Eiropas Savienības
Padome

Briselē, 2022. gada 29. martā
(OR. en)

Starpiestāžu lieta:
2022/0084(COD)

7670/22
ADD 7

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

PAVADVĒSTULE

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2022. gada 22. marts
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN*
K-jas dok. Nr.:	SWD(2022) 65 final
Temats:	KOMISIJAS DIENESTU DARBA DOKUMENTS IETEKMES ANALĪZES ZIŅOJUMA KOPSAVILKUMS Pavaddokuments dokumentam Priekšlikums Eiropas Parlamenta un Padomes regulai par informācijas drošību Savienības iestādēs, struktūrās, birojos un aģentūrās

Pielikumā ir pievienots dokuments SWD(2022) 65 *final*.

Pielikumā: SWD(2022) 65 *final*

EIROPAS
KOMISIJA

Briselē, 22.3.2022.
SWD(2022) 65 final

KOMISIJAS DIENESTU DARBA DOKUMENTS

IETEKMES ANALĪZES ZIŅOJUMA KOPSAVILKUMS

Pavaddokuments dokumentam

Priekšlikums Eiropas Parlamenta un Padomes regulai

par informācijas drošību Savienības iestādēs, struktūrās, birojos un aģentūrās

{COM(2022) 119 final} - {SWD(2022) 66 final}

Kopsavilkums

Ietekmes analīze par informācijas drošību Savienības iestādēs, struktūrās, birojos un aģentūrās

A. Politiskais konteksts

Eiropadomes Stratēģiskajā programmā 2019.–2024. gadam iestādes tiek aicinātas aizsargāt ES informācijas un sakaru tīklus un tās lēmumu pieņemšanas procesus no visu veidu ļaunprātīgām darbībām, tostarp no kiberdraudiem un hibrīddraudiem. Tāpēc Vispārējo lietu padome 2019. gada decembrī secināja, ka ES iestādēm un struktūrām būtu jāizstrādā un jāīsteno visaptverošs pasākumu kopums savas informācijas drošības nostiprināšanai.

Komisija 2020. gada jūlijā pieņēma ES Drošības savienības stratēģiju, ar kuru tā apņēmās papildināt valstu centienus drošības jomā. Šīs stratēģijas ietvaros Komisija ierosināja izveidot minimālo noteikumu kopumu par informācijas drošību un kiberdrošību visās Savienības iestādēs un struktūrās (SIuS).

B. Problēmas būtība

Galvenās problēmas ir šādas: i) būtiskas drošības līmeņa atšķirības SIuS atkarībā no to iekšējiem informācijas drošības noteikumiem un ii) koordinācijas trūkums starp Savienības iestādēm un struktūrām, veicot savus drošības uzdevumus.

Savienības iestādēm un struktūrām pašlaik ir katrai savi informācijas drošības noteikumi, vai arī tās šādus noteikumus nav pieņēmušas vispār. Piemērojamā tiesiskā regulējuma sadrumstalotības sekas bija dažādas neklasificētas informācijas kategorijas, dažādi marķējumi un apstrādes instrukcijas visās jomās. Attiecībā uz ES klasificēto informāciju attiecīgo sistēmu sadarbspēja joprojām ir ierobežota, un tas liedz netraucēti pārsūtīt informāciju starp iestādēm un struktūrām un ar dalībvalstīm.

Šī situācija paaugstina risku, ka uzbrucēji varētu radīt drošības pārkāpumu visvājākajā posmā un izmantot to kā sākumpunktu turpmākiem uzbrukumiem citām iestādēm vai struktūrām.

C. Sasniedzamie mērķi

Iniciatīvas vispārīgais mērķis ir izveidot informācijas drošības noteikumus visām Savienības iestādēm un struktūrām, lai nodrošinātu pastiprinātu un konsekventu aizsardzību pret mainīgiem draudiem to informācijai.

Vispārējais mērķis ir izteikts četros konkrētos mērķos:

- ieviest saskaņotas un visaptverošas informācijas kategorijas;
- apzināt drošības trūkumus un īstenot nepieciešamos pasākumus;
- izveidot vienkāršu sadarbību starp Savienības iestādēm un struktūrām informācijas drošības jomā;
- modernizēt informācijas drošības politiku, ņemot vērā digitālo pārkārtošanos un tāldarbu.

D. Dažādo ieinteresēto personu viedokļi

Ieinteresētās personas, ar kurām notika apspriešanās (Savienības iestādes un struktūras, dalībvalstu valsts drošības iestādes un *JRC* pētniecības eksperti), vienojās, ka visām Savienības iestādēm un struktūrām ir

vajadzīgi kopīgi informācijas drošības standarti, koncentrējoties uz šādiem jautājumiem:

- būtu jāņem vērā SIuS daudzveidība un atšķirīgā darbības vide, un būtu jāpieļauj vietējs risinājums;
- lai gan lielākā daļa iestāžu un struktūru informācijas drošības nolūkos ir gatavas sadarboties ar kolēģiem kopējās struktūrās, tās nevēlas deleģēt savas lēmumu pieņemšanas pilnvaras;
- regulas projekts būtu jāizstrādā, ņemot vērā dalībvalstu starpvaldību nolīgumu[1] par klasificētas informācijas aizsardzību.

E. Priekšlikuma ietekme

Ieguvumi

Izveidojot informācijas drošības noteikumu pamatu visās Savienības iestādēs un struktūrās, regulas projekts palielinās vispārējo informācijas drošības līmeni, vienlaikus samazinot pašreizējās neatbilstības. Regulai būtu arī jāpalīdz novērst iespējamie vājie posmi, vienlaikus aizsargājot informāciju, ar ko apmainās Eiropas administrācija.

No efektivitātes viedokļa regulas projektam būtu jāveicina kopīgu informācijas drošības uzdevumu koordinēta izpilde (piemēram, pielaides, sakaru un informācijas sistēmu akreditācija) un kopīgu pārvaldības struktūru izveide (piemēram, starpiestāžu koordinācijas grupas, tehniskās apakšgrupas).

Ekonomiskā ietekme

Paredzams, ka centienus, kas vajadzīgi jauno tiesību aktu īstenošanai, Savienības iestādēm un struktūrām kompensēs efektivitātes pieaugums, savukārt papildu izmaksas var segt no katras organizācijas esošajām informācijas drošības uzlabošanas programmām. Ilgtermiņā tās gūs labumu no saskaņotas pieejas, risinot arvien pieaugošos draudus informācijas drošībai.

Eiropas Komisijai būtu jānodrošina Iestāžu koordinācijas grupas pastāvīgais sekretariāts un jāpiešķir šim uzdevumam cilvēkresursi (viens AD ierēdnis un viens AST ierēdnis).

Dalībvalstu pārvaldes iestāžu un privātā sektora līmenī nekāda ekonomiskā ietekme nav paredzama.

F. Turpmākie pasākumi

Politikas pārskatīšanas termiņš

Pilns izvērtējums, lai novērtētu regulas projekta ietekmi un īstenošanu, tiks veikts ik pēc pieciem gadiem, sākot no piemērošanas dienas. Komisija sagatavo ziņojumu ar saviem konstatējumiem un iesniedz to Eiropas Parlamentam un Padomei.

[1] Padomē sanākušo Eiropas Savienības dalībvalstu nolīgums par tādas klasificētās informācijas aizsardzību, ar kuru apmainās Eiropas Savienības interesēs, 2011/C202/05.