Euroopa Liidu
Nõukogu

Brüssel, 22. jaanuar 2026
(OR. en)

5611/26
ADD 2

Institutsioonidevahelised dokumendid:
2026/0011 (COD)
2026/0012 (COD)

CYBER 29
JAI 85
DATAPROTECT 22
TELECOM 29
MI 58
IND 48
CADREFIN 26
FIN 100
BUDGET 3
CODEC 90

SAATEMÄRKUSED

Saatja:	Euroopa Komisjoni peasekretär, allkirjastanud Martine DEPREZ, direktor
Kättesaamise kuupäev:	21. jaanuar 2026
Saaja:	Thérèse BLANCHET, Euroopa Liidu Nõukogu peasekretär
Komisjoni dok nr:	SWD(2026) 12 final
Teema:	KOMISJONI TALITUSTE TÖÖDOKUMENT MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE […] Lisatud dokumentidele: 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) ja Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga]

Käesolevaga edastatakse delegatsioonidele dokument SWD(2026) 12 final.

Lisatud: SWD(2026) 12 final

EUROOPA
KOMISJON

Strasbourg, 20.1.2026
SWD(2026) 12 final

KOMISJONI TALITUSTE TÖÖDOKUMENT

MÕJU HINDAMISE ARUANDE KOMMENTEERITUD KOKKUVÕTE

[…]

Lisatud dokumentidele:

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)

ja

Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV,
millega muudetakse direktiivi (EL) 2022/2555 seoses lihtsustamismeetmetega ja vastavusse viimisega [küberturvalisuse 2. määruse ettepanekuga]

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

Mõju hindamise aruande kokkuvõte

Eesmärk

Käesoleva mõjuhinnangu peamine eesmärk on hinnata kehtivate õigusnormide asjakohasust muutuvate küberohtudega tegelemisel kogu ELis. Selles pakutakse välja integreeritud poliitikavariandid, mille eesmärk on tugevdada Euroopa Liidu Küberturvalisuse Ametit (edaspidi „ENISA“), reformida Euroopa küberturvalisuse sertifitseerimise raamistikku ja lihtsustada kehtiva küberturvalisuse õigusraamistiku järgimist. Hinnangus rõhutatakse, kui tähtis on kohandada küberturvalisuse juhtimist, et viia see kooskõlla tehnoloogia arengu ja turunõudlusega, tagades samal ajal konkurentsivõime ja võttes arvesse keskkonnamõju.

Probleemipüstitus

Hoolimata praegustest jõupingutustest on ELi küberturvalisuse valdkonnas aina keerukamate ohtude taustal endiselt märkimisväärseid probleeme. Tõhusat küberturvalisuse juhtimist pärsivad ebapiisav koordineerimine liikmesriikide ja muude ELi tasandi osalejate seas, viivitused poliitikavahendite kasutuselevõtul ning regulatiivsed takistused ja keerukus. Need probleemid põhjustavad ettevõtjate ja avaliku sektori asutuste kulude ja küberintsidentide ohu suurenemist ning kodanike kaitse ebaühtlast taset.

ELi meetme põhjendus

Küberohud ületavad riigipiire, seega on jõuliseks reageerimiseks hädavajalik ühtne lähenemisviis. ELi tasandi sekkumine tagab järjepideva kaitse, suurendab võrdsete tingimuste pakkumise abil konkurentsivõimet ning hõlbustab digiteenuste ja -toodete vaba liikumist ühtsel turul. Lihtsustatud nõuete täitmise ja lihtsustatud menetluste kaudu vähendab ELi tasandi ühtlustamine ka halduskoormust.

Poliitikavariandid ja eelistatud poliitikavariant

Käesolevas aruandes analüüsitakse nelja sekkumisvaldkonda, millest igaühe puhul kaalutakse poliitikavariante, lähtudes konkreetsetest saavutamist ootavatest eesmärkidest: 1) ENISA volitused (kuulub ka praeguse küberturvalisuse määruse alla); 2) Euroopa küberturvalisuse sertifitseerimise raamistik (kuulub samuti praeguse küberturvalisuse määruse alla) ning 3) küberturvalisuse 2. direktiivi sihipärased muudatused, mille eesmärk on lihtsustamine ja mis on samal ajal seotud ka ENISA volituste ja Euroopa küberturvalisuse sertifitseerimise raamistikuga. Kõik need poliitikavariandid on omaette sekkumisvaldkonnad, kuid seejuures omavahel seotud ja vastastikku olulised.

Poliitikavariandid ELi küberturvalisuse poliitikaraamistiku ja sidusrühmade vajaduste kooskõlastamiseks üha vaenulikumas keskkonnas

Variant A.1: *ENISA volituste täpsustamine ja prioriteetide seadmine* – see variant tagaks selge ja stabiilse raamistiku ENISA ülesannete täitmiseks, sest hõlmaks ka muudes õigusaktides sätestatud ülesandeid.

