SELETUSKIRI
Vabariigi Valitsuse otsuse juurde
“Eesti seisukohad Euroopa Liidu küberturvalisuse õigusaktide eelnõude paketi kohta”

20.01.2026 esitas Euroopa Komisjon küberturvalisuse määruse teise ettepaneku (CSA2), mis käsitleb Euroopa Liidu Küberturvalisuse Ametit, Euroopa küberturvalisuse sertifitseerimise raamistikku ning info- ja kommunikatsioonitehnoloogia tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 ehk küberturvalisuse määrus.

Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 (NIS2) muutva direktiivi ettepanek käsitleb NIS2 sihipäraseid muudatusi, et lihtsustada küberturvalisuse raamistiku konkreetseid aspekte, suurendada õiguskindlust ja ühtlustada rakendamist.

Eesti peamised seisukohad CSA2 eelnõu ja NIS2 muudatuste kohta sisaldavad järgmist:

- Eesti toetab Euroopa Liidu küberturvalisuse tugevdamist, kuid peab oluliseks, et NIS2 muutva ja CSA2 eelnõude nõuded, terminoloogia ja kohaldumisala tagavad liikmesriikidele ja puudutatud subjektidele selge ja üheselt mõistetava õigusraamistiku, kuna juba kehtiva NIS2 sõnastused on ebaselged ja mitmeti tõlgendatavad.

- Eesti peab oluliseks, et Euroopa Liidu Küberturvalisuse Ameti (ENISA) rolli ja ülesannete kujundamisel on tagatud selge tööjaotus liikmesriikidega ning välditakse liikmesriikide pädevuste ja olemasolevate mehhanismide dubleerimist (sealhulgas varajase hoiatuse süsteemide, küberintsidentide käsitlemise üksuste ja riiklike operatiivsete funktsioonide osas) ega piirata liikmesriikide pädevate asutuste operatiivtööd. ENISA uued ülesanded peavad toetama kehtivaid koostöömehhanisme, ei tohi luua paralleelseid infovahetuskanaleid ega mõjutada negatiivselt riiklike küberintsidentide käsitlemise üksuste ja erasektori vahelist koostööd.

- Eesti peab oluliseks, et IKT tarneahelate turvalisuse tagamisel pööratakse tähelepanu ka mittetehniliste riskide maandamisele, kuid selleks eelnõus kavandatavad meetmed peavad olema proportsionaalsed ja sihitud. Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaksmääramisel peab liikmesriikidel olema tugev roll, et tagada mittetehniliste riskide määratlemise protsessi läbipaistvus ja usaldusväärsus.

- Eesti toetab eelnõus küberturvalisuse riskijuhtimismeetmete tagamisega seotud nõuete sõnastamist viisil, mis võimaldab liikmesriigil kehtestada riigispetsiifilisi riskijuhtimismeetmete nõudeid ka nende üksuste suhtes, kes on hõlmatud Euroopa Komisjoni samade nõuete alusel vastu võetud rakendusaktiga.

1. Sissejuhatus

Eesti seisukohad on koostatud järgmiste ettepanekute kohta:

1) COM (2026) 11: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS, mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (ENISA), Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 (küberturvalisuse 2. määrus);[1]
2) COM (2026) 13: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga].[2]

Küberturvalisuse 2. määruse ettepaneku (edaspidi *CSA2*) eesmärk on tugevdada Euroopa Liidu küberturvalisust. Küberrünnakute arv on kasvanud ning nende laad muutunud üha keerukamaks, mõjutades elutähtsat taristut, ettevõtjaid ja ühiskonda tervikuna. Uued tehnoloogiad, sealhulgas tehisintellekt ja kvantarvutus, kujundavad ümber nii küberkaitsevõime ülesehitust kui ka vastaste tegutsemisviise. Püsivad küberturvalisuse ohud ei kujuta endast üksnes tehnilisi väljakutseid, vaid strateegilisi riske demokraatiale ja majandusele.

Seda tausta arvestades on CSA2 kavandatava läbivaatamise eesmärk käsitleda nelja peamist probleemi:

1) Liidu küberturvalisuse poliitikaraamistiku ebapiisav vastavus sidusrühmade vajadustele üha keerulisemas ohukeskkonnas;

2) Euroopa küberturvalisuse sertifitseerimisraamistiku (ECCF) aeglane rakendamine;

3) Liidu küberturvalisuse poliitikaraamistiku parem kohandamine sidusrühmade vajadustele üha keerulisemas ohukeskkonnas;

4) IKT-tarneahelate turvalisusega seotud mitte-tehniliste riskide vähendamine.

Üldeesmärk on tugevdada liidu küberturvalisuse juhtimist ning tagada, et asjaomased institutsioonid, asutused ja muud sidusrühmad oleksid küberturbeohtude ennetamiseks, avastamiseks ja neile reageerimiseks paremini ette valmistatud ning suudaksid tegutseda koordineeritult ja tõhusalt. Samuti on eesmärk toetada ühiste liidu küberturbeinstrumentide, sealhulgas sertifitseerimiskavade, väljatöötamist, rakendamist ja laiemat kasutuselevõttu ning luua ühtlustatud raamistikud, mis suurendavad liikmesriikidevahelist usaldust ja koostalitlusvõimet.

Tegemist on seadusandliku tavamenetlusega. CSA2 vastuvõtmiseks nõukogus on vaja kvalifitseeritud häälteenamust. CSA2 arutelud Euroopa Liidu nõukogu horisontaalse küberasjade töögrupis on juba alanud.

[1] https://eur-lex.europa.eu/procedure/ET/2026_11
[2] https://eur-lex.europa.eu/procedure/ET/2026_12

Küberturvalisuse 2. direktiivi (edaspidi *NIS2*) muutmise ettepaneku eesmärk on CSA2 tõttu teha lihtsustamismeetmeid kehtivas direktiivis, et lahendada Euroopa Liidu turvalisuse olekut mõjutava küberturvalisusega seotud poliitika keerukuse ja mitmekesisuse probleemi, eelkõige tehes täpsustusi osade direktiiviga reguleeritud üksuste sõnastustes ja lihtsustades nõudeid, mida need üksused peavad täitma. NIS2 muudatuste eesmärki tuleks käsitada osana CSA2 vastu võtmise eesmärkidest – ennekõike on siin seos CSA2 4. erieesmärgiga, st luua mehhanismid ja tingimused, mis aitavad hõlbustada küberturvalisuse nõuete täitmist ning muuta seeläbi nende rakendamine sidusamaks ja tulemuslikumaks. NIS2 sihipäraste muudatuste eesmärk on lihtsustada küberturvalisuse raamistiku konkreetsete aspektide järgimist ning tagada nende sujuv ja sidus rakendamine, sealhulgas seoses kohaldamisala, määratluste, lunavaraintsidentidest teatamise ja piiriüleseid teenuseid osutavate üksuste järelevalvega.

Tegemist on seadusandliku tavamenetlusega. NIS2 muutva direktiivi vastuvõtmiseks nõukogus on vaja kvalifitseeritud häälteenamust. Eelnõude subsidiaarsustähtpäev oli 13. mai 2026. NIS2-ga seotud muudatusi arutatakse CSA2 ettepaneku järel, kuid Euroopa Liidu nõukogu horisontaalse küberasjade töögrupis ei ole asjakohased arutelud seisukohtade koostamise hetkel veel alanud.

2. Koostajad

Seisukohad ja seletuskirja koostasid Justiits- ja Digiministeeriumi EL asjade nõunik Sandra Kaljumäe (sandra.kaljumae@justdigi.ee), digitaristu- ja küberturvalisuse osakonna küberturvalisuse talituse rahvusvahelise küberturvalisuse koostöö juht Carmen Raal (Carmen.Raal@justdigi.ee), sama talituse õigusnõunikud Raavo Palu (Raavo.Palu@justdigi.ee) ja Guido Pääsuke (Guido.Paasuke@justdigi.ee).

Digitaristu- ja küberturvalisuse valdkonna eest vastutab Justiits- ja Digiministeeriumi asekantsler Tõnu Grünberg (Tonu.Grunberg@justdigi.ee).

3. Sisu ja võrdlev analüüs

3.1. CSA2

20.01.2026 esitas Euroopa Komisjon määruse ettepaneku, mis käsitleb Euroopa Liidu Küberturvalisuse Ametit (edaspidi *ENISA*), Euroopa küberturvalisuse sertifitseerimise raamistikku ning info- ja kommunikatsioonitehnoloogia (IKT) tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/881 ehk küberturvalisuse määrus .

CSA2 ettepanek käsitleb ENISAt, Euroopa küberturvalisuse sertifitseerimise raamistikku ja IKT tarneahela turvalisust ning millega tunnistatakse kehtetuks määrus (EL) 2019/8813.

I jaotis - Üldsätted

I jaotis sätestab määruse üldise raamistiku. Selles määratakse kindlaks määruse reguleerimise ja kohaldamisala, eelkõige ENISA missioon, eesmärgid, ülesanded ja korraldus, Euroopa küberturvalisuse sertifitseerimise raamistik ning usaldusväärse IKT tarneahela raamistik.

Samuti rõhutatakse, et määrus ei piira liikmesriikide põhifunktsioone ega nende ainuvastutust riigi julgeoleku eest. Lisaks koondab I jaotis määruses kasutatavad põhimõisted. Kokkuvõttes loob I jaotis aluse kogu määruse edasisele sisule, määratledes selle kohaldamisala, peamised raamistikud ja keskse terminoloogia.

II jaotis – Euroopa Liidu Küberturvalisuse Amet

Kavandatud määruse II jaotis käsitleb ENISA rolli ja toimimist Euroopa Liidu küberturvalisuse raamistikus. Selles määratakse kindlaks ENISA missioon, eesmärgid ja peamised ülesanded, mille keskmes on liidu küberturvalisuse poliitika toetamine, liikmesriikide suutlikkuse suurendamine ning koostöö parandamine küberohtude ja -intsidentide ennetamisel ja neile reageerimisel. ENISA ülesanded hõlmavad muu hulgas olukorrateadlikkuse parandamist, varajaste hoiatuste andmist, Euroopa Liidu küberreservi käitamist, küberturvalisuse õppuste korraldamist, nõrkusehalduse arendamist ning küberturvalisuse sertifitseerimise, standardimise ja oskuste edendamist. Lisaks sätestatakse jaotises ENISA juhtimis- ja töökorraldus, eelarve- ja personalireeglid ning üldised normid, mis puudutavad ENISA õiguslikku staatust, koostööd liikmesriikide, Euroopa Liidu asutuste, kolmandate riikide ja teiste sidusrühmadega, samuti teabe kaitset ja vastutust. Kokkuvõttes tugevdab II jaotis ENISA positsiooni Euroopa Liidu keskse küberturvalisuse asutusena, andes ametile nii strateegilised, operatiivsed kui ka tehnilised ülesanded.

Võrreldes kehtiva küberturvalisuse määrusega muutub ENISA roll operatiivsemaks ning ENISA saab suurema vastutuse sertifitseerimisskeemide väljatöötamisel. Selgemalt on esile toodud vajadus toetada küberturvalisuse õigusaktide ja poliitikameetmete rakendamise toetamist. Lisaks rõhutatakse sihipärase toe pakkumise olulisust konkreetsetele sektoritele ning olulisust panustada suutlikkuse suurendamisse. Määrusega (EL) 2019/881 võrreldes tuuakse sisse küberturbeoskuste akadeemia rakendamine ja küberturbeoskuste tõendamise kava väljatöötamine.

ENISA rolli tugevdatakse CSIRTide võrgustiku liikmena, eelkõige olukorrateadlikkuse parandamise, varajaste hoiatuste ja analüüside jagamise ning turvaliste sidevahendite kasutamise kaudu. Samuti nähakse ENISAle ette senisest olulisem roll nõrkusehalduses, sealhulgas nõrkustega seotud teenuste arendamisel ja asjakohaste soovituste andmisel. Lisaks toetab ENISA intsidentidest ja nõrkustest teatamise platvormide haldamist ning aitab kaasa küberintsidentidele reageerimisele. Eraldi rõhku pannakse lunavararünnete vastase võimekuse tugevdamisele, sealhulgas soovile luua ettevõtetele keskne kasutajatugi.

III jaotis – Euroopa küberturvalisuse sertifitseerimise raamistik

III jaotis keskendub Euroopa küberturvalisuse sertifitseerimise raamistikule. Eesmärk on hõlbustada vastavust küberkerksuse määrusele (edaspidi *CRA*[3]) ja NIS2-le ning potentsiaalselt ka teistele õigusaktidele. Võrreldes kehtiva küberturvalisuse määrusega, kus oli skoobis määratletud IKT-tooted, IKT-teenused, IKT-protsessid ja hallatud turbeteenused, siis uue määrusega lisandub juurde veel üksuste turvaolek. Üksuste turvaolek on sisuliselt organisatsiooni või asutuse küberturvalisuse tase ehk see kui hästi on tema süsteemid,

[3] Regulation - 2024/2847 - EN - EUR-Lex

protsessid ja korralduslikud meetmed küberriskide vastu kaitstud. Euroopa Komisjoni selgituse järgi saavad üksused tulevikus sertifitseerida oma turvaolekut, et tõendada vastavust näiteks NIS2-le ja teistele õigusaktidele. Võrreldes kehtiva määrusega tuuakse selgemalt välja ka sertifitseerimisskeemide rollijaotus ja tähtajad. ENISA-l on 12 kuud, et koostada küberturvalisuse sertifitseerimise ettevalmistava kava.

IV jaotis - IKT tarneahelate turvalisus

IV jaotis käsitleb mittetehnilisi riske IKT tarneahelate turvalisuse vaatest. Varasemad õigusraamistikud (NIS2, CRA) keskenduvad tehniliste riskide maandamisele ning mittetehnilsite IKT tarneahelate riskidega pole Euroopa Liidul olnud võimalik ühtselt tegeleda.

