Consiliul
Uniunii Europene

Bruxelles, 29 martie 2022
(OR. en)

Dosar interinstituțional:
2022/0084 (COD)

7670/22
ADD 7

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	22 martie 2022
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2022) 65 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI care însoţeşte documentul Propunere de regulament al Parlamentului European și al Consiliului privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii

În anexă, se pune la dispoziția delegațiilor documentul SWD(2022) 65 final.

Anexă: SWD(2022) 65 final

COMISIA
EUROPEANĂ

Bruxelles, 22.3.2022
SWD(2022) 65 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI

care însoţeşte documentul

Propunere de regulament al Parlamentului European și al Consiliului

privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii

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

Fișă rezumat

Evaluare a impactului privind securitatea informațiilor în instituțiile, organele, oficiile și agențiile Uniunii

A. Contextul politic

În Agenda strategică a Consiliului European pentru perioada 2019-2024 se solicită instituțiilor să protejeze rețelele de informații și comunicații ale UE și procesele sale decizionale de toate tipurile de activități răuvoitoare, inclusiv amenințările cibernetice și hibride. În consecință, Consiliul Afaceri Generale din decembrie 2019 a concluzionat că instituțiile și organele UE ar trebui să elaboreze și să pună în aplicare un set cuprinzător de măsuri pentru a asigura securitatea informațiilor.

În iulie 2020, Comisia a adoptat Strategia UE privind o uniune a securității, prin care s-a angajat să completeze eforturile naționale în domeniul securității. Ca parte a acestei strategii, Comisia a propus crearea unui set minim de norme privind securitatea informațiilor și securitatea cibernetică în toate instituțiile și organele Uniunii (IOU).

B. Care este problema?

Principalele probleme sunt: i) diferența semnificativă dintre nivelul de securitate al IOU în funcție de normele lor interne de securitate a informațiilor și ii) lipsa de coordonare între instituțiile și organele Uniunii în ceea ce privește îndeplinirea sarcinilor lor în materie de securitate.

Instituțiile și organele Uniunii au în prezent propriile norme de securitate a informațiilor sau nu au adoptat deloc astfel de norme. Fragmentarea cadrului juridic aplicabil a condus la existența unor categorii diferite de informații neclasificate, precum și a unor marcaje și instrucțiuni de manipulare diferite în toate domeniile. În ceea ce privește informațiile clasificate ale UE, interoperabilitatea sistemelor relevante rămâne limitată, împiedicând transferul continuu de informații între instituții și organe și cu statele membre.

Această situație conduce la un risc sporit ca atacatorii să creeze o încălcare a securității în veriga cea mai slabă și să utilizeze acest lucru ca punct de plecare pentru noi atacuri asupra altor instituții sau organe.

C. Ce ar trebui realizat?

Obiectivul general al inițiativei este de a crea norme de securitate a informațiilor pentru toate instituțiile și organele Uniunii, cu scopul de a asigura o protecție sporită și coerentă împotriva amenințărilor în continuă evoluție la adresa informațiilor acestora.

Obiectivul general este transpus în patru obiective specifice:

- stabilirea unor categorii de informații armonizate și cuprinzătoare;
- identificarea lacunelor în materie de securitate și punerea în aplicare a măsurilor necesare;
- instituirea unei cooperări simplificate în materie de securitate a informațiilor între instituțiile și organele Uniunii;
- modernizarea politicilor în domeniul securității informațiilor, ținând seama de transformarea digitală și de munca la distanță.

D. Care sunt opiniile diferitelor părți interesate?

Părțile interesate consultate (instituțiile și organele Uniunii, autoritățile naționale de securitate ale statelor membre și experții în cercetare din cadrul JRC) au convenit asupra necesității unor standarde comune în materie de securitate a informațiilor pentru toate instituțiile și organele Uniunii, punând accentul pe următoarele aspecte:

- ar trebui să se țină seama de diversitatea și de diferitele medii de lucru ale fiecărei IOU și ar trebui permisă găsirea unei soluții locale;
- deși majoritatea instituțiilor și organelor sunt pregătite să coopereze cu omologii lor din cadrul organismelor comune în scopuri de securitate a informațiilor, acestea nu sunt dispuse să își delege competențele decizionale;
- proiectul de regulament ar trebui elaborat în conformitate cu acordul interguvernamental[1] între statele membre privind protecția informațiilor clasificate.

E. Care este impactul propunerii?

Beneficii

Prin crearea unui nivel de referință al normelor de securitate a informațiilor la nivelul instituțiilor și organelor Uniunii, proiectul de regulament va spori nivelurile generale de securitate a informațiilor, reducând, în același timp, discrepanțele actuale. Aceasta ar trebui, de asemenea, să contribuie la eliminarea eventualelor verigi slabe, protejând, în același timp, informațiile partajate în cadrul administrației europene.

Din punctul de vedere al eficienței, proiectul de regulament ar trebui să genereze beneficii prin îndeplinirea coordonată a sarcinilor comune în materie de securitate a informațiilor (de exemplu, autorizări, acreditarea sistemelor informatice și de comunicații) și prin crearea unor organisme comune de guvernanță (de exemplu, Grupul de coordonare interinstituțională, subgrupurile tehnice).

Impacturi economice

Pentru instituțiile și organele Uniunii, se preconizează că eforturile necesare pentru punerea în aplicare a noii legislații vor fi compensate de creșterea eficienței, în timp ce costurile suplimentare pot fi acoperite în cadrul programelor existente de îmbunătățire a securității informațiilor ale fiecărei organizații. Pe termen lung, acestea vor avea de câștigat de pe urma abordării coerente a amenințărilor în continuă evoluție la adresa securității informațiilor.

Comisia Europeană ar trebui să asigure secretariatul permanent al Grupului de coordonare interinstituțională și să aloce resurse umane pentru această sarcină (un funcționar AD și un funcționar AST).

Nu se preconizează niciun impact economic la nivelul administrațiilor statelor membre și al sectorului privat.

[1] Acord între statele membre ale Uniunii Europene, reunite în cadrul Consiliului, privind protecția informațiilor clasificate schimbate în interesul Uniunii Europene, 2011/C202/05.

F. Măsuri ulterioare
Când va fi revizuită politica?
O evaluare completă va fi efectuată o dată la 5 ani de la data aplicării, pentru a evalua impactul și punerea în aplicare a proiectului de regulament. Comisia prezintă un raport care include constatările sale și îl transmite Parlamentului European și Consiliului.