Variant A.2: *ENISA volituste reform* – selle variandiga tunnistataks küberturvalisuse määrus kehtetuks ja asendataks see, nähes ette ameti volituste läbivaatamise.

Variant A.3: *ENISA volituste reform, milles pööratakse suurt tähelepanu operatiivtoetusele* – see variant oleks variandi A.2 edasiarendus. Täiendavalt suurendataks ENISA suutlikkust, et pakkuda liikmesriigi taotlusel üksustele, kelle suhtes kohaldatakse küberturvalisuse 2. direktiivi, otsest tuge küberintsidentidele reageerimisel ja neist taastumisel.

Euroopa küberturvalisuse sertifitseerimise raamistikuga seotud poliitikavariandid

Variant B.1: *Euroopa küberturvalisuse sertifitseerimise raamistiku kohaldamisala, elementide ja eesmärkide täpsustamine ning haldusmehhanismi kasutuselevõtt* – selle variandiga nähakse ette kavade vastuvõtmise järel ENISA rakendatav uus kavade haldamise mehhanism.

Variant B.2: *Euroopa küberturvalisuse sertifitseerimise raamistiku reform, mille raames vaadatakse läbi raamistiku menetlused ja laiendatakse selle kohaldamisala, et aidata lihtsustada õigusnormidele vastavust* – selle variandi puhul tunnistataks küberturvalisuse määrus kehtetuks ja asendataks uue määrusega. Lisaks variandis B.1 kavandatule vaadataks läbi kavade taotlemise, väljatöötamise ja vastuvõtmisega seotud menetlused, et suurendada vastutust ja tõhusust.

Variant B.3: *Euroopa küberturvalisuse sertifitseerimise raamistiku reform, nagu on ette nähtud variandi B.2 korral, ja turvaoleku sertifitseerimise kohustuse kehtestamine* – see variant põhineks variandil B.2, kuid selle eesmärk on raamistiku mõju veelgi tugevdada, kehtestades küberturvalisuse 2. direktiiviga hõlmatud elutähtsate üksuste sertifitseerimise kohustuse, võttes arvesse konkreetseid riskistsenaariume, selle asemel, et tugineda ainult üksuste vabatahtlikule sertifitseerimisele.

Lihtsustamisega seotud poliitikavariandid

Variant C.1: *pehmel õigusel ja muudel kui seadusandlikel vahenditel põhineva lähenemisviisi, sh olemasolevate volituste kasutamine (rakendusaktide vastuvõtmine küberturvalisuse 2. direktiivi artikli 21 lõike 5 ja artikli 23 lõike 11 alusel)* – selle variandi kohaselt võetaks vastu rakendusaktid, kasutades olemasolevaid küberturvalisuse 2. direktiivis sätestatud volitusi, et tagada küberriskide juhtimise meetmete, intsidentidest teatamise künniste ning teabe liigi, vormi ja teatamise korra parem ühtlustamine. Samuti on kavandatud suuniste vastuvõtmine, et suurendada õiguskindlust ja ühtlustada rakendamist.

Variant C.2: *sihipärane sekkumine – asjaomase liidu küberturvalisuse õigusraamistiku järgimise edasine lihtsustamine* – see variant hõlmab piiratud sekkumist küberturvalisuse määruse ja küberturvalisuse 2. direktiivi muutmise kaudu, mille eesmärk on lihtsustada küberturvalisuse raamistiku konkreetseid aspekte, sealhulgas kohaldamisala kohandamine, rakendusaktide võimalikult suur ühtlustamine, nõuete täitmise tõendamine sertifitseerimise kaudu ja variandi C.1 all ette nähtud suuniste vastuvõtmine.

Variant C.3: *liidu õiguses sätestatud küberturvalisuse meetmete ühtlustamine* – see variant põhineks variandil C.2 ja sellega eemaldataks kõik valdkondlikes õigusaktides sätestatud küberturvalisuse riskijuhtimismeetmed või volitused. Selle asemel muudetaks

küberturvalisuse 2. direktiivi ökosüsteemi, et näha ette ühtlustatud nõuded igat liiki üksustele, tagades sel viisil suurema ühtlustamise.

IKT tarneahela turvalisusega seotud poliitikavariandid

Variant D.1: *pehme õiguse lähenemisviisi kasutamine IKT tarneahelate küberriskide käsitlemiseks* – see variant ei näeks ette ELi tasandi regulatiivset sekkumist. Selle asemel suurendaks komisjon koordineeritud riskihindamiste ja vabatahtlike abivahendite arvu.

Variant D.2: *sihipärane regulatiivne sekkumine, millega kodifitseeritakse 5G meetmepakett* – selle variandiga kodifitseeritaks 5G meetmepaketi meetmed. Sellega kehtestataks liikmesriikidele kohustus tagada, et võrgu põhivarades ei kasutata suure riskiga tarnijate komponente.

Variant D.3: *terviklik ja horisontaalne raamistik IKT tarneahelate küberriskide käsitlemiseks* – selle variandiga loodaks IKT tarneahelates esinevate mittetehniliste küberriskide käsitlemiseks tehnoloogia- ja sektorineutraalne horisontaalne õigusraamistik.

