõju, kuna olemasolevad küberintsidendist teavitamise vormid on juba praegu üldjoontes samad ehk olulise mõjuga küberintsidendist teavitav üksus ei pea esmase teate, intsidenditeate, vahearuande ega lõppraporti edastamiseks uut laadi teavet koguma hakkama. Seda enam, et esmase teate puhul on olemas ka paindlikkus valida, mis laadi andmeid esitada. Määruse muudatusel on lühiajaliselt suurem mõju neile üksustele, kes pole varem küberintsidendi teavitust teinud (kas kohustuslikult või vabatahtlikult). Tegemist on lühiajalise mõjuga, kuna küberintsidendi toimumise korral ei pruugi üksus kohe alguses saada teada ega aru, mis teavet küberintsidendi kohta tuleb esitada, kuid siin aitabki vastava vormi kasutamine, mis on leitav asjakohaselt veebilehelt (vt ka järgmist selgitust).

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

Eelnõuga tulusid ei prognoosita.

Eelnõu määrusena jõustumise korral peab Riigi Infosüsteemi Amet üle vaatama nii enda võrgulehel kui ka ettenähtud veebikeskkonnas olevad vormid, et need vastaksid määrusega kindlaks määratud teadete sisule. Kuna julgeolekuasutused ei esita kõnealuseid teateid Riigi

Infosüsteemi Ametile (vt küberturvalisuse seaduse § 8 lõike 1 sissejuhatavat lauset ja lõiget 10), tuleb ka julgeolekuasutustel üle vaadata enda asjakohased vormid, sh on neil võimalik taaskasutada neid vorme, mille on loonud Riigi Infosüsteemi Amet (tehes vajalikud enda spetsiifikaga seotud täpsustused). Selle käigus tuleb ka üle vaadata, kas olemasolevad kättesaadavad juhised või kasutusjuhendid (nt veebikeskkonna kasutusjuhend) on lihtsad, selged ja piisavalt arusaadavad. Nii Riigi Infosüsteemi Ameti kui ka julgeolekuasutuste tehtavad toimingud (vormide ja juhiste ülevaatamine) ei tekita märkimisväärset kulu.

6. Määruse jõustumine

Määrus jõustub 1. aprillil 2026. Jõustumisaja puhul on lähtutud kuupäevast, mis võimaldab eelnõul kooskõlastusringi läbida ning Riigi Infosüsteemi Ametil ja julgeolekuasutustel asjakohased vormid üle vaadata.

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 määruse eelnõuga sätestatavate nõuete kohta. Sellekohane tagasiside ja 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. Eelnõu esitatakse eelnõude infosüsteemi kaudu kooskõlastamiseks ministeeriumitele, Riigikantseleile ning Eesti Linnade ja Valdade Liidule.

7.3. Eelnõu saadetakse arvamuse avaldamiseks Andmekaitse Inspektsioonile, Eesti Pangale, Riigi Infosüsteemi Ametile, 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.

7.4. Riigikantselei, Haridus- ja Teadusministeerium, Kultuuriministeerium, Rahandusministeerium ja Sotsiaalministeerium kooskõlastasid eelnõu märkusteta. Kaitseministeerium ning Eesti Linnade ja Valdade Liit kooskõlastasid eelnõu märkustega. Andmekaitse Inspektsioonil ja Eesti Arstide Liidul lisaettepanekuid polnud. Arvamusi esitasid Kaitsevägi (AK-teave), Riigi Infosüsteemi Amet, Eesti Haiglate Liit, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Kaubandus-Tööstuskoda, Eesti Perearstide Selts, Eesti Põllumajandus-Kaubanduskoda ning Eesti Vee-ettevõtete Liit. Eelnõule esitatud tagasiside on leitav seletuskirja lisast.