Consiliul
Uniunii Europene

Bruxelles, 22 ianuarie 2026
(OR. en)

5611/26
ADD 2

Dosare interinstituționale:
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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	21 ianuarie 2026
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	SWD(2026) 12 final
Subiect:	DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI […] care însoțește documentele Propunere de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2) și Propunere de directivă a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2022/2555 în ceea ce privește măsurile de simplificare și alinierea la [Propunerea de regulament privind securitatea cibernetică 2]

În anexă, se pune la dispoziția delegațiilor documentul SWD(2026) 12 final.

Anexă: SWD(2026) 12 final

COMISIA
EUROPEANĂ

Strasbourg, 20.1.2026
SWD(2026) 12 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL RAPORTULUI PRIVIND EVALUAREA IMPACTULUI

[…]

care însoțește documentele

Propunere de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881 (Regulamentul privind securitatea cibernetică 2)

și

Propunere de directivă a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2022/2555 în ceea ce privește măsurile de simplificare și alinierea la [Propunerea de regulament privind securitatea cibernetică 2]

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

Rezumatul evaluării impactului

Obiectiv

Obiectivul principal al prezentei evaluări a impactului este de a analiza caracterul adecvat al reglementărilor în vigoare din perspectiva modului în care acestea abordează amenințările în continuă evoluție la adresa securității cibernetice în întreaga UE. Documentul propune un set integrat de opțiuni de politică menite să consolideze mandatul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), să reformeze Cadrul european de certificare a securității cibernetice (ECCF) și să simplifice respectarea cadrului legislativ existent în domeniul securității cibernetice. Evaluarea subliniază importanța modulării guvernanței cibernetice pentru a o armoniza cu progresele tehnologice și cu cererile pieței, asigurând în același timp competitivitatea și luând în considerare impacturile asupra mediului.

Definirea problemei

În pofida eforturilor care s-au depus, peisajul securității cibernetice al UE se confruntă în continuare cu provocări semnificative în contextul unor amenințări din ce în ce mai complexe. Coordonarea insuficientă între statele membre și alți actori de la nivelul UE, întârzierile în aplicarea instrumentelor de politică, obstacolele în materie de reglementare și complexitatea reglementărilor împiedică gestionarea eficientă a securității cibernetice. Aceste probleme generează costuri mai mari pentru întreprinderi și autoritățile publice, presupun un risc sporit de incidente cibernetice și creează niveluri inegale de protecție pentru cetățeni.

Justificarea acțiunii UE

Amenințările la adresa securității cibernetice depășesc frontierele naționale, astfel că o abordare unificată rămâne cheia unui răspuns eficient. O intervenție la nivelul UE asigură o protecție consecventă, sporește competitivitatea prin asigurarea unor condiții de concurență echitabile și facilitează libera circulație a serviciilor și produselor digitale în cadrul pieței unice. Armonizarea la nivelul UE reduce, de asemenea, sarcinile administrative prin simplificarea procesului de respectare a legislației și raționalizarea procedurilor.

Opțiuni de politică și opțiunea preferată

Raportul analizează patru domenii de intervenție, fiecare cu un set de opțiuni de politică care au fost analizate din perspectiva obiectivelor specifice care trebuie atinse: (1) mandatul ENISA (stabilit și în Regulamentul privind securitatea cibernetică în vigoare); (2) ECCF (reglementat și în Regulamentul privind securitatea cibernetică în vigoare) și (3) modificări specifice ale Directivei NIS 2, care vizează simplificarea și care sunt totodată interconectate cu mandatul ENISA și cu ECCF. Fiecare dintre aceste seturi de opțiuni constituie, în sine, un domeniu de intervenție, fiind în același timp interconectate și relevante unul pentru celelalte.

Opțiuni de abordare a neconcordanței dintre cadrul de politică al UE în materie de securitate cibernetică și nevoile părților interesate într-un mediu din ce în ce mai ostil

Opțiunea A.1: *Clarificarea mandatului ENISA și stabilirea priorităților* – Această opțiune ar urma să asigure un cadru clar și stabil pentru sarcinile ENISA prin încorporarea sarcinilor stabilite de alte acte legislative.

