Eiropas Savienības Padome

Briselē, 2026. gada 22. janvārī
(OR. en)

Starpiestāžu lietas:
2026/0011 (COD)
2026/0012 (COD)

5611/26
ADD 2

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

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2026. gada 21. janvāris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	SWD(2026) 12 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS Pavaddokuments dokumentiem Priekšlikums. Eiropas Parlamenta un Padomes Regula par Eiropas Savienības Kiberdrošības aģentūru (ENISA), Eiropas kiberdrošības sertifikācijas satvaru un IKT piegādes ķēdes drošību, un ar ko atceļ Regulu (ES) 2019/881 (2. kiberdrošības akts) Priekšlikums. Eiropas Parlamenta un Padomes Direktīva, ar ko groza Direktīvu (ES) 2022/2555 saistībā ar vienkāršošanas pasākumiem un salāgošanu ar [priekšlikumu 2. kiberdrošības aktam]

Pielikumā ir pievienots dokuments SWD(2026) 12 final.

Pielikumā: SWD(2026) 12 final

EIROPAS
KOMISIJA

Strasbūrā, 20.1.2026.
SWD(2026) 12 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES NOVĒRTĒJUMA KOPSAVILKUMA ZIŅOJUMS

Pavaddokuments dokumentiem

Priekšlikums. Eiropas Parlamenta un Padomes Regula par Eiropas Savienības Kiberdrošības aģentūru (ENISA), Eiropas kiberdrošības sertifikācijas satvaru un IKT piegādes ķēdes drošību, un ar ko atceļ Regulu (ES) 2019/881 (2. kiberdrošības akts)

Priekšlikums. Eiropas Parlamenta un Padomes Direktīva, ar ko groza Direktīvu (ES) 2022/2555 saistībā ar vienkāršošanas pasākumiem un salāgošanu ar [priekšlikumu 2. kiberdrošības aktam]

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

Ietekmes novērtējuma kopsavilkums

Mērķis

Šā ietekmes novērtējuma galvenais mērķis ir izvērtēt pašreizējo noteikumu piemērotību mainīgo kiberdrošības apdraudējumu novēršanai visā ES. Tajā ir ierosināts integrēts politikas risinājumu kopums, kura nolūks ir stiprināt Eiropas Savienības Kiberdrošības aģentūru (*ENISA*), reformēt Eiropas kiberdrošības sertifikācijas satvaru (*ECCF*) un vienkāršot pašreizējā kiberdrošības tiesiskā regulējuma ievērošanu. Novērtējumā ir uzsvērts, ka svarīgi ir kiberpārvaldību pielāgot, lai saskaņotu to ar tehnoloģiskajiem sasniegumiem un tirgus prasībām, vienlaikus nodrošinot konkurētspēju un ņemot vērā vidisko ietekmi.

Problēmas izklāsts

Neraugoties uz pašreizējiem centieniem, ES kiberdrošības vidē joprojām ir jārisina būtiskas problēmas situācijā, kad apdraudējumi kļūst arvien sarežģītāki. Nepietiekama koordinācija starp dalībvalstīm un citiem ES līmeņa dalībniekiem, pārrāvumi politikas instrumentu īstenošanā, regulatīvie šķēršļi un sarežģītība kavē efektīvu kiberdrošības pārvaldību. Minētās problēmas palielina izmaksas uzņēmumiem un publiskajām iestādēm, paaugstina kiberincidentu risku un apgrūtina vienāda līmeņa aizsardzības nodrošināšanu iedzīvotājiem.

ES rīcības pamatojums

Kiberdrošības apdraudējumi sniedzas pāri valstu robežām, tāpēc pienācīgai reaģēšanai uz tiem ir būtiski izmantot vienotu pieeju. ES līmeņa intervence sniedz konsekventu aizsardzību, uzlabo konkurētspēju, nodrošinot vienlīdzīgus konkurences apstākļus, un veicina digitālo pakalpojumu un produktu brīvu apriti vienotajā tirgū. Saskaņošana ES līmenī arī samazina administratīvo slogu, vienkāršojot atbilstības nodrošināšanu un racionalizējot procedūras.