Menetluse võib algatada komisjon või vähemalt kolm liikmesriiki. Lisaks, on komisjonil võimalik algatada erakorraline menetlus. Menetlus hõlmab riskihindamiste tegemist, oluliste varade kindlaksmääramist ning riskipõhiste ja proportsionaalsete leevendusmeetmete kohaldamist, lähtudes turuanalüüsist ning majandusliku ja ühiskondliku mõju põhjalikust hindamisest. Tekib võimalus kehtestada piiranguid ka konkreetsetele kolmandate riikide ettevõtjatele. Kehtestatud meetmed kehtivad NIS2 I ja II lisas osutatud liiki üksuste jaoks.

Raamistik näeb ette küberturvalisuse seisukohast muret tekitavate riikide kindlaksmääramist vastavate kriteeriumide alusel. Samuti hõlmab see oluliste IKT-varade kindlakstegemist, leevendusmeetmete, sealhulgas võimalike piirangute kohaldamist ning vajaduse korral üleminekuperioodi ette nägemist konkreetsete tarneahelate jaoks teatavate kriitilise tähtsusega üksuste puhul. Komisjon peab ja ajakohastab tehtud otsuste osas avalikku registrit, kus on märgitud üksuste nimed, kellele piirangud kehtima hakkavad.

VI jaotis - Lõppsätted

VI jaotis sisaldab määruse lõppsätteid, millega reguleeritakse komiteemenetlust, komisjoni delegeeritud volituste kasutamist, määruse korrapärast hindamist ja läbivaatamist ning senise määruse (EL) 2019/881 kehtetuks tunnistamist. Samuti sätestatakse selles õigusjärgluse põhimõtted, et tagada ENISA tegevuse, olemasolevate otsuste ja käimasolevate menetluste sujuv jätkumine uue määruse alusel.

3.2. NIS2 muudatused

NIS2 muutva direktiivi ettepanek käsitleb NIS2 sihipäraseid muudatusi, et lihtsustada küberturvalisuse raamistiku konkreetseid aspekte, suurendada õiguskindlust ja ühtlustada rakendamist.

Kohaldamisala ja üksused

Kohaldamisala puhul jäetakse NIS2 kohaldamisalast välja mikro- ja väikeettevõtjatest domeeninimede süsteemi teenuse osutajad. Kohaldamisalasse lisanduvad digiidentiteedikukrute pakkujad ja Euroopa ettevõtluskukrute pakkujad ning need üksused, kes

on eraldiseisva EL määruse ettepaneku[4] kohaselt kindlaks määratud strateegilise kahesuguse kasutusega taristu omanike, haldajate ja käitajatena. Kohaldamisala kontekstis muudetakse ka NIS2 I ja II lisade sõnastusi. Näiteks arvatakse NIS2 kohaldamisalast välja elektrienergia tootjad, kelle kogu tootmisvõimsus ei ületa 1 MW. Samuti parandatakse viiteid seoses vesiniku[5] ja intelligentsete transpordisüsteemidega[6] seotud üksustega kui ka üksustega, kellele ei kohaldata Euroopa Parlamendi ja nõukogu direktiivi[7] 2011/24/EL (st pikaajalise hoolduse teenused). Samuti korrigeeritakse kemikaalide valdkonnaga seotud üksuste sõnastusi: edaspidi on "kemikaalide valmistamise, tootmise ja levitamise" asemel NIS2ga hõlmatud "kemikaalide valmistamine ja tootmine". Samas lisatakse I lisasse merealuse andmeedastustaristu operaatorid tingimusel, et nad ei ole hõlmatud muud liiki üksusena.

Lisandunud üksuste puhul käsitatakse NIS2 tähenduses elutähtsate üksustena digiidentiteedikukrute pakkujad, Euroopa ettevõtluskukrute pakkujad ning üksused, mis on kindlaks määratud strateegilise kahesuguse kasutusega taristu omanike, haldajate ja käitajatena. Elutähtsate üksustega seonduvalt võetakse kasutusele uus kategooria – väikeste keskmise turukapitalisatsiooniga ettevõtja (edaspidi *VKTKE*)[8] – , mille nõuetele vastavad üksused tuleb edaspidi määrata olulisteks üksusteks (varem olid nad NIS2 tähenduses elutähtsad üksused), vähendades nende nõuete täitmisega seotud koormust ja pädevate asutuste järelevalvekoormust. VKTKEdest suuremad üksused on edaspidi elutähtsad üksused. Domeeninimede süsteemi teenuse osutajad on edaspidi olulised üksused. Lisanduvate üksuste puhul täiendatakse ka mõisteid: ettepanekuga lisatakse VKTKE mõiste (komisoni soovituse[9] (EL) 2025/1099 lisas määratletud ettevõtja) ning merealuse andmeedastustaristu mõiste (andmeid edastavad merekaablid, nendega seotud taristu ja muud andmeedastusega seotud rajatised või elemendid).

Üksuste kohta käivad andmed ja ENISA register

Ettepanekuga muudetakse ka andmekoosseisude nimetusi, mida üksuste kohta kohustuslikus korras kogutakse (kui üksus neid kasutab ehk kui tal on need andmed olemas): täiesti uus on üksuse Euroopa ettevõtluskukru(te) kordumatu(d) tunnus(ed) ja digitaal(ne/sed) aadress(id). Ülejäänud andmekoosseisu on juba kehtivas direktiivis juba olemas. Lisaks muutub teatud üksuste (digitaalse teenuse osutajate) puhul nõue, mis aja jooksul nad peavad enda andmeid uuendama, kui nendes on toimunud muudatused. Hetkel on neil selleks aega kuni kolm kuud,

[4] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52025PC0847&qid=1776094303364
[5] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024L1788&qid=1776094772390
[6] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02010L0040-20231220&qid=1776094831948
[7] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02011L0024-20250112&qid=1776094876153
[8] Mikro-, väikeste ja keskmise suurusega ettevõtete (VKEd) kategooriasse kuuluvad ettevõtted, millel on vähem kui 250 töötajat ja mille aastakäive ei ületa 50 miljonit eurot ja/või aastabilansi kogumaht ei ületa 43 miljonit eurot.
Väikeste keskmise turukapitalisatsiooniga ettevõtjate kategooriasse kuuluvad ettevõtjad, kes ei ole väikesed ja keskmise suurusega ettevõtjad soovituse 2003/361/EÜ järgi, kellel on vähem kui 750 töötajat ja kelle aastakäive ei ületa 150 miljonit eurot või aastabilansi kogumaht ei ületa 129 miljonit eurot.
https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32025H1099, lisa punkt 2.

kuid ettepaneku tulemusena on selleks aega kuni kaks nädalat (sarnaselt nende üksustega, kes ei ole digitaalse teenuse osutajad).

Ettepanekuga muudetakse ka seda, mis teavet liikmesriigi üksuste kohta ENISAle edastatakse liikmesriigi keskse kontaktpunkti (Eestis Riigi Infosüsteemi Ameti) poolt. Kui hetkel on ENISA ülesanne pidada registrit, milles on digitaalsete teenuste teatud valdkondadega seotud üksused (nt need, mis on seotud ennekõike liikmesriikide piire ületavate teenustega; ehk nn digitaalse teenuse osutajad), siis edaspidi tuleb ENISA-le edastada tema peetavasse registrisse kõikide üksuste kõik andmed, kes on liikmesriigi siseriikliku õigusakti (millega NIS2 üle võeti) kohaldamisalas: NIS2 mõttes elutähtsad üksused ja olulised üksused, Domeeninimede registreerimise teenuse osutajate puhul otsesõnu taolist edastamise kohustust ei ole ette nähtud, kuid ettepaneku kohaselt sisaldab register ka nende üksuste kohta käivaid andmeid. Eesti puhul tähendab see muudatus, et sinna registrisse esitatakse (sisuliselt) kõikide üksuste andmed, kes on enda andmed pädevatele asutustele (Riigi Infosüsteemi Amet, Kaitsepolitseiamet, Välisluureamet) esitanud, st nii avalikust- kui erasektorist. Pädevad asutused saavad taotleda juurdepääsu ENISA registrile ainult osas, mis on seotud eelmainitud digitaalsete teenuste osutajate andmetega. Samas ei ole ettepanekus täpsemalt reguleeritud selle registri pidamisega seotud muud asjaolud: mida ENISA nende andmetega teeb, kes ja millisel õiguslikul alusel saab juurdepääsu registri andmetele, millal andmed kustutatakse jne. Ettepanekuga muudetakse tähtaega, mis aja jooksul peavad digitaalse teenuse osutajad enda andmete muutumise korral enda andmeid uuendama – varem oli selleks aega kuni kolm kuud, kuid edaspidi on selleks aega kuni kaks nädalat.

Küberturvalisuse riskijuhtimismeetmed

Ettepanekuga soovitakse saavutada NIS2 artikli 21 lõike 5 kohaste rakendusaktide (milles täpsustatakse küberturvalisuse riskijuhtimismeetmed) võimalikult suur ühtlustamine, et hõlbustada üksuste jaoks nõuete täitmist ja ametiasutuste jaoks järelevalve tegemist. Selleks hindab komisjon edaspidi regulaarselt, kas on vaja tolle artikli alusel teha rakendusakte, nt konkreetse sektori või ettevõtja tüübi jaoks. Ettepanekuga nähakse ette, et kui komisjoni on teinud viidatud sätte alusel rakendusakti(d), siis liikmesriigid ei kehtesta nende rakendusakti(de) kohaldamisalasse kuuluvatele üksustele NIS2 artikli 21 lõikes 2 osutatud meetmetega seoses täiendavaid tehnilisi, metoodilisi ega valdkondlikke nõudeid. Ettepanek ei anna aimu, kas rakendusaktide puhul nähakse ette ka üleminekuajad, mis ajaks rakendusaktis nimetatud üksus peab vastavad nõuded ära täitma.

Lisaks pakutakse ettepanekus välja, et komisjon võtaks vastu suunised selliste tarneahela turvanõuete kohaldamise kohta, mida NIS2 kohaldamisalasse kuuluvad üksused nõuavad oma tarnijatelt, et tagada õiguskindlus ja vältida kohustuste põhjendamatut edasiandmist üksustele, mis ei kuulu NIS2 kohaldamisalasse. Paraku ei ole ettepanekust selgelt näha, millise NIS2 artikli alusel vastav ülesanne komisjonile antakse, kuid arvatavasti on selle puhul tegemist komisjonile antava ülesandega ettepanekuga ette nähtud direktiivi põhjenduse tasandil, mis viiakse ellu NIS2 artikli 21 lõike 5 alusel antavas rakendusaktis.

Lunavara

Ettepanekuga soovitakse ühtlustada ühe olulise intsidendiga seotud andmete kogumist: soovitakse ette näha, et kui komisjon annab NIS2 art 23 lõike 11 alusel rakendusakti, siis peab komisjon rakendusaktis ette nägema lunavara korral teatud andmekoosseisud. Lisaks soovitakse kindlaks määrata, mis laadi teavet võib pädev asutus lunavara olukorras teavituse esitanud üksuselt küsida: kas üksus on saanud lunavaranõude ja asjakohasel juhul ka nõude esitaja info; ning kas lunaraha on makstud ja kui on, siis milline summa, millise maksevahendi kaudu ja millisele saajale, sh asjakohasel juhul krüptovara ja krüptovarateenuse osutaja andmed.

Küberturvalisuse sertifitseerimine

Selleks et üksustel ja tarnijatel oleks lihtsam tõendada vastavust NIS2le, on NIS2ga reguleeritud üksustel võimalik saada sertifikaate organisatsioonide küberturvalisuse sertifitseerimise kavade alusel, mis on välja töötatud Euroopa küberturvalisuse sertifitseerimise raamistikus kooskõlas CSA2ga. Ettepanek näeb liikmesriikidele ette võimaluse näha ette kohustuse NIS2ga reguleeritud üksustele, et üksus saaks sertifikaadi küberturvalisuse sertifitseerimise kavade alusel, mis on välja töötatud Euroopa küberturvalisuse sertifitseerimise raamistikus kooskõlas CSA2ga. Lisaks näeb ettepanek sisuliselt ette ka võimalus, et üksus võib vabatahtlikult saada eelmainitud sertifikaati, et tõendada enda organisatsiooni vastavust NIS2s ette nähtud küberturvalisuse riskijuhtimismeetmetega seotud nõuetele (mille detailid on ette nähtud komisjoni rakendusaktis või liikmesriigi enda õiguses). Sel juhul ei või liikmesriigid nende üksuste suhtes kohaldada järelevalvemeetmena sihipärast turvaauditit nende valdkondade või teenuste osas, mis on sertifikaadi käsitlusala.

ENISA ülesanded ja pädevused

Ettepanekuga lisatakse küberintsidentide käsitlemise riiklike üksuste võrgustiku ehk CSIRTide võrgustiku liikmeks ka ENISA (mis hetkel on sekretariaaditeenuse osutamise ja toetavas rollis).