Põhjaliku analüüsi tulemusel kuuluvad eelistatud poliitikapaketti: variant A.2 – ENISA volituste reform; variant B.2 – Euroopa küberturvalisuse sertifitseerimise raamistiku reform, mille raames vaadatakse läbi menetlused ja laiendatakse kohaldamisala, et aidata lihtsustada õigusnormidele vastavust; variant C.2 – sihipärane sekkumine – asjaomase liidu küberturvalisuse õigusraamistiku järgimise edasine lihtsustamine ning variant D.3 – terviklik ja horisontaalne raamistik IKT tarneahelate küberriskide käsitlemiseks.

See kombinatsioon pakub hästi tasakaalustatud lahenduse tuvastatud poliitilistele probleemidele ning suurendab märkimisväärselt tulemuslikkust, tõhusust ja sidusust kogu ELis.

Peamine mõju

Kulude-tulude analüüs. Kavandatud õigusraamistikule üleminekuga kaasnevad kulud nii ENISA-le – hinnanguliselt kuni 161,3 miljonit eurot viie aasta jooksul selle uute ülesannete täitmiseks –, kui ka ELi avaliku sektori asutustele – kuni 80 miljonit eurot viie aasta jooksul järelevalve tegemiseks (võttes arvesse asjakohast kulude kokkuhoidu). Ettevõtjate puhul võib teatavate suure riskiga seadmete järkjärguline kasutuselt kõrvaldamine tuua mobiilsideoperaatoritele kolme aasta pikkuse üleminekuperioodi jooksul kaasa 3,4–4,3 miljardi euro ulatuses kulusid aastas, samal ajal kui investeeringud usaldusväärsetesse tarnijatesse võivad kasvada kuni 2 miljardi euroni aastas. Lisaks peaksid nõuete täitmise ühtlustatud ja vähendatud kohustused eeldatavasti aitama ettevõtjatel kokku hoida kuni 14,6 miljardi euro ulatuses kulusid. Märkimisväärset kasu kodanikele, avaliku sektori asutustele ja ettevõtjatele tooks samuti ELi üldise turvaoleku ja tehnoloogilise suveräänsuse parandamine ning innovatsiooni ja konkurentsivõime stimuleerimine, mis peaks pikas perspektiivis suuresti korvama esialgsed kulutused.

Konkurentsivõime. Eelistatud poliitikavariandid suurendavad turu killustatuse vähendamise ja eeskirjade ühtlustamise kaudu konkurentsialast võrdsust ELis, pakkudes ettevõtjatele selgemaid võimalusi nõuete täitmiseks ja innovatsiooniks.

Kliimaeesmärkidega kooskõla kontroll. Hindamisel võeti arvesse iga poliitikavariandi võimalikku keskkonnamõju. Erilist tähelepanu pöörati energiatõhususele, reisimisega seotud heitkogustele ja taristu tugevdamisele. Eelistatud poliitikavariantide A.2, B.2 ja C.2 keskkonnamõju on piiratud, samas kui D.3 puhul võetakse arvesse keskkonnaneutraalsust, toote elutsüklit ja üleminekuperioode peamiste varade asendamiseks. See on kooskõlas ELi võetud kestlikkuskohustustega.

Vaikimisi digitaalsus. Rõhuasetus ühtlustatud digiprotsessidele näitab, et EL on pühendunud lähenemisviisile „kõigepealt digitaalne“, et tagada kiirem ja usaldusväärsem andmevahetus ja otsuste tegemine. Ka variandil D.3 võib olla suur mõju digiüleminekule, kuna see hõlmaks selliste komponentide asendamist, mis on pärit üksustest, mis on asutatud küberturvalisuse seisukohast muret tekitavates kolmandates riikides, või nende üksuste kontrolli all olevatest üksustest.

Lihtsustamine ja koormuse vähendamine. Eelistatud poliitikavariandid aitavad lihtsustamisele kaasa kohaldamisala täpsustamise ning nõuete täitmise ja järelevalve ühtlustamise meetmete kehtestamisega, millega vähendatakse halduskoormust. Kaalutakse põhimõtet „üks sisse, üks välja“, tagades, et uusi kohustusi tasakaalustavad vähendamised mujal.

Kokkuvõte

Käesolevas mõjuhinnangus on esitatud terviklik strateegia ELi küberturvalisuse suurendamiseks, regulatiivse ebatõhususe kõrvaldamiseks ja digikeskkonna ettevalmistamiseks tulevasteks probleemideks. Selles on soovitatud koostööl põhinevat ja sidusat lähenemisviisi, mis tugineb olemasolevate raamistike poliitikareformidele, ja samal ajal kohanemist tehnoloogiavaldkonna uue tegelikkusega. Nende meetmete abil püüab EL tagada vastupidava, konkurentsivõimelise ja kestliku digimajanduse.