Politikas risinājumi un vēlamais risinājums

Šajā ziņojumā ir analizētas četras tālāk norādītās intervences jomas, un katrā no tām tika izskatīts politikas risinājumu kopums, ņemot vērā izvirzītos konkrētos mērķus: 1) *ENISA* pilnvaras (ietilpst arī pašreizējā KDA); 2) *ECCF* (ietilpst arī pašreizējā KDA); un 3) mērķtiecīgi grozījumi TID 2 direktīvā tās vienkāršošanai, kas tomēr ir saistīti arī ar *ENISA* pilnvarām un *ECCF*. Katrs risinājumu kopums ir atsevišķa intervences joma, kas vienlaikus tomēr ir saistīta ar pārējiem risinājumu kopumiem un ir tiem svarīga.

Risinājumi, kā novērst ES kiberdrošības politikas satvara nepietiekamu saskaņotību ar ieinteresēto personu vajadzībām arvien naidīgākā vidē

Risinājums Nr. A.1. ENISA *pilnvaru precizēšana un prioritāšu noteikšana*. Šis risinājums nodrošinātu skaidru un stabilu *ENISA* uzdevumu satvaru, iekļaujot tajā arī citos tiesību aktos noteiktos uzdevumus.

Risinājums Nr. A.2. ENISA *pilnvaru reforma.* Šis risinājums paredz atcelt un aizstāt KDA, būtiski pārskatot aģentūras pilnvaras.

Risinājums Nr. A.3. ENISA *pilnvaru reforma ar īpašu uzsvaru uz operatīvo atbalstu.* Šā risinājuma pamatā būtu risinājums Nr. A.2. Piedevām *ENISA* attīstītu spējas pēc dalībvalsts pieprasījuma sniegt tiešu atbalstu vienībām, uz kurām attiecas TID 2 direktīva, tām reaģējot uz kiberdrošības incidentu un atgūstoties no tā.

Risinājumi attiecībā uz Eiropas kiberdrošības sertifikācijas satvaru

Risinājums Nr. B.1. ECCF *tvēruma, elementu un mērķu precizēšana un uzturēšanas mehānisma ieviešana*. Šis risinājums paredz ieviest jaunu mehānismu shēmu uzturēšanai pēc to pieņemšanas, ko paveiks *ENISA*.

Risinājums Nr. B.2. ECCF *reforma, pārskatot tā procedūras un paplašinot tvērumu, lai būtu vieglāk vienkāršot procesu, kādā nodrošina atbilstību regulējumam*. Saskaņā ar šo risinājumu KDA tiktu atcelts un aizstāts ar jaunu regulu. Papildus risinājumam Nr. B.1 pārskatatbildības un efektivitātes uzlabošanai tiktu pārskatīta procedūra, kas ir saistīta ar shēmu izstrādes pieprasīšanu un shēmu izstrādi un pieņemšanu.

Risinājums Nr. B.3. *Risinājumā Nr. B.2 paredzētā* ECCF *reforma un drošības parametru obligātas sertifikācijas ieviešana*. Šā risinājuma pamatā būtu risinājums Nr. B.2, taču tas vēl vairāk palielinātu satvara ietekmi, ieviešot TID 2 direktīvas aptverto būtisko vienību obligātu sertifikāciju atkarībā no konkrētu risku scenārijiem, nevis paļaujoties tikai uz vienību brīvprātīgu sertifikāciju.

Vienkāršošanas risinājumi

Risinājums Nr. C.1. *Pieeja, kas paredz izmantot ieteikuma tiesību un neleģislatīvus instrumentus, arī esošos pilnvarojumus (par īstenošanas aktu pieņemšanu saskaņā ar TID 2 direktīvas 21. panta 5. punktu un 23. panta 11. punktu).* Šis risinājums paredz pieņemt īstenošanas aktus, izmantojot esošos pilnvarojumus, kas piešķirti ar TID 2 direktīvu, lai nodrošinātu lielāku saskaņotību attiecībā uz kiberdrošības risku pārvaldības pasākumiem, incidentu ziņošanas robežvērtībām, kā arī uz informāciju, tās formātiem un paziņošanas procedūrām. Vienlaikus tiktu pieņemts arī pamatnostādņu kopums, kas palīdzētu uzlabot juridisko noteiktību un veicināt saskaņotu īstenošanu.