Mitme riigiga seotud üksustes küberturvalisuse riskijuhtimismeetmete järgimise hõlbustamiseks (mille üle teevad järelevalvet mitme liikmesriigi pädevad asutused), antakse ENISAle uus roll toetada liikmesriike nende üksuste järelevalves, hõlbustades vastastikust abi ja luues parema ülevaate NIS2 kohaldamisalasse kuuluvatest üksustest. ENISA analüüsib põhjalikult piiriüleseid küberriske seoses piiriüleste üksustega ning analüüsi käigus hinnatakse elutähtsaid ja olulisi üksuseid mõjutavate intsidentide võimalike piiriüleste ja siseturule avalduvate tagajärgede ulatust. ENISA töötab nimetatud analüüsi metoodika välja koostöös komisjoni ja NIS2 artiklis 14 nimetatud koostöörühmaga. Analüüsi pinnalt koostatakse piiriülese küberriski hindamise aruanne, mida uuendatakse igal aastal. Selle aruande põhjal võib ENISA: soovitada mitme riigi pädevaid järelevalveasutusi looma ühiseid järelevalve rühmi; koostada suuniseid ühiste järelevalvemeetmete kohta või asjaomaste riikide pädevate asutuste taotluse korral praktilise korra ühiste järelevalvemeetmete võtmiseks; abistada liikmesriike järelevalves (näiteks ise osaleda järelevalves või aidata hinnata konkreetse üksuse küberturvalisuse taset: selleks tuleb esitada kogu teave, sh järelevalve failid ja üksuse enda dokumendid ENISAle). Liikmesriigi kontaktpunkt peab edaspidi teavitama ENISAt, kui vastastikuse abi meedet kasutati kahe riigi vahel, sh anda teada ka millise piiriülese intsidendi tõttu seda tehti.

Muud muudatused

Ettepanekuga muudetakse ka NIS2 minimaalse ühtlustamise eesmärki, lisades seos NIS2 artikli 21 lõike 5 viienda lõiguga. Samuti kehtestatakse nõue liikmesriikidele seoses riigi loodava küberturvalisuse valdkonna strateegiaga – see peab sisaldama ka poliitikameetmeid postkvantkrüptograafiale üleminekuks, võttes arvesse kohaldatavates liidu õigusaktides ja poliitikas sätestatud ülemineku tähtaegu ja asjakohaseid nõudeid. Ettepanekuga muudetakse lennuettevõtjatega seotud jurisdiktsiooni ning ka seda, millal Euroopa Liidu väline üksus peab esindaja määrama.

Liikmesriikidel on aega ettepanekus toodud õigusnormide üle võtmiseks 12 kuud.

4. Euroopa Liidu asja vastavus pädevuse andmise, subsidiaarsuse ja proportsionaalsuse põhimõtetele

4.1. Õiguslik alus

Mõlema ettepaneku (CSA2 ja NIS2 muutva direktiivi) õiguslikuks aluseks on valitud Euroopa Liidu toimimise lepingu artikkel 114, millega on ette nähtud meetmete võtmine, et tagada siseturu loomine ja toimimine. Selle sätte alusel on vastu võetud ka määrus (EL) 2019/881, mis käsitleb ENISAt ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist (tuntud kui küberturvalisuse määrus) kui ka NIS2.

4.2. Subsidiaarsus

4.2.1. CSA2

CSA2 keskendub peamiselt kolmele valdkonnale: ENISA mandaadile, küberturvalisuse sertifitseerimisskeemidele ning IKT tarneahela riskide maandamisele. Kõigis neis küsimustes annab Euroopa Liidu tasandi regulatsioon lisaväärtuse. ENISA rolli tugevdamine aitab tagada liikmesriikide parema koostöö ja koordineerituse. Ühtsed sertifitseerimisskeemid aitavad vältida olukorda, kus ettevõtted peavad täitma eri liikmesriikides erinevaid nõudeid. Samuti eeldab IKT tarneahela mittetehniliste riskide maandamine ühist lähenemist, sest tarneahelad on rahvusvahelised ja ühe liikmesriigi meetmetest üksi ei piisa.

CSA2 ei ole vastuolus subsidiaarsuse põhimõttega, sest käsitletavad küsimused on oma olemuselt piiriülesed ning neid ei ole võimalik riigi tasandil piisava tõhususega lahendada. Küberturvalisuse ohud, eriti IKT tarneahelaga seotud riskid, ei piirdu ühe liikmesriigi territooriumiga, vaid mõjutavad kogu Euroopa Liitu.

4.2.2. NIS2 muudatused

Eesti hinnangul on Euroopa Liidu sekkumine võrgu- ja infoturbe vallas on õigustatud subsidiaarsuse põhimõttega. Direktiiv kohaldub valdkonnas, kus on üha enam piiriüleseid mõjusid. NIS2 sihipäraste muudatuste eesmärk on lihtsustada küberturvalisuse raamistiku konkreetsete aspektide järgimist ning tagada nende sujuv ja sidus rakendamine, sealhulgas seoses kohaldamisala, määratluste, lunavaraintsidentidest teatamise ja piiriüleseid teenuseid osutavate üksuste järelevalvega. Käesolev ettepanek soodustab liidu küberturvalisuse

õigusaktide järgimist, vähendades mõjutatud üksuste nõuete täitmisega seotud kulusid ja õiguskindlusetust ning hõlbustades ja parandades küberturvalisuse nõuete täitmise määra. Samuti aitab see liikmesriikides ühtlustada lähenemisviise järelevalvele ja vastavuskontrollile.

4.3. Proportsionaalsus

4.3.1. CSA2

Euroopa Liidu lepingu artikli 5 lõikes 4 sätestatud proportsionaalsuse põhimõtte kohaselt peavad konkreetse meetme laad ja tugevus olema vastavuses tuvastatud probleemiga.

Komisjoni hinnangul on CSA2 proportsionaalsus tagatud, kuna kavandatud meetmete eesmärk on kajastada õiguslikult paremini ENISA volitusi ning Euroopa küberturvalisuse sertifikaatide väljatöötamise, vastuvõtmise ja haldamise protsessi. Lisaks, mis puudutab IKT tarneahelate turvalisust, eesmärk on vähendada küberturvalisuse osas ohtu kujutavate kolmandate riikide tarnijate riske Euroopa Liidu IKT tarneahelast. Raamistikus on ette nähtud tõendite kogumine oluliste varade ning meetmete kohta, mis oleksid proportsionaalsed ja vajalikud, et vähendada riske kriitilise tähtsusega tarneahelates.

Eesti hinnangul on kavandatud meetmed üldises plaanis proportsionaalsed. Siiski tuleks suuremat tähelepanu pöörata sellele, et meetmete kavandamisel oleks selgelt eristatud ühelt poolt need tegevused, mis eeldavad Euroopa-ülest koordineerimist, et tagada küberturvalisuse tulemuslik ja ühtlane tugevdamine kõigis liikmesriikides. On oluline selgelt piiritleda ka need ülesanded ja vastutusvaldkonnad, mille prioriseerimine ning elluviimine peaks jääma liikmesriikide siseseks pädevuseks, arvestades riikide erinevaid vajadusi, riskiprofiile ja olemasolevaid võimekusi.

4.3.2. NIS2 muudatused

Käesoleva direktiivi kavandatud eeskirjadega reguleeritakse üksnes seda, mis on vajalik, et saavutada kindlad eesmärgid rahuldaval tasemel. Kavandatav kohaldamisala, turvameetmete ja teatamiskohustuste vastavusse viimine ja ühtlustamine lähtub liikmesriikide ja ettevõtjate taotlustest praegust raamistikku parandada.

Ettepanekuga muudetakse kehtivat NIS2 ja ühtlustatakse veelgi ettevõtjatele kehtestatud kohustusi, tagades seega kogu liidus ühtlasema taseme. Käesoleva ettepaneku jaoks valitud vahend on vastab muudetavale õigusaktile, s.t NIS2le. Käesolevas ettepanekus tuginetakse NIS2 eesmärgile anda liikmesriikidele paindlikkus, mida on vaja riiklike eripärade arvesse võtmiseks.

Eesti hinnangul on kavandatavad meetmed õigustatud proportsionaalsuse põhimõttega, kuid läbirääkimiste käigus tuleb veelgi rõhuda paindlikkusele, kaasamaks konkreetsemalt ja selgemalt vaid kriitilisemad sektorid, sätestamaks proportsionaalsed nõuded ning vältimaks liigse halduskoormuse tekitamist väikestele ettevõtetele.

5. Esialgne mõjude analüüsi kokkuvõte

5.1. CSA2

Esialgse hinnangu kohaselt toob CSA2 kaasa mõju ettevõtetele, regulaatoritele ja riigieelarvele.

Mõju ettevõtjatele

Komisjoni hinnangul, turu killustatuse vähendamine ja regulatiivsete nõuete ühtlustamine aitavad valitud lahenduste kaudu parandada Euroopa Liidus võrdseid konkurentsitingimusi ning annavad ettevõtjatele selgema raamistiku nii nõuete täitmiseks kui ka innovatsiooni edendamiseks.

Euroopa sertifitseerimisskeemide abil tekib võimalus tõendada küberriskide juhtimise nõuete täitmist. See võib vähendada dubleerivaid kontrolle, teha järelevalve ühtlasemaks. Lisaks, peaks vähenema eri riikide erinevatest tõendamisnõuetest tulenev koormus, mis teeb piiriülese tegutsemise lihtsamaks. Komisjon on hinnanud, et lihtsustatud ja vähendatud vastavuskohustused võimaldavad ettevõtjatel viie aasta jooksul kokku hoida kuni 15,3 miljardit eurot.

Seoses IKT tarneahelate turvalisusega on Komisjon hinnanud, kõrge riskiga tarnijatekõrvaldamine võib tuua mobiilsideoperaatoritele viie aasta jooksul kaasa kulu suurusega 3,4–4,3 miljardit eurot aastas ning investeeringud usaldusväärsetesse tarnijatesse võivad kasvada kuni 2 miljardile eurole aastas, kuid see hinnang on kogu Euroopa Liidu peale kokku. Praeguses etapis on täpset kulu Eesti ettevõtjatele veel keeruline hinnata, kuna CSA2-s ei ole ära määratletud, kui sügavale tarneahelates riskihinnangud võivad minna, st seisukohtade koostamise hetkel puudub selgus, mis valdkonna tehnoloogia ja nendega seotud komponentide osas võidakse CSA2-s neid nõudeid ette näha. Lisaks on Eesti rakendanud 5G turvalisuse tööriistakasti, mille raames oleme juba tegelenud ka mittetehniliste riskidega elektroonilise side sektoris. Sellest tulenevalt võivad täiendavad kulud Eestile olla minimaalsed või neid ei pruugi üldse tekkida.

Mõju regulaatoritele (RIA, TTJA ja teised asutused)

CSA2 toob regulaatoritele rohkem kontrolli-, hindamis- ja rakendusülesandeid, mis tähendab, et hinnanguliselt võivad avalikus sektoris kulud kasvada kuni 80 miljonit eurot viie aasta jooksul.

Personalikulude kasv on tõenäoline, kuna IKT tarneahelatega seotud riskide käsitlemine nõuab liikmesriikidelt senisest suuremat ja järjepidevamat panust Euroopa tasandi koostöövormidesse. Eelkõige tähendab see aktiivsemat osalemist NIS CG tegevustes, sealhulgas riskide hindamises, seisukohtade kujundamises ja ühiste lähenemiste väljatöötamises. Lisaks eeldab ENISA rolli tugevnemine suuremat panust ka liikmesriikidelt, muu hulgas riiklike ekspertide (SNEde) lähetamise kaudu. Sellega kaasneb vajadus planeerida täiendavaid personalikulusid, kuna ekspertide suunamine Euroopa tasandi ülesannetesse võib vähendada riigisisest võimekust ning nõuda asenduste või lisapersonali kaasamist.

Mõju riigieelarvele

Praeguses etapis on täpset kulu veel keeruline hinnata, kuna CSA2-s ei ole ära määratletud, kui sügavale tarneahelates riskihinnangud võivad minna, st puudub siinsete seisukohtade koostamise hetkel selgus, mis valdkonna tehnoloogia ja nendega seotud komponentide osas võidakse neid nõudeid ette näha. Lisaks on Eesti rakendanud 5G turvalisuse tööriistakasti[9], mis hõlmab ka mittetehnilisi riske. Seetõttu ei ole selge, kas CSA2 rakendamiseks tuleb veel midagi lisaks teha (näiteks Eesti õigusakti või olemasoleva protsessi muutmine) või kehtestatakse tulevikus kesksed ELi ülesed nõuded, mida Eesti on juba täitnud. Komisjon on välja toonud järelevalvekulu mõju avaliku sektori asutustele kogu Euroopa Liidus, mis on kuni 80 miljonit eurot viie aasta jooksul. Eesti peaks arvestama kuludega eelkõige järelevalveks, täiendavaks personaliks ja tarneahela riskide maandamiseks. Eelarvelisi kulusid menetletakse edaspidi riigieelarve strateegia ja riigieelarve koostamise käigus vastavalt riigi eelarvelistele võimalustele. Eesti eesmärk on saavutada eelnõu läbirääkimistel proportsionaalne lahendus, mis jätaks liikmesriikide ühekordsed ja püsikulud võimalikult madalaks.

Algse lisakulu kõrval võib tekkida ka hilisem halduslik kokkuhoid, kuna üks eesmärke on vähendada killustatust ja parandada koordineerimist, mis peaks tagama vahendite tõhusama kasutamise riiklikes asutustes.

5.2. NIS2 muudatused

Esialgse hinnangu kohaselt toovad NIS2 muudatused kaasa mõju KüTSi kohaldamisalas olevatele üksustele (erasektorist ja avalikust sektorist), pädevatele asutustele, Justiits- ja Digiministeeriumile kui ka riigieelarvele.

Mõju KüTSi kohaldamisalas olevatele üksustele

Mikro- ja väikeettevõtjatest domeeninimede süsteemi teenuse osutajatele avaldub mõju selles, et nad ei pea ettepaneku kohaselt edaspidiselt NIS2 nõudeid järgima. Samuti muudetakse elektrienergia tootmisega seotud sõnastust, millega on edaspidi NIS2 kohaldamisalast välistatud need elektrienergia tootjad, kelle kogu tootmisvõimsus ei ületa 1 MW. Ettepanekuga parandatakse ka teatud valdkondade (vesinik, intelligentsed transpordisüsteemid, pikaajalise hoolduse teenuse, kemikaalid) üksustega seotud sõnastusi. Kuna Eestis on siinsete seisukohtade koostamise hetkel KüTSi subjektide nimekiri alles koostamisel, siis ei ole ka võimalik anda hinnangut kui paljusid taolisi üksusi see muudatus mõjutab. Üksused, kelle kohaldamisala määratlemisega seotud sõnastusi korrigeeritakse – nende puhul on eelduslikult ettepanekuga seotud mõjud samad, mis on üksustel, kelle sõnastuses muudatusi ei tehta, mistõttu ei analüüsita neid eraldi sihtgrupina.

