Küberturvalisuse eelnõude pakett

COM(2026) 11 ja COM(2026) 13

Otsuse ettepanek koordinatsioonikogule

Kujundada seisukoht

Kaasvastutaja sisendi tähtpäev 09.03.2026

KOKi esitamise tähtpäev 18.03.2026

VV esitamise tähtpäev 26.03.2026

Peavastutaja Justiits- ja digiministeerium,

Kaasvastutajad Majandus- ja kommunikatsiooniministeerium, Kaitseministeerium, Kliimaministeerium, Rahandusministeerium, Sotsiaalministeerium ja Siseministeerium.

Seisukoha valitsusse toomise alus ja põhjendus

Algatuse reguleerimisala nõuab vastavalt Eesti Vabariigi põhiseadusele seaduse või Riigikogu otsuse vastuvõtmist, muutmist või kehtetuks tunnistamist (RKKTS § 152¹ lg 1 p 1);

Algatuse vastuvõtmisega kaasneks oluline majanduslik või sotsiaalne mõju (RKKTS § 152¹ lg 1 p 2).

Sisukokkuvõte

Pakett sisaldab ettepanekut läbivaadatud küberturvalisuse määruse kohta, millega tugevdatakse ELi info- ja kommunikatsioonitehnoloogia (IKT) tarneahelate turvalisust. Lihtsama sertifitseerimisprotsessi kaudu soovitakse tagada, et ELi kodanikeni jõudvad tooted on algusest peale küberturvalised. Samuti on eesmärk hõlbustada ELi küberturvalisuse eeskirjade järgimist ning tugevdada Euroopa Liidu Küberturvalisuse Ameti (ENISA) rolli liikmesriikide ja ELi toetamisel küberohtude ohjamisel.

<u>IKT tarneahelate turvalisuse suurendamine ELis</u>

Uue küberturvalisuse määruse eesmärgiks on vähendada riske, mida ELi IKT tarneahelale kujutavad kolmandate riikide tarnijate küberturvalisusega seotud probleemid. Määruses sätestatakse usaldusväärne IKT tarneahelate turvalisuse raamistik, mis põhineb ühtlustatud, proportsionaalsel ja riskipõhisel lähenemisviisil. See võimaldab ELil ja liikmesriikidel ühiselt tuvastada ja leevendada riske 18 ELi jaoks elutähtsas sektoris,

võttes arvesse ka majanduslikku mõju ja pakkumist turul. IKT tarneahelad on elutähtsate teenuste ja elutähtsa taristu toimimiseks hädavajalikud. Hiljutised küberintsidendid on toonud esile nende nõrkustest tulenevad suured riskid. Tänapäeval ei tähenda tarneahelate turvalisus enam ainult toote või teenuse tehnilist turvalisust, vaid ka tarnijaga seotud riske, eelkõige sõltuvusi ja välissekkumist. Küberturvalisuse määrus näeb ette kohustuse leevendada Euroopa mobiilsidevõrkudele suure riskiga kolmandate riikide tarnijatest tulenevaid riske, tuginedes 5G küberturvalisuse meetmepaketi raames tehtule.

Euroopa küberturvalisuse sertifitseerimise raamistiku lihtsustamine ja tõhustamine

Uue küberturvalisuse määrusega tagatakse, et ELi tarbijateni jõudvate toodete ja teenuste turvalisust testitakse senisest tõhusamalt Euroopa küberturvalisuse sertifitseerimise raamistiku kaudu. Raamistikuga soovitakse pakkuda suuremat selgust ja lihtsamaid menetlusi, võimaldades sertifitseerimiskavade väljatöötamist vaikimisi 12 kuu jooksul. Samuti võetakse kasutusele paindlikum ja läbipaistvam juhtimine, et sidusrühmi avaliku teavitamise ja konsulteerimise kaudu paremini kaasata.

ENISA hallatavatest sertifitseerimiskavad võimaldavad ettevõtjatel tõendada oma tegevuse vastavust ELi õigusaktidele ning vähendada koormust ja kulusid. Lisaks IKT-toodetele, -teenustele, -protsessidele ja hallatud turbeteenustele saavad ettevõtjad ja organisatsioonid sertifitseerida oma turvaolekut, et see vastaks turu vajadustele.

Küberturvalisuse eeskirjade järgimise hõlbustamine

Paketiga täiendatakse digivaldkonna lihtsustamise koondpaketis kavandatud küberintsidentidest teavitamise ühtset kontaktpunkti. Pakett sisaldab meetmeid, millega lihtsustatakse ELis tegutsevate ettevõtjate jaoks ELi küberturvalisuse eeskirjade ja riskijuhtimisnõuete täitmist. Küberturvalisuse NIS2 direktiivi sihipäraste muudatuste eesmärk on suurendada õigusselgust, lihtsustatakse mikro- ja väikeettevõtjate ning väikeste keskmise turukapitalisatsiooniga ettevõtjate jaoks nõuete täitmist. Muudatustega lihtsustatakse kohtualluvuse reegleid, ühtlustatakse andmete kogumist lunavararünnete kohta ja hõlbustatakse piiriüleste üksuste järelevalvet ENISA koordineeriva rolli kaudu.

ENISA roll Euroopa küberturvalisuse alase vastupanuvõime tugevdamisel

ENISA ülesandeks on aidata ELil ja selle liikmesriikidel mõista ühiseid ohte, et võimaldada neil küberintsidentideks valmistuda ja neile reageerida. ENISA toetab ELis tegutsevaid ettevõtjaid ja sidusrühmi, andes varajasi hoiatusi küberohtude ja -intsidentide kohta. Koostöös Europoli ja küberintsidentidele reageerimise üksustega toetab ENISA ettevõtjaid lunavararünnetele reageerimisel ja neist taastumisel. ENISA töötab välja ka liidu nõrkusehalduse teenuste lähenemisviisi. ENISA hakkab haldama digivaldkonna lihtsustamise koondpaketis kavandatud küberintsidentidest teavitamise ühtset kontaktpunkti. Küberturvalisuse valdkonnas kvalifitseeritud tööjõu olemasolu tagamiseks

võetakse kasutusele küberoskuste akadeemia ja luuakse kogu ELi hõlmavad küberturbeoskuste tõendamise kavad.

Kas EL algatus reguleerib karistusi või haldustrahve? Jah

Kas nähakse ette uue asutuse loomine (järelevalvelised või muud asutused)? Jah

Ei pruugi tähendada uue asutuse loomist, kuid liikmesriigid peavad määrama pädeva asutuse.

Kas lahenduse rakendamine vajab IT-arendusi? Jah

Vajab selgitamist, kas algatusega kaasneb IT-arenduste vajadust.

Kaasamine

Kaasata eelnõude paketiga hõlmatud huvirühmad.