Risinājums Nr. C.2. *Mērķtiecīga intervence – atbilstības nodrošināšanas procesa turpmāka vienkāršošana attiecībā uz atbilstību attiecīgajam Savienības kiberdrošības tiesiskajam regulējumam*. Šis risinājums paredz ierobežotu intervenci, ieviešot izmaiņas KDA un TID 2 direktīvā nolūkā vienkāršot kiberdrošības regulējuma konkrētus aspektus, tai skaitā pielāgojot darbības jomas, maksimāli saskaņojot īstenošanas aktus, atzīstot sertifikāciju par atbilstības pierādījumu un pieņemot pamatnostādņu kopumu, kā paredzēts risinājumā Nr. C.1.

Risinājums Nr. C.3. *Savienības tiesību aktos noteikto ar kiberdrošību saistīto pasākumu saskaņošana*. Šā risinājuma pamatā ir risinājums Nr. C.2, un tas paredz atcelt visus nozaru tiesību aktos noteiktos kiberdrošības risku pārvaldības pasākumus un ar šādiem pasākumiem saistītos pilnvarojumus. Tā vietā TID 2 direktīvas ekosistēmā tiktu izdarīti grozījumi ar mērķi racionalizēt visu veidu vienībām izvirzītās prasības un tādējādi nodrošināt ciešāku saskaņošanu.

Risinājumi IKT piegādes ķēžu drošībai

Risinājums Nr. D.1. *Pieeja, kas IKT piegādes ķēžu kiberdrošības risku novēršanai paredz izmantot ieteikuma tiesības*. Šis risinājums neparedz ES līmeņa regulatīvu intervenci. Tā vietā Komisija palielinātu koordinētu riska novērtējumu un brīvprātīgi izmantojamu rīkkopu skaitu.

Risinājums Nr. D.2. Ad hoc *regulatīvā intervence 5G rīkkopas kodificēšanai*. Šis risinājums paredz kodificēt 5G rīkkopas pasākumus. Ar to tiktu ieviests pienākums dalībvalstīm nodrošināt, ka tīkla galvenajos aktīvos nav no augsta riska piegādātājiem saņemtu komponentu.

Risinājums Nr. D.3. *Visaptverošs un horizontāls satvars IKT piegādes ķēžu kiberdrošības risku novēršanai*. Šis risinājums paredz izveidot horizontālu, tehnoloģiju un nozaru ziņā neitrālu tiesisko regulējumu netehnisku kiberdrošības risku novēršanai IKT piegādes ķēdēs.

Pēc rūpīgas analīzes vēlamo politikas pasākumu kopumā iekļāva šādus risinājumus: risinājums Nr. A.2 (*ENISA* pilnvaru reforma); risinājums Nr. B.2 (*ECCF* reforma, pārskatot procedūru un paplašinot tvērumu, lai būtu vieglāk vienkāršot procesu, kādā nodrošina atbilstību regulējumam); risinājums Nr. C.2 (mērķtiecīga intervence – atbilstības nodrošināšanas procesa turpmāka vienkāršošana attiecībā uz atbilstību attiecīgajam Savienības kiberdrošības tiesiskajam regulējumam) un risinājums Nr. D.3 (visaptverošs un horizontāls satvars IKT piegādes ķēžu kiberdrošības risku novēršanai).

Šāda risinājumu kombinācija piedāvā līdzsvarotu atbildi uz konstatētajām politikas problēmām, ievērojami uzlabojot lietderīgumu, efektivitāti un saskanību visā ES.