Uute lisanduvate üksuste (st digiidentiteedikukrute pakkujad, Euroopa ettevõtluskukrute pakkujad ning strateegilise kahesuguse kasutusega taristu omanikud, haldajad ja käitajad ning merealuse andmeedastustaristu operaatorid) puhul on peamised mõjud seotud küberturvalisusega seotud turvameetmete rakendamisega, kohustusega teavitada olulise mõjuga küberintsidentidest Riigi Infosüsteemi Ametit, selle üksuse juhatuse liikme

[9] Vt eelmist altviidet.

kohustustega ning Riigi Infosüsteemi Ametile enda andmete esitamisega. Enamike nende nõuete puhul sõltub mõju mitmest asjaolust. Näiteks, kas konkreetne üksus on mõne muu tegevusvaldkonna või teenuse tõttu juba KüTSi kohaldamisalas; kui tegemist on uue üksusega, siis mis on konkreetse üksuse küberturvalisuse nõuete tagamise tase, st kui palju on küberturvalisuse nõuete peale mõeldud ning mida on riskide haldamiseks või küberintsidentide käsitlemiseks ette võetud ning mil viisil on organisatsiooni juhtkond (st ennekõike asjakohane juhatuse liige) on läbinud asjakohaseid koolitusi ning saanud aru, mis on tema roll küberturvalisuse tagamises enda organisatsioonis. Eelduslikult ei oma olulist mõju üksuse andmete esitamine Riigi Infosüsteemi Ametile, mida on võimalik üksuse esindusõiguslikul isikul teha riigiportaalis eesti.ee ettevõtja vaates.[10] Eeltoodud nõuete mõju on eelduslikult sarnane nendele mõjudele, mida on hinnatud NIS2 ülevõtmise käigus, mistõttu neid siin ei korrata.[11]

Ettepanekuga muudetakse käsitlust, millal mingi üksus on NIS2 tähenduses elutähtis üksus, mis on KüTSi tähenduses ülioluline üksus. Kui seni on üliololuliseks üksuseks NIS2 I lisas olev üksus, kes ületab keskmise suurusega ettevõtja ülemmäärasid, siis edaspidi on vastavaks lävendiks need üksused, kes on suuremad kui VKTKEd. Need üksused, kes varem olid üliolulised üksused, on edaspidi olulised üksused. Sellel muudatusel ei ole mõju üksuse põhikohustustele (vt eelmist tekstilõiku), kuid ennekõike selles, kuidas nende üksuste puhul toimub järelevalve korraldus (vt allpool pädevate asutuste mõjude selgitust) ning mis on võimalik rahatrahvi ülemmäär (mida ettepanekuga ei muudeta). Kuna Eestis on siinsete seisukohtade koostamise hetkel KüTSi subjektide nimekiri alles koostamisel, siis ei ole ka võimalik anda hinnangut kui paljusid taolisi üksusi see muudatus mõjutab. Eelduslikult on Eestis väga vähe neid ettevõtjaid, kes on suuremad kui VKTKEd.

Ettepanek näeb ette muudatusi, mida üksuste kohta kogutakse. Võrreldes varasemalt kogutud andmetega on uuteks andmekategooriateks üksuse Euroopa ettevõtluskukru(te) kordumatu(d) tunnus(ed) ja digitaal(ne/sed) aadress(id). Neid andmeid tuleb esitada Riigi Infosüsteemi Ametile siis, kui vastavaid teenuseid kasutatakse. Lisaks muutub ka teatud üksuste (st digitaalse teenuse osutajatel ehk üksused, kes on seotud piiriüleste ja digitaalsete teensutega) puhul tähtaeg, mis aja jooksul peavad nad uuenenud andmetest ametit teavitada. Kui hetkel on nendel üksustel selleks aega kuni kolm kuud, siis edaspidi on selleks aega kuni kaks nädalat (sarnaselt teiste üksustega, kes ei ole digitaalse teenuse osutajad). Selle muudatuse mõju on eelduslikult väike, kuna see sõltub sellest, millised andmed ja millise intervalliga muutuvad. Sellel muudatusel on väiksem mõju nende üksuste puhul, kes osutab mitmeid teenuseid, mille tulemusena on tal senini kohustus andmeid uuendada mõlemata tähtaja jooksul.

Ettepanek näeb ette, et kui komisjon on teinud rakendusakti NIS2 artikli 21 lõike 5 alusel, siis liikmesriigid ei kehtesta nende rakendusaktide kohaldamisalasse kuuluvatele üksustele NIS2 artikli 21 lõikes 2 osutatud meetmetega seoses täiendavaid tehnilisi, metoodilisi ega

[10] Lisainfo: https://ria.ee/kuberturvalisus/riigi-infoturbe-meetmete-haldus/teenuseosutaja-eits-auditi-iso-sertifikaadi-pilvandmetootluse-teade.
[11] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine/

valdkondlikke nõudeid. Hetkel on olemas ainult üks rakendusakt[12] ning sedasorti rakendusaktide (st olemasoleva kui ka tulevaste rakendusaktide) puhul on lähtutud põhimõttest, et üksus rakendab rakendusaktis oleva teenus(t)e puhul rakendusaktis olevaid turvameetmete nõudeid. Muude teenuste puhul tuleb rakendada esmaseid turvameetmeid[13] või teatud juhtudel[14] Eesti infoturbestandardit või selle alternatiivi (rahvusvaheline standard ISO/IEC 27001 või Eesti standard EVS-EN ISO/IEC 27001). Kui lähtuda ettepanekus toodud lahendusest, siis üksus, kes saanus piirduda oma muude teenuste puhul ainult esmaste turvameetmetega peab edaspidi rakendama rakendusaktis olevaid nõudeid ka nende muude teenuste suhtes. See lähenemine võib tõsta nende ettevõtjate halduskoormust – eriti, kui arvestada seda, et seni ei ole tolles rakendusaktis ette nähtud üleminekuaegasid nõuete täitmiseks nii praeguste kui ka uute üksuste korral. Lisaks ei ole selle muudatuse puhul selgus, kuivõrd on liikmesriigil üldse võimalik ette näha muid nõudeid, mis ei ole seotud NIS2 ülevõtmisega, kuid mis on kehtestud muu õigusakti alusel ning nendel nõuetel on ka teatav küberturvalisuse tagamise element või kriteeriumid. Näiteks infosüsteemide infovahetuskihi ehk X-teega seotud nõuded, mis kohalduvad ka neile üksustele, kes on X-teega liidestunud.

Ettepanekuga soovitakse reguleerida, mis teavet lunavara ehk ühe olulise mõjuga küberintsidendi korral tuleks esitada intsidendist teavitamisel või mida pädev asutus saaks täiendavalt küsida teavituse tegijalt. Selle muudatuse mõju jääb hetkel arusaamatuks, kuna praktikas on juba praegu võimalik sama teavet esitada ning pädeval asutusel on võimalik sama teavet ka omaalgatuslikult küsida (kui on saabunud esmane teavitus või intsidenditeade).

Sertifitseerimisega seotud nõuete muudatuste osas (NIS2 artikkel 24 täiendamine) ei ole üksustele olulise mõjuga, kuna senini ei ole Eesti tekitanud volitust nõuda üksuselt konkreetse Euroopa Liidu sertifitseerimiskava alusel sertifikaati. Kui taoline kohustus tekitatakse (nt siinse ettepaneku ülevõtmise käigus või kunagi hiljem), siis on võimalik hinnata sellega seotud mõju. Ettepanek annab üksustele sisuliselt ka võimaluse vabatahtlikult tõendada enda organisatsiooni vastavust NIS2s ette nähtud küberturvalisuse riskijuhtimismeetmetega seotud nõuetele (mille detailid on ette nähtud komisjoni rakendusaktis või liikmesriigi enda õiguses) – saades asjakohase sertifikaadi. Tolle muudatuse mõju ei oma olulist mõju, kuna see sõltub konkreetse üksuse enda soovist vabatahtlikult saada vastav sertifikaat. Üksuste vaatest on ettepanekul teatav positiivne mõju, kuna pädevad asutused ei või kohaldada järelevalvemeetmena sihipärast turvaauditit nende valdkondade või teenuste osas, mis on sertifikaadi käsitlusala.

Mõjud Eesti pädevatele asutustele ning Justiits- ja Digiministeeriumile

VKTKE käsitlus seostamine NIS2 I lisas olevate üksustega ehk NIS2 tähenduses olevate elutähtsate üksustega (KüTSi tähenduse üliohuliste üksustega) seotud muudatused mõjutavad ennekõike Riigi Infosüsteemi Ameti tegevust järelevalvemenetluse kontekstis. Edaspidi peab amet eristama, millal teostatakse nende üksuse suhtes ainult järelkontrolli (vt KüTS § 2 punkti

[12] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1777370813433
[13] Vt Vabariigi Valitsuse 09.12.2022 määruse nr 121 "Võrgu- ja infosüsteemide küberturvalisuse nõuded" § 3 lõige 2^1 ja § 5^1 ning https://eits.ria.ee/et/abimaterjalid/esmased-turvameetmed.
[14] Vt eelnevalt viidatud määruse § 3 lõiget 2^1.

14 ning § 14 lõike 6 punkte 2 ja 3). Samas tuleb arvestada ka asjaoluga, et üks üksus võib osutada mitmeid teenuseid, mistõttu võib ta olla ülioluline üksus ka mõne muu tegevusala või kriteeriumi tõttu - näiteks on tegemist elutähtsa teenuse osutajaga.

Ettepanek näeb ette, et kõikide KüTSi kohaldamisalas olevate üksuste (st ülioluliste üksuste ja oluliste üksuste) kohta käivad andmed tuleb keskse kontaktpunkti (Riigi Infosüsteemi Amet) poolt edastada ENISAle, kes lisab need andmed tema peetavasse registrisse. Ettepanek näeb ette, et ENISA peetavas registris on ka andmed domeeninimede registreerimise teenuse osutajate kohta, kuid nende üksuste andmeid justkui ühtsed kontaktpunktid ei pea edastama. Selle ettepaneku mõju Riigi Infosüsteemi Ameti töökoormusele on keeruline hinnata, kuna see on sõltuvuses sellest, kui tihti üksused enda andmeid muudavad. Selle mõju on ka julgeolekuasutustele (Kaitsepolitseiamet ja Välisluureamet, vt KüTS § 5 lõiget 4), kuid see on tunduvalt väiksem kui on Riigi Infosüsteemi Ametil. Tolle Samas ei ole ettepanekus täpsemalt reguleeritud selle registri pidamisega seotud muud asjaolud: mida ENISA nende andmetega teeb, kes ja millisel õiguslikul alusel saab juurdepääsu registri andmetele, millal andmed kustutatakse jne. Seetõttu on selle registri pidamise mõju keeruline hinnata.

Kehtiv NIS2 näeb ette võimaluse mitme liikmesriigi pädevatel asutustel viia läbi ühismenetlusi ehk nö taotleda järelevalve- ja täitemeetmete teostamisel vastastikust abi. Ettepanekuga antakse ENISAle volitus abistada neid pädevaid üksusi ning volitus analüüsida üliolulisi ja olulisi üksuseid mõjutavate intsidentide võimalike piiriüleste ja siseturule avalduvate tagajärgede ulatust. Selle aruande põhjal võib ENISA: soovitada mitme riigi pädevaid järelevalveasutusi looma ühiseid järelevalve rühmi; koostada suuniseid ühiste järelevalvemeetmete kohta või asjaomaste riikide pädevate asutuste taotluse korral praktilise korra ühiste järelevalvemeetmete võtmiseks; abistada liikmesriike järelevalves (näiteks ise osaleda järelevalves või aidata hinnata konkreetse üksuse küberturvalisuse taset: selleks tuleb esitada kogu teave, sh järelevalve failid ja üksuse enda dokumendid ENISAle). Liikmesriigi kontaktpunkt peab edaspidi teavitama ENISAt, kui vastastikuse abi meedet kasutati kahe riigi vahel, sh anda teada ka millise piiriülese intsidendi tõttu seda tehti. Hetkel on keeruline hinnata, milline on selle muudatuse mõju pädevate asutuste (st ennekõike Riigi Infosüsteemi Ameti) töökoormusele, kuna see sõltub sellest, kas ja kui tihti vastastikuse abi raamistikku kasutatakse.

Ettepaneku kohaselt peavad riigi loodav küberturvalisuse valdkonna strateegia sisaldama ka poliitikameetmeid postkvantkrüptograafiale üleminekuks, võttes arvesse kohaldatavates liidu õigusaktides ja poliitikas sätestatud ülemineku tähtaegu ja asjakohaseid nõudeid. Tolle strateegia koostamine on seotud Justiits- ja Digiministeeriumi tegevusega, kuid see ei oma suurt mõju, kuna kehtiv strateegia juba sisaldab seda teemat.

Mõjud riigieelarvele

Ettepanekus endas on eelarveliste mõjude osas viidatud CSA2 mõjude hinnangule, kuid paraku ei ole tolles analüüsis piisavalt käsitletud NIS2ga seotud muudatusi. Seetõttu on mõju riigieelarvele keeruline hinnata. Teatavas osas leevendub Riigi Infosüsteemi Ameti töökoormus (nt osad üksused muutuvad olulisteks üksusteks ning osad üksused ei ole NIS2 kohaldamisalas), kuid samas lisandub ametile uusi kohustusi (nt kõikide ülioluliste üksuste ja oluliste üksuste

andmete edastamine ENISAle, vastastikuse abi korral teatud andmete edastamine ENISAle), Kui mingil põhjusel on vaja lisaressursse, analüüsitakse seda eelarve planeerimise käigus.

