RIIGIKANTSELEI

Riigikogu juhatus

Meie: 28.05.2026
nr 4-2/25-00837-3

Eesti seisukohad Euroopa Liidu küberturvalisuse õigusaktide eelnõude paketi kohta

Austatud Riigikogu juhatus

Edastan Vabariigi Valitsuse 28. mai 2026. a istungil heaks kiidetud järgmised Eesti seisukohad Euroopa Komisjoni küberturvalisuse õigusaktide eelnõude paketi kohta, mis koosneb küberturvalisuse 2. määruse eelnõust (edaspidi CSA2) (COM(2026) 11 final) ning küberturvalisuse 2. direktiivi (edaspidi NIS2) muudatuste eelnõust (COM(2026) 13 final):

NIS2 muudatuste ja CSA2 üldised põhimõtted

1.1. Eesti toetab Euroopa Liidu küberturvalisuse tugevdamist, kuid peab oluliseks, et NIS2 muutva ja CSA2 eelnõu nõuded, terminoloogia ja kohaldumisala tagavad liikmesriikidele ja puudutatud subjektidele selge ja üheselt mõistetava õigusraamistiku, kuna juba kehtiva NIS2 sõnastus on ebaselge ja mitmeti tõlgendatav.

1.2. 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 puhul) 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.

CSA2 eelnõuga seotud seisukohad

1.3. 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 neil säilima piisav paindlikkus otsustada, millisest asutusest pädev esindaja määrata. Oluline on vältida väikeriikidele liigse töökoormuse tekkimist.

1.4. Eesti toetab küberoskuste tõendamise kavade ja küberoskuste akadeemia loomist ning nendega seotud ülesannete andmist ENISA-le, kuid peab oluliseks vältida liikmesriikide

Stenbocki maja / Rahukohtu 3 / 15161 Tallinn / Estonia / registrikood 70004809
+372 693 5555 / riigikantselei@riigikantselei.ee / www.riigikantselei.ee

õppeasutustele lisanduvat halduskoormust. Loodavad küberoskuste tõendamise kavad peavad arvestama olemasolevaid kompetentsimudeleid ja sertifikaate. Kaasnevad lisakulud ja -ülesanded peavad olema põhjendatud ning arvestama liikmesriikide olemasolevate õppekavade mahtu ja korraldust. Kompetentsiprofiilide väljatöötamisel peab arvestama ka Euroopa Liidu tööturu olukorra ning juba kasutusel olevate rahvusvaheliste sertifikaatidega.

1.5. 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.

1.6. 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 lisanõuete täitmist juhul, kui sertifikaat ei kata kogu vajalikku riskispektrit või ei anna piisavat kindlust kõigi asjakohaste nõuete täitmise kohta (näiteks julgeoleku valdkond).

1.7. Eesti peab oluliseks, et IKT tarneahelate turvalisuse tagamisel pööratаks 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 kindlaksmääramise protsessi läbipaistvus ja usaldusväärsus.

1.8. 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.

NIS2 muudatuste eelnõuga seotud seisukohad

1.9. Eesti toetab Euroopa digiidentiteedikukrute pakkujate ja Euroopa ettevõtluskukrute pakkujate ning nii 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 väljajätmist NIS2 kohaldamisalast.

1.10. 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.

1.11. 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 ENISA-le 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 nii registri pidamises, sellele juurdepääsus, registri ja selles sisalduvate andmete kaitses, andmete säilitamistähtaegades kui ka muudes asjakohastes korralduslikes aspektides.

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

1.13. 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.

1.14. 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 olla üleminekuperiood kuni kolm aastat.

1.15. 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 lahendatud intsidendi lõpparuanne. Teavitustega seotud andmeväljad peavad võimaldama tagada ka teiste Euroopa Liidu õigusaktide alusel sama intsidendi kohta esitatavate teavituste kohustuste täitmist.

1.16. 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.

1.17. 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.

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

Lugupidamisega

(allkirjastatud digitaalselt)
Heili Tõnisson
Valitsuse nõunik

Lisad:
1. Seletuskiri
2. Seletuskirja lisa kaasamise tabel
3. Eelnõu COM(2026) 11 (CSA2)
4. Eelnõu COM(2026) 11 (CSA2) lisa
5. Eelnõu COM(2026) 13 (NIS2 muudatused)

Teadmiseks:
Riigikogu Euroopa Liidu asjade komisjon

Sandra Metste
Sandra.Metste@riigikantselei.ee