Galvenā ietekme

Izmaksu un ieguvumu analīze. Pāreja uz ierosināto tiesisko regulējumu radīs izmaksas gan *ENISA*, lai tā varētu pildīt savus jaunos uzdevumus (saskaņā ar aplēsēm – līdz 161,3 miljoniem EUR piecu gadu laikā), gan publiskajām iestādēm visā Savienībā saistībā ar uzraudzību (saskaņā ar aplēsēm – līdz 80 miljoniem EUR piecu gadu laikā, ierēķinot attiecīgos izmaksu ietaupījumus). Izmaksas radīsies arī uzņēmumiem, kuriem būs trīs gadu pārejas periodā pakāpeniski jāpārtrauc lietot konkrētas augsta riska iekārtas. Mobilo tīklu operatoriem šādas izmaksas varētu būt 3,4–4,3 miljardi EUR gadā, kamēr ieguldījumi uzticamos piegādātājos varētu vienlaikus sasniegt 2 miljardus EUR gadā. Tajā pašā laikā racionalizēti un samazināti atbilstības nodrošināšanas pienākumi varētu sniegt uzņēmumiem izmaksu ietaupījumus līdz 14,6 miljardu EUR apmērā. Turklāt ES vispārējo drošības parametru un tehnoloģiskās suverenitātes uzlabošana un inovācijas un konkurētspējas stimulēšana sniegtu ievērojamus ieguvumus iedzīvotājiem, publiskajām iestādēm un uzņēmumiem, un ilgtermiņā šie ieguvumi varētu lielā mērā kompensēt sākotnējos izdevumus.

Konkurētspēja. Samazinot tirgus sadrumstalotību un saskaņojot regulējumus, vēlamie risinājumi stiprina vienlīdzīgu konkurenci visā ES, norādot uzņēmumiem skaidrāku virzienu uz atbilstību un inovāciju.

Klimatatbilstības pārbaude. Novērtējumā tika aplūkota katra risinājuma iespējamā vidiskā ietekme. Īpašu uzmanību pievērsa energoefektivitātei, ar ceļošanu saistītām emisijām un infrastruktūras konsolidācijai. Vēlamajiem risinājumiem Nr. A.2, B.2 un C.2 ir ierobežota vidiskā ietekme, savukārt risinājums Nr. D.3 ir vidiski neitrāls, ņemot vērā produkta aprites ciklu un galveno aktīvu aizstāšanai noteiktos pārejas periodus. Tas saskan ar ES apņemšanos panākt ilgtspēju.

Digitāls pēc noklusējuma. Uzsvars uz racionalizētiem digitālajiem procesiem apliecina Savienības apņemšanos īstenot pieeju "vispirms digitāls", nodrošinot ātrāku un uzticamāku datu apmaiņu un lēmumu pieņemšanu. Risinājums Nr. D.3 turklāt varētu būtiski ietekmēt digitalizāciju, jo tas paredz aizstāt komponentus, kuri ir saņemti no vienībām, kas iedibinātas tādās trešās valstīs vai ko kontrolē vienības no tādām trešām valstīm, kuras rada bažas par kiberdrošību.

Vienkāršošana un sloga samazināšana. Vēlamie risinājumi veicina vienkāršošanu, sniedzot skaidrojumus par tvērumu un ierosinot pasākumus atbilstības nodrošināšanas un uzraudzības racionalizēšanai, un tādā veidā samazinot administratīvo slogu. Ir ņemts vērā princips "viens pieņemts – viens atcelts", nodrošinot jauno pienākumu līdzsvarošanu ar citur īstenojamiem samazinājumiem.

Secinājums

Šajā ietekmes novērtējumā ir izklāstīta visaptveroša stratēģija ES kiberdrošības uzlabošanai, regulējuma nepilnību novēršanai un digitālās vides sagatavošanai nākotnes problēmu pārvarēšanai. Stratēģijā ir ieteikta sadarbīga un saskanīga pieeja, kas paredz politikas reformas balstīt uz esošo regulējumu, vienlaikus pielāgojoties jaunajai realitātei tehnoloģiju jomā. Īstenojot ierosinātos pasākumus, ES tiecas nodrošināt noturīgu, konkurētspējīgu un ilgtspējīgu digitālo ekonomiku.