6. Eesti seisukohad

Eesti seisukohad on jaotatud erinevatesse alapeatükkidesse järgmiselt:

- NIS2 muudatuste ja CSA2 üldised põhimõtted ehk seisukohad, mis kohalduvad mõlema õigusakti ettepanekule; järgnevad alapeatükid on konkreetsete temaatikatega seotud seisukohad;
- CSA2 ettepanekuga seotud seisukohad;
- NIS2 muudatuste ettepanekuga seotud seisukohad.

A. NIS2 muudatusi ja CSA2 eelnõusid puudutavad üldised põhimõtted

6.1. Eesti toetab Euroopa Liidu küberturvalisuse tugevdamist, kuid peab oluliseks, et NIS2 muutva ja CSA2 eelnõude nõuded, terminoloogia ja kohaldumisala tagavad liikmesriikidele ja puudutatud subjektidele selge ja üheselt mõistetava õigusraamistiku, kuna juba kehtiva NIS2 sõnastused on ebaselged ja mitmeti tõlgendatavad.

Selgitus:

Euroopa Liidu õigusaktide nõuded ja kohaldumisala on paljuski seotud ka asjaoluga, mis teemade osas on nõuete kehtestamise ainupädevus Euroopa Liidul või liikmesriikidel ning millisel juhul on tegemist jagatud pädevusega. Kavandatavates õigusaktides tuleks selgelt lähtuda või õigusakti enda tekstis välja tuua seisukohast, et kavandatavad regulatsioonid ei puuduta valdkondi, kus Euroopa Liidu aluslepingutest tulenev pädevus puudub ega piira seal täiendavate nõuete kehtestamist. Samuti ei või kavandatavad õigusaktid piirata riikide õigusi valdkondades, kus liikmesriigid võtavad õigusakte vastus Euroopa Liidu toel[15]. Ehk NIS2 ja CSA2 eelnõude lõplikud sõnastused peavad olema kooskõlas aluslepingutest tulenevate pädevustega. Samuti ei tohi need piirata liikmesriikide õigust kehtestada täiendavaid nõudeid nendes valdkondades, mis jäävad liikmesriikide pädevusse või kus Euroopa Liidu üleselt pole valdkondlikke või konkreetseid nõudeid kehtestatud.

Eesti hinnangul on mitmes NIS2-ga seotud artiklis ja teemavaldkonnas endiselt ebaselgust, mis takistab kehtiva direktiivi ühtset ja õiguspärast rakendamist. Seetõttu peab Eesti oluliseks saada Euroopa Komisjonilt täiendavaid selgitusi nii direktiivi kohaldamisala kui ka konkreetsete mõistete ja kohustuste tõlgendamise kohta. Selgitamist vajavad eelkõige küsimused, mis puudutavad sektorite ja teenuste käsitlust, erineva suurusega ettevõtjate tuvastamise metoodikat, üksuse mõiste kohaldumist filiaalidele, hallatud teenuste ja hallatud turbeteenuste ulatust, liikmesriikide osalust kriisihalduse mehhanismides, juhatuse liikmete vastutuse sisu ning sunniraha kohaldamise põhimõtteid. Nende küsimuste lahendamine on vajalik, et tagada

[15] https://commission.europa.eu/about/role/law/areas-eu-action_et

NIS2 muudatuste järjepidev, proportsionaalne ja õigusselge rakendamine kõigis liikmesriikides.

NIS2 muutmise ettepanekuga muudetakse ka lennuettevõtjatega seotud jurisdiktsiooni kui ka seda, millal Euroopa Liidu väline üksus peab Euroopa Liidu territooriumil esindaja määrama. Tegemist on muudatustega, mis suurendavad õigusselgust ja õiguskindlust.

Kuna küberturvalisuse määrus tunnistatakse kehtetuks uue CSA2ga, siis tuleb NIS2s teha ka vastavad muudatused, mis viitavad kehtetuks tunnistatavale määrusele. Siin tuleb direktiivi puhul ennekõike üle vaadata artikkel 6 punktid 3 (küberturvalisus), 10 (küberoht), 11 (IKT-toode), 12 (IKT-teenus) ja 13 (IKT-protsess), artikli 18 lõige 2 (ENISA teeb aruande küberturvalisuse olukorra kohta liidus) ning artikli 24 lõiked 1-3 (seotud Euroopa Liidu sertifitseerimisskeemidega).

6.2. Eesti peab oluliseks, et Euroopa Liidu Küberturvalisuse Ameti (ENISA) rolli ja ülesannete kujundamisel on tagatud selge tööjaotus liikmesriikidega ning välditakse liikmesriikide pädevuste ja olemasolevate mehhanismide dubleerimist (sealhulgas varajase hoiatuse süsteemide, küberintsidentide käsitlemise üksuste ja riiklike operatiivsete funktsioonide osas) ega piirata liikmesriikide pädevate asutuste operatiivtööd. ENISA uued ülesanded peavad toetama kehtivaid koostöömehhanisme, ei tohi luua paralleelseid infovahetuskanaleid ega mõjutada negatiivselt riiklike küberintsidentide käsitlemise üksuste ja erasektori vahelist koostööd.

Selgitus:

ENISA rolli ja ülesannete edasisel kujundamisel tuleb tagada selge ja läbipaistev tööjaotus. See aitab vältida olemasolevate funktsioonide dubleerimist ning tagab, et iga osapool tegutseb oma pädevuse piires võimalikult tõhusalt. Oluline on ka see, et ENISAle uute ülesannete lisandumine toetaks juba toimivaid koostöömehhanisme ning ei mõjutaks negatiivselt küberintsidentide käsitlemise üksuste (CSIRT) ja erasektori vahelist koostööd.

CSA2 näeb ette varajase hoiatuse süsteemi loomist, mis sisaldab teavet oluliste või ulatuslike intsidentide ja piiriüleste küberohtude kohta. Tuleb kindlaks teha, et kavandatav süsteem ei dubleeriks juba olemasolevaid teavitamismehhanisme, näiteks CSIRTide võrgustik ja CERT-EU raamistikus. Samuti on oluline selgitada, kuidas tagatakse teavituste ajakohasus, täpsus ja operatiivsus, arvestades, et ENISA tugineb sageli kaudsetele andmetele. Süsteem hõlmab ka soovituste andmist, millega kaasneb risk, et ENISA soovitused ei ole kohandatud liikmesriikide vajadustega. puudub vahetu ja põhjalik ülevaade Eesti küberruumis toimuvast ning soovitused ei pruugi seetõttu olla täielikult kohandatud Eesti vajadustele. Samuti tuleb vältida olukorda, kus riiklik CSIRT ei ole piisavalt kaasatud olulisse infovahetusse ega suhtlusesse asjaomaste üksustega.

Lisaks näeb määrus ette lunavara intsidentidele reageerimiseks operatiivtoe pakkumist läbi kasutajatoe loomise, mis tõstatab küsimuse võimaliku kattuvuse kohta riiklike CSIRTide tegevusega. Sellega seoses on oluline selgitada, kuidas on kavandatud operatiivse toe koordineerimine ning millised on infovahetuse mehhanismid. Ilma selgete protseduurideta võib tekkida olukord, kus oluline teave ei jõua riikliku CSIRTini või kus asjaomased üksused saavad

paralleelselt erinevaid suuniseid riiklikult ja ENISA tasandilt. Samuti vajab täpsustamist, kuidas tagatakse pakutava toe kvaliteet, arvestades, et detailne ja kontekstipõhine teadmus paikneb eeskätt riiklikul tasandil.

NIS2 muudatuste ettepanekuga on edaspidiselt ENISA NIS2 artikli 15 alusel moodustatud küberintsidentide käsitlemise riiklike üksuste võrgustiku ehk CSIRTide võrgustiku liige. Hetkel on tal samas võrgustikuga seos sekretariaaditeenuse osutamise ja toetava rollina. NIS2 muutvas direktiivi ettepanekus ei ole määratletud, mida see endaga kaasa toob, st millised on sel juhul ENISA tulevased ülesanded.

Ettepanekuga luuakse ka NIS2 artikkel 37a, mis annab ENISAle ülesande abistada liikmesriike vastastikuse abi osutamisel ning analüüsida piiriüleseid küberriske. Analüüsi põhjal koostatakse iga-aastane piiriülese küberriski hindamise aruanne, mille alusel võib ENISA teha soovitusi ühiste kontrollrühmade moodustamiseks, järelevalvemeetmete ühtlustamiseks või aidata hinnata üksuste vastavust NIS2 artikli 21 nõuetele. Samuti peavad liikmesriigid teavitama ENISAt vastastikuse abi kasutamisest.

Eesti seisukohtade koostamise ajal ei ole veel toimunud arutelusid NIS2 muutva direktiivi ettepaneku osas, mistõttu ei ole veel olnud võimalik selgeks teha, mis on lisanduvate sätete lisandväärtus ja otsene vajadus. Siiski ei tohi ENISA ülesanded dubleerida liikmesriikide, st pädevate asutuste tegevust.

B. CSA2 eelnõu puudutavad seisukohad

6.3. Eesti peab oluliseks, et liikmesriikidele säilib otsustuspädevus ENISA kontaktisikute määramisel ning võimalus otsustada, millises ulatuses ja millise esindatusega nad ENISA töös osalevad. Juhul kui liikmesriikidel tuleb nimetada esindaja ENISA koostööformaati või nõukogusse, peab neile säilima piisav paindlikkus otsustada, millisest asutusest pädev esindaja määrata. Oluline on vältida väikeriikidele liigse töökoormuse tekkimist.

Selgitus:

Liikmesriikide ressursid on piiratud ning seetõttu on oluline tagada, et need oleksid suunatud eelkõige sisuliste eesmärkide saavutamisele, sealhulgas küberturvalisuse tegelikule tugevdamisele, vältides samal ajal ebaproportsionaalselt koormavaid kohustusi. Sama põhimõte peab kehtima ka ekspertide kaasamisel. Kontaktametnike ülesanded, vastutus, töökorraldus ja oodatav panus peavad olema selgelt määratletud ning nende lähetamine peab andma selget lisaväärtust.

Üldine nõue määrata kindel arv kontaktametnikke võib osutuda ebaproportsionaalseks, eriti väiksema haldus- ja eksperdivõimekusega riikide jaoks. Samuti võib tekkida olukord, kus määratud isikute pädevus ei vasta ENISA tegelikele vajadustele, arvestades, et tehnilised eksperdid on liikmesriikides piiratud ressurss. Paindlik lähenemine, mis võimaldab liikmesriikidel lähtuda oma tegelikest võimalustest ja ENISA praktilistest vajadustest, oleks seetõttu otstarbekam.

Samuti arvame, et kahe kontaktametniku määramise nõue on väikeriikidele ebaproportsionaalselt ressursimahukas.

Lisaks, liikmesriikide halduskorraldus ei ole ühesugune ning seetõttu ei pruugi ühetaoline lähenemine esindajate määramisele olla alati põhjendatud ega praktiliselt toimiv. Paindlikkus võimaldab igal liikmesriigil määrata esindaja sellest asutusest, kus asjakohane pädevus ja vastutus tegelikult paikneb, aidates seeläbi tagada nii sisuliselt tugevama panuse kui ka tõhusama töökorralduse.

Mitmes liikmesriigis on küberturvalisuse valdkonna vastutused ja pädevused jaotatud mitme asutuse vahel ning kõige asjakohasem ekspertiis ENISA haldusnõukogu või kontaktametniku töös osalemiseks ei pruugi alati paikneda nimetatud asutuses Seetõttu peame oluliseks, et liikmesriikidele jääks paindlikkus määrata haldusnõukogusse ja kontaktametnikuks esindaja, kes kõige paremini vastab riigi vajadustele ja omab vajalikku sisulist pädevust.

6.4. Eesti toetab küberturvalisuse atesteerimisskeemi ja küberoskuste akadeemia loomist ning nendega seotud ülesannete andmist ENISAle, kuid peab oluliseks vältida liikmesriikide õppeasutustele lisanduvat halduskoormust. Loodavad atesteerimisskeemid peavad arvestama olemasolevaid kompetentsimudeleid ja sertifikaate. Kaasnevad lisakulud ja -ülesanded peavad olema põhjendatud ning arvestama liikmesriikide olemasolevate õppekavade mahtu ja korraldust. Kompetentsiprofiilide välja töötamisel peab arvestama ka Euroopa Liidu tööturu olukorra ning juba kasutusel olevate rahvusvaheliste sertifikaatidega.

Selgitus:

Atesteerimine on ette nähtud liikmesriikide riiklike atesteerimisasutuste eestvedamisel, atesteerimisasutused peavad ENISAle mandaadi saamiseks tasu alusel luba taotlema. Sealjuures pole asutuste puhul kehtestatud nõudeid või profiile ning atesteerimine toimub vabatahtlikkuse alusel. Määrusega EL-üleselt loodavad kompetentsiprofiilid ei peaks dubleerima eksisteerivaid küberturvalisuse valdkonna sertifikaate. Oskuste akadeemia ja atesteerimisskeem loovad selgema aluse küberturvalisuse valdkonna atesteerimiseks.

Kaasnev mõju õppeasutustele ja lisanduv halduskoormus peavad olema kooskõlas eksisteerivate õppekavadega. Oskuste akadeemia loob täiendavad võimalused atesteerimiseks, ent täiendavad kulud ja halduskoormus pole praeguseks määratletud kuna spetsiifilised kompetentsiprofiilid ja atesteerimisskeemid pole veel piiritletud. Eeldatavalt toob atesteerimisskeemide loomine kaasa täiendava vajaduse õppekavade ja õpiväljundite täpsustamiseks IKT hariduses.

Loodav atesteerimisskeem peab arvestama tööturu ja küberturvalisuse valdkonna muutlikkusega, arvestades sealjuures uute tehnoloogiate kasutuselevõttu. ENISA peab atesteerimisskeeme vajadusel uuendama, hoides sealjuures kõrget standardit ning arvestades uute tehnoloogiate kasutuselevõttu. Ühtne Euroopa Liidu ülene standard ja atesteerimisskeem peaks võimaldama ka riikide-ülest atesteerimist, loomaks ühtset baasi ja arusaama küberturvalisuse valdkonna kompetentsiprofiilidest.

6.5. Eesti toetab eelnõu ettepanekut, mille kohaselt jääb küberturvalisuse sertifitseerimine IKT-toodete, -teenuste ja -protsesside pakkujatele vabatahtlikuks ning küberturvalisuse sertifitseerimisskeemid ei raskenda mikro- ja väikeettevõtete ja uute ettevõtete turule tulemist ja turul tegutsemist. Oluline on tagada, et sertifitseerimisega seotud nõuded ei too ettevõtetele kaasa põhjendamatut haldus- ega kulukoormust, kuna ka vabatahtlik sertifitseerimine võib praktikas muutuda turul osalemise, hanketingimustele vastamise või klientide usalduse saavutamise eeltingimuseks.

Selgitus:

Kohustusliku sertifitseerimise kehtestamine võib kaasa tuua märkimisväärse haldus- ja kulukoormuse ning piirata innovatsiooni, eriti väiksemate ettevõtjate puhul. Vabatahtlik mudel võimaldab kasutada sertifitseerimist sihipärase ja riskipõhise vahendina juhtudel, kus selleks on selge praktiline vajadus või turupõhine põhjendus. Nii saab sertifitseerimine täita oma peamist eesmärki, mis on usalduse suurendamine IKT-lahenduste turvalisuse osas ning pakkuda ettevõtjatele võimalust tõendada nõuetele vastavust seal, kus see on asjakohane. Kui sertifitseerimisega kaasnev halduskoormus, ajakulu või rahaline kulu kujuneb liiga suureks, võib see pärssida uute ja innovaatiliste toodete ning teenuste arendamist ja turule toomist, vähendada konkurentsi ning tugevdada ebaproportsionaalselt juba turul tegutsevate suuremate osalejate positsiooni.

Tuleb arvestada, et ka vabatahtlik sertifitseerimine võib praktikas omandada ettevõtjate jaoks vältimatu iseloomu, eelkõige juhul, kui sellest kujuneb turul osalemise, hanketingimustele vastamise või klientide usalduse saavutamise eeltingimus. Seetõttu on oluline vältida olukorda, kus vabatahtlikuna kavandatud raamistik muutub sisuliselt kohustuslikuks ning toob ettevõtjatele kaasa põhjendamatu haldus- ja kulukoormuse.

6.6. Eesti peab oluliseks, et liikmesriikidele jääks piisav õigus võimaldada põhjendatud juhtudel kontrollida küberturvalisuse sertifikaadi aluseks olevate nõuete tegelikku täitmist. Samuti peab olema liikmesriigil võimalik nõuda sertifikaadi omanikult täiendavate nõuete täitmist juhul, kui sertifikaat ei kata kogu vajalikku riskispektrit või ei anna piisavat kindlust kõigi asjakohaste nõuete täitmise kohta (näiteks julgeoleku valdkond).

Selgitus:

Tuleb arvestada, et keskselt väljatöötatud sertifitseerimisskeemid ei pruugi alati täiel määral peegeldada kiiresti muutuvat ohupilti ning nende nõuded põhinevad sageli erinevate lähenemiste vahel saavutatud kompromissidel. Arvestades liikmesriikide erinevat küberturvalisuse taset ja vajadusi, ei ole põhjendatud näha ette kohustust selliseid sertifikaate tingimusteta aktsepteerida. Oluline on säilitada liikmesriikidele võimalus põhjendatud juhtudel nõuetele vastavust täiendavalt hinnata või auditeerida.

Lisaks võib sertifikaadi tingimusteta ja täiendava kontrollita aktsepteerimise kohustus tekitada küsimusi seoses liikmesriikide pädevusega julgeolekuvaldkonnas. Selline lähenemine võib piirata liikmesriikide võimalusi võtta arvesse konkreetseid riiklikke julgeolekukaalutlusi,

sealhulgas vajadust teatud tehnoloogiaid täiendavalt hinnata või põhjendatud juhtudel nende kasutamist piirata

6.7. Eesti peab oluliseks, et IKT tarneahelate turvalisuse tagamisel pööratakse tähelepanu ka mittetehniliste riskide maandamisele, kuid selleks eelnõus kavandatavad meetmed peavad olema proportsionaalsed ja sihitud. Küberturvalisuse seisukohast muret tekitavate kolmandate riikide kindlaksmääramisel peab liikmesriikidel olema tugev roll, et tagada mittetehniliste riskide määratlemise protsessi läbipaistvus ja usaldusväärsus.

Selgitus:

Mittetehniliste riskidega tegelemine on IKT tarneahelate turvalisuse tagamisel oluline. Selliste riskide hindamisel ja maandamisel on tähtis, et kasutatavad meetmed oleksid läbimõeldud, proportsionaalsed, paindlikud ning kohandatud tegelikele vajadustele ja riskitasemele. See aitab tagada, et turvalisuse tugevdamine ei tooks kaasa liigset halduskoormust, põhjendamatuid piiranguid ega lahendusi, mis ei ole konkreetse olukorra seisukohast vajalikud või tõhusad.

Mittetehniliste riskide maandamise raamistik peab võimaldama arvestada nii tehnoloogilise keskkonna, turuolukorra kui ka liikmesriikide julgeoleku- ja halduseripäradega. Seetõttu on oluline suurendada liikmesriikide rolli otsustusprotsessis. Liikmesriikide varajane ja sisuline kaasamine võimaldab teha paremini informeeritud otsuseid.

Komisjoni ja liikmesriikide rollid peavad olema kogu protsessi vältel selgelt määratletud, et liikmesriikidel oleks sisulisem ja mõjusam roll otsuste ettevalmistamisel ja kujundamisel. Arvestades, et rakendamine toimub suures osas liikmesriikide tasandil ning mõju avaldub otseselt nende asutustele ja turuosalistele on põhjendatud, et liikmesriigid oleksid protsessis varakult ja sisuliselt kaasatud.

6.8. Eesti peab oluliseks, et liikmesriikide ja ettevõtjate jaoks on eelnõus IKT tarneahelate mittetehniliste riskide maandamise protsessid sätestatud selgelt, läbipaistvalt ja etteaimatavalt. CSA2 eelnõus või selle alusel kehtestatavates rakendusaktides tuleb ette näha mõistlikud üleminekuajad vastavalt IKT tarneahelate riskihinnangutele, et liikmeriigid ja ettevõtjad saaksid oma IKT tarneahelatega seotud protsessid, tooted ja investeeringud uute küberturvalisuse nõuetega kooskõlla viia.

Selgitus:

On oluline, et liikmesriikide ja ettevõtjate jaoks oleksid eelnõus IKT tarneahelate mittetehniliste riskide maandamise protsessid selged, läbipaistvad ja etteaimatavad, võimaldades neil oma tegevusi ja investeeringuid aegsasti kavandada. Kui protsessid, tähtajad, nõuded või hindamiskriteeriumid ei ole liikmesriikidele ja ettevõtjatele piisavalt selged või muutuvad ootamatult, võib see raskendada strateegilist planeerimist, suurendada kulusid ning pidurdada nii vastavusmeetmete rakendamist kui ka uute toodete ja teenuste turule toomist. Osalistel peab olema võimalik aegsasti aru saada, millised kohustused neile kohalduvad, millal need jõustuvad, milliseid samme tuleb vastavuse tagamiseks astuda ning millised võivad olla võimalike muudatuste praktilised mõjud.

Seetõttu on oluline, et mittetehniliste riskide määramise protsess ja nõuded oleksid hästi põhjendatud ja praktiliselt rakendatavad. Siinsete seisukohtade koostamise hetkel on keeruline välja pakkuda, mis on mõistlikud üleminekutähtajad, kuna see sõltub paljuski sellest, mis valdkonna tehnoloogia ja nendega seotud komponentide osas võidakse neid nõudeid ette näha, st kuivõrd sügavale tarneahelate riskihinnangutega minnakse. Samuti on oluline kaasata tööstust ja teisi osalisi varases etapis, et võimalikud probleemkohad oleks aegsasti tuvastatavad ning vältida lahendusi, mis tekitavad põhjendamatuid ootamatusi või ebaproportsionaalset koormust.

C. NIS2 muudatuste ettepanekuga seotud seisukohad

6.9. Eesti toetab Euroopa digiidentiteedikukrute pakkujate ja Euroopa ettevõtluskukrute pakkujate ning strateegilise kahesuguse kasutusega taristu omanike, haldajate ja käitajatena kindlaks määratud üksuste kui ka merealuse andmeedastustaristu operaatorite lisandumist NIS2 kohaldamisalasse. Eesti toetab mikro- ja väikeettevõtjatest domeeninimede süsteemi teenuse osutajate välja jätmist NIS2 kohaldamisalast.

Selgitus:

Euroopa digiidentiteedikukrute ja Euroopa ettevõtluskukrute pakkujad on üks osa Euroopa ülesest digiidentiteedi valdkonnast, mistõttu on kohane nende lisamine ka NIS2 kohaldamisalasse, olenemata nende suurusest.

Strateegilise kahesuguse kasutusega taristu omanike, haldajad ja käitajate lisamine NIS2 kohaldumisalasse on kooskõlas eesmärgiga tugevdada kriitilise taristu kaitset ning toetab ka Eesti varasemat väljendatud seisukohta, et sõjalistel eesmärkidel varustuse, kaupade ja personali transporti osas tuleb minimeerides selle mõju tsiviiltranspordile.

Merealuse andmeedastustaristu operaatorid hõlmatakse NIS2 kohaldamisalasse, kuna seda võivad käitada üksused, kes on juba direktiivi kohaldamisalas, näiteks üldkasutatava elektroonilise side võrkude või -teenuste osutajad või pilvandmetöötlusteenuse osutajad, kuid neid võivad käitada ka muud üksused, mis ei kuulu veel NIS2 kohaldamisalasse mõne muu teenuse või tegevusala tõttu.

Eelnimetatud Eesti üksustele tähendab see muudatus, et nad peavad rakendama küberturvalisuse seadust ja selle nõudeid. Nendeks nõueteks on ennekõike kohustus määrata juhtorgani liige, kes tegeleb küberturvalisuse teemadega; nad peavad enda andmed esitama Riigi Infosüsteemi Ametile; samuti peavad tegelema turvameetmete rakendamisega ning olulise mõjuga küberintsidendi korral teavitama sellest juhtumist Riigi Infosüsteemi Ametit.

Hetkel on kõik domeeninimede süsteemi teenuse osutajad NIS2 kohaldamisalas. Ettepaneku muudatuste tulemusena ei ole enam NIS2 kohaldamisalas selliste teenuste osutajad, kes on mikro- või väikeettevõtjad, arvestades komisjoni soovitust 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratluse kohta. Samuti on need direktiivi kohaldamisalas olevad üksused edaspidi elutähtsate üksuste küberturvalisuse seaduse tähenduses ülioluliste

üksuste asemel olulised üksused. Ettepaneku ajendiks on soov vähendada ettevõtjate halduskulusid kokku 25 % ning väikeste ja keskmise suurusega ettevõtjate puhul 35 %.

6.10. Eesti toetab NIS2 tähenduses elutähtsate üksustega seotud lävendi muudatust, mille kohaselt käsitatakse edaspidi elutähtsate üksustena NIS2 I lisas osutatud ettevõtjaid, kes ületavad väikese keskmise turukapitalisatsiooniga ettevõtjate (VKTKE) ülemmäärasid.

Selgitus:

Ettepaneku kohaselt muudetakse NIS2 artikli 3 lõike 1 punkti a nii, et direktiivi tähenduses elutähtsate üksuste (inglise k *"essential entity"*; küberturvalisuse seaduse tähenduses üliolulised üksused[16]) hulgas on NIS2 I lisas olevad üksused, kes ületavad väikeste keskmise turukapitalisatsiooniga ettevõtja ehk VKTKEde[17] ülemmäärasid. NIS2 I lisas olevad üksused, kes varasemalt oli suuremad kui väikese ja keskmise suurusega ettevõtjad[18], kuid kes on väiksemad kui VKTKE ülemmäärad, on edaspidi olulised üksused (inglise k "important entity"; küberturvalisuse seaduses[19] samuti olulised üksused) – st nende puhul muutub järelevalve korraldus (see on edaspidi järelkontrollina) kui ka võimalike trahvide ülemmäärad. See siiski ei muuda NIS2ga ette nähtud peamisi kohustusi: ennekõike näiteks riskijuhtimismeetmete (küberturvalisuse seaduse tähenduses turvameetmete) rakendamise kohustust, olulise mõjuga küberintsidentidest teavitamise kohustust kui ka juhtorgani liikmega seotud kohustusi.

Direktiivi ettepanek ei muuda NIS2 artikli 3 lõike 1 punkte c–h, kuid täpsustab punkti b, lisades elutähtsate üksustena Euroopa digiidentiteedikurkute pakkujad ja Euroopa ettevõtluskukrute pakkujad ning eemaldades domeeninimede süsteemi teenuse osutajad. Punkti h lisatakse strateegilise kahesuguse kasutusega taristu omanikud, haldajad ja käitajad. Need üksused (v.a. domeeninimede süsteemi teenuse osutajad) on edaspidi NIS2 tähenduses elutähtsad üksused ning küberturvalisuse seaduse tähenduses üliolulised üksused olenemata nende suurusest. Domeeninimede süsteemi teenuse osutajad on edaspidi NIS2 tähenduses olulised üksused ning küberturvalisuse seaduse tähenduses olulised üksused.

Eesti toetab muudatusi, kuid peab vajalikuks täiendavat selgust tagajärgedest. Eelkõige tuleb selgelt määratleda, kuidas pädevad asutused teostavad järelevalvet nende üksuste osas, kes muutuvad olulisteks üksusteks – eriti siis, kui nad on NIS2 tähenduses elutähtsad üksused (KüTSi tähenduses üliolulised üksused) mõne muu kriteeriumi tõttu: näiteks on nad Eesti õigusaktide tähenduses elutähtsa teenuse osutajad. NIS2 näeb ette, et elutähtsate üksuste puhul on võimalik teha nii ennetavata kui ka järelkontrolli, see tähendab vastavalt *ex nunc* ja *ex post* järelevalvet, kuid oluliste üksuste puhul on võimalik teha ainult järelkontrolli.

[16] Vt võrdluseks küberturvalisuse seaduse § 3 lõikeid 2 ja 3, st ennekõike lõiget 3.
[17] Väikeste keskmise turukapitalisatsiooniga ettevõtjate kategooriasse kuuluvad ettevõtjad, kes ei ole väikesed ja keskmise suurusega ettevõtjad soovituse 2003/361/EÜ järgi, kellel on vähem kui 750 töötajat ja kelle aastakäive ei ületa 150 miljonit eurot või aastabilansi kogumaht ei ületa 129 miljonit eurot.
https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32025H1099, lisa punkt 2.
[18] Mikro-, väikeste ja keskmise suurusega ettevõtete (VKEd) kategooriasse kuuluvad ettevõtted, millel on vähem kui 250 töötajat ja mille aastakäive ei ületa 50 miljonit eurot ja/või aastabilansi kogumaht ei ületa 43 miljonit eurot.
[19] Vt võrdluseks küberturvalisuse seaduse § 3 lõikeid 4 ja 5, st ennekõike lõike 4 punkti 8.

Seetõttu on vaja saada selgust, kuidas eristada *ex nunc* ja *ex post* järelevalvet olukorras, kui üks üksus on ühe tegevuse tõttu NIS2 mõttes ülioluline üksus ja teise tegevuse tõttu oluline üksus.

6.11. Eesti leiab, et elutähtsad üksused, olulised üksused ja domeeninimede registreerimise teenuse osutajad peavad esitama liikmesriigi pädevatele asutustele enda kohta käivat teavet üksnes mahus, mis on eesmägipärane ja vajalik pädevate asutuste ülesannete täitmiseks. Samuti peaksid pädevad asutused edastama samadest andmetest ENISAle üksnes need andmed, mis on eesmärgipärased ja vajalikud ameti ülesannete täitmiseks. ENISA peetavat eelnimetatud üksuste registrit puudutavad nõuded tuleb eelnõus täpsemalt reguleerida, tagades muu hulgas selguse registri pidamises, sellele juurdepääsus, registri ja selles sisalduvate andmete kaitses, andmete säilitamistähtaegades kui ka muudes asjakohastes korralduslikes aspektides.

Selgitus:

NIS2 kohaselt peavad elutähtsad üksused, olulised üksused ja domeeninimede registreerimise teenuse osutajad esitama pädevatele asutustele teatud andmed, mis on vajalikud järelevalve ja muude ülesannete täitmiseks. Ettepaneku tulemusena koondatakse need andmekoosseisud NIS2 artikli 3 lõikesse 4 ning lisatakse täiendavad andmed, nagu Euroopa ettevõtluskukru kordumatu tunnus ja digiaadressid.

Eesti jaoks on oluline, et üksustelt kogutavad andmed oleksid eesmärgipärased ja proportsionaalsed ning et pädevad asutused edastaksid ENISAle ainult need andmed, mis on ameti ülesannete täitmiseks vältimatult vajalikud. Praegu ei ole selge, miks on vaja edastada kõikide üksuste andmed ENISAle ega millisel viisil ENISA neid andmeid kasutab. Need küsimused tuleb arutelude käigus selgeks teha. Eesti seisukohtade koostamise ajal ei ole veel toimunud arutelusid NIS2 muutva direktiivi ettepaneku osas, mistõttu ei ole veel olnud võimalik selgeks teha, mida tähendaks eelmainitud muudatus liikmesriikidele ning mis on minimaalne andmekoosseis, mida liikmesriikide pädevatel asutustel kui ka ENISAl on enda töö jaoks vaja.

Samuti vajab täpsustamist, milliseid IP-aadresse (sh IP-vahemikke) üksustelt oodatakse. Kui nõue hõlmaks ka dünaamilisi IP-aadresse, oleks see ebaproportsionaalselt koormav ning ei annaks pädevatele asutustele sisulist lisaväärtust. Seetõttu tuleb selgitada, millist eesmärki IP-aadresside kogumine teenib ja kuidas pädevad asutused neid andmeid kasutavad.

Kuna ENISA hakkab pidama registrit kõikide elutähtsate üksuste, oluliste üksuste ja domeeninimede registreerimise teenuse osutajate kohta, tuleb tagada, et registri pidamine vastaks nt Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 artikli 4 põhimõtetele. See hõlmab selgust registri pidamise korra, juurdepääsuõiguste, andmete kaitse, säilitamistähtaegade ja muude korralduslike aspektide osas. Arvestada tuleb ka seda, et registris võivad sisalduda füüsiliste isikute andmed (nt kontaktisikud või esindajad), mis nõuab täiendavat tähelepanu andmekaitsele.

Eestis on vastavad üksuste nimekirjad käsitletud asutusesisese teabena, mistõttu tuleb arutelude käigus tagada, et ENISA registri lahendus oleks kooskõlas riiklike andmekaitse- ja juurdepääsupiirangutega.

6.12. Eesti toetab muudatust, mille kohaselt peavad liikmesriigid enda küberturvalisuse strateegia osana võtma vastu postkvantkrüptograafiale üleminekuga seotud poliitikameetmeid.

Selgitus:

NIS2 muutva direktiivi ettepaneku tulemusena täiendatakse NIS2 artikli 7 (riiklik küberturvalisuse strateegia) lõiget 2 (*Riikliku küberturvalisuse strateegia osana võtavad liikmesriigid vastu eelkõige poliitikameetmed,*) punktiga k järgmises sõnastuses *postkvantkrüptograafiale üleminekuks, võttes arvesse kohaldatavates liidu õigusaktides ja poliitikas sätestatud ülemineku tähtaegu ja asjakohaseid nõudeid*.

Eesti koostatud küberturvalisuse strateegia üheks osaks on postkvantkrüptograafiaga seotud teemad, mistõttu saame seda lisandust toetada. Euroopa Komisjon on avaldanud teekaardi[20] postkvantkrüptograafiale üleminekuks, millega on arvestatud Eesti postkvant-krüptograafia ülemineku riikliku teekaardi[21] koostamisel.

6.13. Eesti toetab eelnõus küberturvalisuse riskijuhtimismeetmete tagamisega seotud nõuete sõnastamist viisil, mis võimaldab liikmesriigil kehtestada riigispetsiifilisi riskijuhtimismeetmete nõudeid ka nende üksuste suhtes, kes on hõlmatud Euroopa Komisjoni samade nõuete alusel vastu võetud rakendusaktiga.

Selgitus:

NIS2 muutva direktiivi ettepaneku tulemusena täiendatakse NIS2 artikli 21 (küberturvalisuse riskijuhtimismeetmed) lõiget 5:

- üks muudatus on seotud sellega, et komisjonile antakse ülesanne siseturu toimimise parandamise eesmärgil regulaarselt hinnata, kas selle artikliga seotud meetmete osas on vaja koostada konkreetsete sektorite või üksuste liikide kohta rakendusakte; kui selliseid rakendusakte on vaja, siis viiakse läbi kõiki huvitatud osapooli kaasav konsultatsiooniprotsess;
- teise muudatusega soovitakse teha nõue, et kui komisjon koostab sama lõike esimeses ja teises lõigus osutatud rakendusaktid, siis liikmesriigid ei kehtesta "nende rakendusaktide kohaldamisalasse kuuluvatele üksustele NIS2 artikli 21 lõikes 2 osutatud meetmetega seoses täiendavaid tehnilisi, metoodilisi ega valdkondlikke nõudeid".

Eesti seisukohtade koostamise ajal ei ole veel toimunud arutelusid NIS2 muutva direktiivi ettepaneku osas, mistõttu ei ole veel olnud võimalik selgeks teha, mida tähendaks eelmainitud muudatus liikmesriikidele. Näiteks, kas ettepanekus toodud sõnastus kohalduks rakendusaktis mainitud üksusele ka siis, kui konkreetse ettevõtja puhul on märgitud ainult üks teenus, kuid praktikas on ta veel muude teenuste (nt 4-5 tk) alusel NIS2 kohaldamisalas. Kui vastus on

[20] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography
[21] https://www.justdigi.ee/digi-side-ja-kuber/analuusid-ja-uuringud, täpsemalt 2026_ROAD2PQ_final_report__avalik_v1.0.pdf

jaatav, siis tekib küsimus, kuidas näiteks side valdkonnas suhestub see lähenemine nendesse õigusnormidesse, millega 5G turvalisuse tööriistakast on üle võetud (mis on samuti mõeldud tarneahela turvalisuse tagamise nõuetena). Samuti on vaja saada selgust, kuidas siinne muudatus suhestub CSA2 ettepaneku artikkel 98 ([Usaldusväärse IKT tarneahela raamistiku] kohaldamisala) lõikega 2: *Käesolevas jaotises sätestatud kohustused ei piira kohustusi mis on sätestatud määruse (EL) 2024/2847 artiklis 13 ning riiklikes sätetes, millega võetakse üle direktiivi (EL) 2022/2555 artikkel 21.*

Sellest hoolimata leiab Eesti, et liikmesriikidel peab jääma võimalus kehtestada NIS2 artikli 21 lõike 5 alusel vastu võetud rakendusaktide kohaldamisalasse jäävate üksuste suhtes ka täiendavaid tehnilisi, metoodilisi või valdkondlikke nõudeid. Eesti on kehtestanud teiste õigusaktide alusel kui KüTS teatud nõudeid ja tingimusi, millede kohaldumine tekitab küsitavusi, kui NIS2 artikli 21 lõike 5 sõnastuse tulemiks on nii nagu on direktiivi ettepanekus sõnastatud. Näiteks on üheks Eesti digiriigi keskseks komponendiks infosüsteemide andmevahetuskiht ehk X-tee, mille kasutamiseks on ette nähtud teatavad tingimused (st ka turvameetmed).[22] Kui kõnealuse lõik 5 sõnastuseks on nii nagu on direktiivi ettepaneku sõnastus, siis arvestatav osa Eesti digiühiskonnaga seotud üksuste puhul (kelle suhtes on juba kehtestatud rakendusmäärus[23] (EL) 2024/2690) muutub ebaselgeks, kuivõrd neile on üldse võimalik X-tee kasutamisega seotud nõudeid kehtestada. Seetõttu peab liikmesriikidel olema jätkuvalt võimalik taolisi nõudeid kehtestada või ette näha.

6.14. Eesti leiab, et NIS2 nõuete ning selle alusel antavate rakendusaktide täitmiseks peavad olema ette nähtud konkreetsed üleminekuperioodid, kuna üleminekuperioode ei ole sätestatud kehtivas NIS2s ega selle alusel antud rakendusaktis ning neid pole ka ette nähtud NIS2 muutvas eelnõus. See on eriti oluline üksuste puhul, kes satuvad esmakordselt NIS2 või selle alusel antud rakendusakti kohaldamisalasse. Üleminekuperioodid peavad olema sobilikud konkreetsete nõuete olemuse ja keerukusega, näiteks võiks küberturvalisuse riskijuhtimismeetmetega seotud nõuete rakendamise puhul kuni kolm aastat.

Selgitus:

NIS2 ülevõtmise käigus ilmnes, et direktiiv ega selle rakendusmäärus (EL) 2024/2690 ei sätesta tähtaegu, mille jooksul peavad üksused täitma neile kehtestatud kohustused. Sama probleem tekib ka uute rakendusaktide puhul, eelkõige artikli 21 lõike 5 alusel antavate nõuete rakendamisel. Selgusetus puudutab nii andmete esitamise tähtaegu, riskijuhtimismeetmete rakendamise ajaraame, esindaja määramise kohustuse jõustumist kui ka intsidentidest teavitamise kohustuse rakendumist.

Tähtajad on olulised nii üksustele, kes juba kuuluvad NIS2 kohaldamisalasse, kui ka neile, kes lisanduvad direktiivi muutmise tulemusena või satuvad kohaldamisalasse uue tegevuse alustamise tõttu. Ilma selgete üleminekuperioodideta ei ole võimalik tagada nõuete ühtset, proportsionaalset ja realistlikku rakendamist.

[22] https://www.riigiteataja.ee/akt/106082019017
[23] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1776514494611

Samad probleemkohad tekivad nii nende üksuste suhtes, kes on tulevikus kehtiva NIS2 kohaldamisalas (näiteks kes hakkavad pakkuma usaldusteenust või saavad Eesti õigusaktide tähenduses elutähtsa teenuse osutajateks) kui ka nende üksuste puhul, kes lisanduvad siinse ettepaneku tulemusena.

Üleminekuperioodid peavad olema selged, konkreetsed, ettenähtavad ehk kokkuvõtlikult sobilikud, arvestades konkreetse kohustuse olemust. Seetõttu on ka siinsete seisukohtade koostamise käigus keeruline ette näha, mis oleksid sobilikud üleminekuperioodid - seetõttu on seisukohas esitatud näitena, et küberturvalisuse riskijuhtimisega seotud nõuete puhul võiks see olla kuni kolm aastat. Sarnane üleminekuperiood on ette nähtud ka küberturvalisuse seaduses turvameemete (NIS2 tähenduses küberturvalisuse riskijuhtimisega seotud nõuete) rakendamise kontekstis nendele üksustele, kes peavad selle seaduse nõudeid esmakordselt täitma pärast 01.01.2026. a.

6.15. Eesti leiab, et liikmesriigi pädevale asutusele NIS2 tähenduses olulisest intsidendist teavitamine peab toimuma nii, et varajase hoiatusega esitatakse kogu teave, mis on teavitamise hetkel teada. Järgnevad teavitused, sealhulgas intsidenditeade ja vahearuanne, peavad täiendama ja ajakohastama varajase hoiatusega esitatud teavet. Varajase hoiatuse andmekoosseis peab tagama piisava paindlikkuse teavitajale, kuid samal ajal võimaldama pädeval asutusel täita oma ülesandeid ning andma teavitavale üksusele aluse koostada lõpparuanne lahendatud intsidendist. Teavitustega seotud andmeväljad peavad võimaldama tagada ka teiste Euroopa Liidu õigusaktide alusel sama intsidendi kohta esitatavate teavituste kohustuste täitmist.

Selgitus:

NIS2 artikli 23 lõikes 4 on sätestatud varajase hoiatuse, intsidenditeate, vahearuande ja lõpparuande esitamise tähtajad ning nende üldine sisu. Praktikas ei anna varajase hoiatuse miinimumnõuded pädevale asutusele piisavat ülevaadet toimunud intsidendist, kuna need ei sisalda teavet selle kohta, mis juhtus, millal intsident aset leidis ega milline teave on teavitamise hetkel teada. Selline andmekoosseis ei võimalda pädeval asutusel oma ülesandeid tõhusalt täita.

NIS2 ülevõtmise käigus kujunes Eestis arusaam, et varajane hoiatus peab sisaldama kogu teavet, mis on teavitamise hetkel teada, sealhulgas neid elemente, mis NIS2 järgi kuuluvad intsidenditeate koosseisu. Seejuures edastatakse üksnes need andmed, mis on teavitamise hetkel olemas, ning järgnevad teavitused täiendavad ja ajakohastavad varasemalt esitatud teavet. Selline lähenemine tagab, et pädev asutus saab varakult piisava ülevaate intsidendist ning et üksusel on võimalik koostada lõpparuanne ühtse loogika alusel.

Ühtne ja sisuline teavituste struktuur peab vähendama üksuste halduskoormust, võimaldades sama teavitusega täita ka teiste õigusaktide alusel kehtivaid teavituskohustusi, kui sama intsident kuulub mitme õigusakti reguleerimisalasse.

Eesti leiab, et sama põhimõte peab kajastuma ka NIS2 artikli 23 lõike 4 kohaldamisel ning komisjoni võimalike rakendusaktide ettevalmistamisel artikli 23 lõike 11 alusel. Varajase hoiatuse andmekoosseis peab olema piisavalt paindlik, et üksus saaks esitada teabe vastavalt

sellele, mis on teavitamise hetkel teada, kuid samal ajal piisavalt sisuline, et pädev asutus saaks täita oma ülesandeid ja hinnata intsidendi mõju.

Kui selline lähenemine ei leia toetust NIS2 muutmise aruteludes, on võimalik seda põhimõtet edendada ka digivaldkonna lihtsustamise koondpakettide (COM(2025) 836 ja COM(2025) 837) ning nende alusel koostavate rakendusaktide menetluses.

6.16. Eesti leiab, et küberturvalisuse valdkonnas lunavararünnetega seotud intsidendist teavitamise andmeväljade ning küberintsidentide käsitlemise üksustele või pädevale asutusele täiendava selgituse küsimuse volituse lisamine dubleerib kehtivaid NIS2 nõudeid, mistõttu tuleks vastavad muudatused eelnõust välja jätta.

Selgitus:

NIS2 muutva direktiivi ettepanekuga lisatakse artikli 23 (teatamiskohustus) juurde lõiked 12 ja 13, mis näevad ette täiendavad teavitamisnõuded lunavararünnete kohta. Lõike 12 kohaselt peab komisjon rakendusaktis sätestama lunavararünnete kohta esitatava teabe, ning lõige 13 kohustab üksusi esitama küberintsidentide käsitlemise üksusele (CSIRT) või pädevale asutusele täiendavat teavet lunarahanõuete ja maksete kohta, kui pädev asutus seda taotleb.

Eesti hinnangul ei ole nende lõigete lisamise vajadus praegu piisavalt põhjendatud. Lõike 12 puhul ei ole selge, millist täiendavat lisandväärtust see loob, arvestades, et lunavararünnakud on juba praegu olulised küberintsidendid, millest tuleb teavitada. Samuti ei ole üheselt määratletud, mida peetakse ründevektori või leevendusmeetmete all, mistõttu vajaks nende sisu täiendavat sisustamist. Selliste spetsiifiliste nõuete lisamine võib viia olukorrani, kus NIS2 raamistikku hakatakse täiendama eraldi nõuetega konkreetsete intsidenditüüpide kohta, mis ei ole kooskõlas direktiivi horisontaalse ülesehitusega.

Lõike 13 puhul ei ole selge, millist lisandväärtust see loob võrreldes juba kehtiva regulatsiooniga. CSIRTil ja pädeval asutusel on juba praegu õigus küsida täiendavat teavet vahearuande esitamise käigus NIS2 artikli 23 lõike 4 punkti c alusel. Kavandatav lõige dubleerib sisuliselt olemasolevat volitust ning ei loo uut sisulist vajadust.

Seetõttu leiab Eesti, et enne lõigete 12 ja 13 lisamist on vaja täiendavat õigusselgust nende sisu, ulatuse ja vajalikkuse kohta, kuid dubleerimise korral tuleks need välja jätta. Vajaduse korral oleks otstarbekam kohe reguleerida lunavararünnete teavitamise täpsustused komisjoni rakendusaktis artikli 23 lõike 11 alusel, mitte lisada neid direktiivi tasandil eraldi lõigetena.

6.17. Eesti toetab muudatust, mille kohaselt on võimalik küberturvalisuse sertifitseerimist kasutada riskijuhtimismeetmete täitmise tõendamiseks. Eesti leiab, et seda lähenemist tuleks rakendada ka teiste Euroopa Liidu õigusaktide puhul, mis käsitlevad küberturvalisuse riskijuhtimismeetmete või turvameetmete täitmise tõendamist.

Selgitus:

NIS2 artiklisse 24 kavandatavad lõiked 4–6 seonduvad küberturvalisuse sertifitseerimise kasutamisega riskijuhtimismeetmete täitmise tõendamisel. Nende lõigete puhul tuleb arvestada ka seisukohtadega 6.6 ja 6.7, mille kohaselt peab küberturvalisuse sertifitseerimine jääma

vabatahtlikuks ning liikmesriikidel peab säilima pädevus kontrollida sertifikaatide aluseks olevate nõuete täitmist.

Kavandatav lõige 4 võimaldab liikmesriikidel nõuda, et elutähtsad ja olulised üksused tõendaksid NIS2 artikli 21 nõuete täitmist CSA2 artikli 75 alusel vastu võetud Euroopa küberturvalisuse sertifitseerimiskava kohase turvaoleku sertifikaadiga. See tähendab, et sertifikaati kasutatakse konkreetse NIS2 kohustuse täitmise tõendina. Eesti toetab seda lähenemist.

Kui selline lähenemine jääb direktiivi, tuleb analüüsida, kas sama põhimõtet saab rakendada ka muude Euroopa Liidu õigusaktide puhul, mis sisaldavad küberturvalisuse riskijuhtimise või turvameetmete nõudeid. Kui see on võimalik, siis Eesti leiab, et seda lähenemist on võimalik laiendada ka muudesse õigusaktidesse. NIS2 kohaldamisalasse kuulub mitmeid üksusi, kellele kohalduvad ka teised valdkondlikud õigusaktid *lex specialis*'na. Näiteks:

- finantssektorile kohaldub DORA määrus (EL) 2022/2554;
- kosmosevaldkonna üksustele hakkab tulevikus kohalduma Euroopa Liidu kosmosemäärus;
- usaldusteenuste osutajatele kohalduvad eIDAS määruse (EL) 910/2014 nõuded ja standardid;
- piiriüleste elektrivoogudega seotud üksustele kohalduvad võrgueeskirjad (nt delegeeritud määrus (EL) 2024/1366);
- lennundussektorile kohalduvad infoturbe eeskirjad (nt rakendusmäärus (EL) 2023/203 ja delegeeritud määrus (EL) 2022/1645).

Need valdkonnad ei ole ammendavad, kuid näitavad, et küberturvalisuse sertifitseerimise kasutamine vastavuse tõendina võib mõjutada mitut õigusraamistikku. Seetõttu tuleb hinnata, kas ja millisel kujul on selline käsitlus kooskõlas teiste Euroopa Liidu õigusaktidega ning kas see võib tekitada kattuvusi või vastuolusid valdkondlike nõuetega.

6.18. Eesti leiab, et NIS2 muudatuste ülevõtmise tähtaeg peab olema vähemalt 18 kuud. Direktiivi ülevõtmise tähtaeg peab arvestama liikmesriikide õigusloomeprotsessiga ning kaasneva haldus- ja töökoormusega.

Selgitus:

NIS2 muutva direktiivi ettepaneku artikli 2 kohaselt võtavad liikmesriigid selle direktiivi ettepanekuga seotud meetmed vastu ja avaldavad need hiljemalt 12 kuud pärast ettepanekuga seotud direktiivi jõustumist. NIS2 üle võtmine Euroopa Liidus on läinud vaevaliselt, sh mitmed riigid (sh Eesti) ei suutnud seda tähtaegselt üle võtta. Ka osad riigid tegelevad tänaseni sellega, et vajalikud siseriiklikud muudatused saaks lõpule viia. Kui arvestada asjaoluga, et liikmesriikide samad esindajad on eelduslikult küberturvalisuse valdkonnaga seotud teiste õigusaktide läbirääkimiste (nt nn digivaldkonna lihtsustamise koondpakettidega seotud läbirääkimised) ja ülevõtmistega, näiteks küberkerksuse määrusega[24] kui ka kübersolidaarsuse

[24] Euroopa Parlamendi ja nõukogu määrus (EL) 2024/2847, 23. oktoober 2024, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse

määrusega[25] seotud sätted seotud, siis ei pruugi olla liikmesriikidel piisavalt võimekust, et mitut teemat hallata. Samamoodi on vaja ka NIS2 rakendajatel aega, et valmistuda uute nõuetest arusaamiseks ja rakendamiseks. Seetõttu peab direktiivi muudatuste ülevõtmise tähtaeg olema pikem kui 12 kuud, st vähemalt 18 kuud.

7. Arvamuse saamine ning seisukohtade kooskõlastamine

7.1. Justiits- ja Digiministeerium on seisukohtade ettevalmistamisel küsinud sisendit Majandus- ja Kommunikatsiooniministeeriumilt, Haridus- ja Teadusministeeriumilt, Kaitseministeeriumilt, Kliimaministeeriumilt, Välisministeeriumilt, Kultuuriministeeriumilt, Rahandusministeeriumilt, Siseministeeriumilt, Sotsiaalministeeriumilt, Regionaal- ja Põllumajandusministeeriumilt, Andmekaitse Inspektsioon, Finantsinspektsioon, Kaitsepolitseiamet, Politsei- ja Piirivalveamet, Põllumajandus- ja Toiduamet, Registrite ja Infosüsteemide Keskus, Riigi Info- ja Kommunikatsioonitehnoloogia Keskus, Riigi Infosüsteemi Amet, Siseministeeriumi infotehnoloogia- ja arenduskeskus, Tarbijakaitse ja Tehnilise Järelevalve Amet, Terviseamet, Transpordiamet, Välisluureamet, Kaitsevägi (küberväejuhatus), Kaitseliit (küberkaitseüksus), Eesti Pank, Eesti Interneti Sihtasutus, Eesti Kaubandus-Tööstuskoda, Eesti Tarbijakaitse Liit, Eesti Tööandjate Keskliit, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Tervise Arengu Instituut, Tallinna Tehnikakõrgkool, Tallinna Tehnikaülikool, Tallinna Ülikool, Tartu Ülikool, Cleveron, Cybernetica, Eesti Raudtee, Health Founders, Metrosert, Startup Leaders Club, Sunly, Tehnopol, Utilitas.

7.2. Arvamuste avaldamiseks saadeti huvigruppidele kaasamiskiri ning tagasiside esitamise tähtaeg oli 31.03.2026.

7.3. Kooskõlastuse ja arvamuse saatsid Kliimaministeerium, Majandus- ja Kommunikatsiooniministeerium, Rahandusministeerium, Siseministeerium, Sotsiaalministeerium, Andmekaitse Inspektsioon, Riigi Infosüsteemi Amet, Tarbijakaitse ja Tehnilise Järelevalve Amet, Eesti Maaülikool, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Kaubandus-Tööstuskoda ning Eesti Tööandjate Keskliit.

7.4. Saabunud sisendid on esitatud kaasamistabelis (lisa 1) ning saabunud ettepanekutega on võimaluse korral arvestatud. Ministeeriumid on seisukohad kooskõlastanud EL koordinatsioonikogus.

määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) - https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02024R2847-20241120.

[25] Euroopa Parlamendi ja nõukogu määrus (EL) 2025/38, 19. detsember 2024, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks, ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) - https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02025R0038-20250115.