Opțiunea A.2: *Reformarea mandatului ENISA* – Această opțiune ar urma să abroge și să înlocuiască Regulamentul privind securitatea cibernetică, ceea ce ar implica o revizuire cuprinzătoare a mandatului agenției.

Opțiunea A.3: *Reformarea mandatului ENISA, cu un accent puternic pe sprijinul operațional* – Această opțiune s-ar baza pe opțiunea A.2 și ar presupune, în plus, ca ENISA să dezvolte capacități pentru a sprijini direct entitățile prevăzute de Directiva NIS 2 în a răspunde la incidentele de securitate cibernetică și a se redresa în urma acestora, la cererea unui stat membru.

Opțiuni pentru cadrul european de certificare a securității cibernetice

Opțiunea B.1: *Clarificarea domeniului de aplicare, a elementelor și a obiectivelor ECCF și introducerea unui mecanism de întreținere a sistemelor* – Această opțiune ar urma să prevadă un nou mecanism de întreținere pentru sisteme, după adoptarea acestora, care să fie pus în aplicare de ENISA.

Opțiunea B.2: *Reformarea ECCF prin revizuirea procedurilor aferente și extinderea domeniului său de aplicare pentru a facilita simplificarea respectării legislației* – Această opțiune ar presupune abrogarea Regulamentului privind securitatea cibernetică și înlocuirea lui cu un nou regulament. În plus față de opțiunea B.1, procedura legată de solicitarea, dezvoltarea și adoptarea sistemelor ar urma să fie revizuită pentru a îmbunătăți asumarea răspunderii și eficiența.

Opțiunea B.3: *Reformarea ECCF, astfel cum se prevede în cadrul opțiunii B.2, și introducerea certificării obligatorii pentru postura de securitate cibernetică* – Această opțiune s-ar baza pe opțiunea B.2, dar vizează să sporească și mai mult impactul cadrului prin introducerea obligativității certificării entităților esențiale care intră în domeniul de aplicare al Directivei NIS 2, analizând scenarii de risc specifice, în loc să se bazeze exclusiv pe certificarea voluntară a entităților.

Opțiuni de simplificare

Opțiunea C.1: *Adoptarea unei abordări bazate pe instrumente juridice neobligatorii și pe instrumente fără caracter legislativ, inclusiv utilizarea delegărilor de competențe existente [adoptarea de acte de punere în aplicare în temeiul articolului 21 alineatul (5) și al articolului 23 alineatul (11) din Directiva NIS 2]* – Această opțiune prevede adoptarea de acte de punere în aplicare în baza delegărilor de competențe existente în temeiul Directivei NIS 2 pentru a asigura un grad mai ridicat de armonizare a măsurilor de gestionare a riscurilor în materie de securitate cibernetică, a pragurilor de raportare a incidentelor, precum și a informațiilor, a formatelor și a procedurilor de notificare, împreună cu adoptarea unui set de orientări pentru a spori securitatea juridică și implementarea armonizată.

Opțiunea C.2: *Intervenție țintită – simplificarea în continuare a procesului de respectare a legislației relevante a Uniunii în materie de securitate cibernetică* – Această opțiune implică o intervenție limitată prin modificări ale Regulamentului privind securitatea cibernetică și ale Directivei NIS 2, cu scopul de a simplifica aspecte specifice ale cadrului de securitate cibernetică, inclusiv adaptări ale domeniului de aplicare, armonizarea maximă a actelor de punere în aplicare, dovada conformității prin certificare și adoptarea setului de orientări prevăzut în opțiunea C1.

Opțiunea C.3: *Armonizarea măsurilor legate de securitatea cibernetică prevăzute în legislația Uniunii* – Această opțiune s-ar baza pe opțiunea C.2 și ar elimina toate măsurile de gestionare a riscurilor în materie de securitate cibernetică și delegările de competențe în legătură cu astfel de măsuri incluse în legislația sectorială. În schimb, ecosistemul Directivei NIS 2 ar urma să fie modificat pentru a prevedea cerințe raționalizate pentru toate tipurile de entități, asigurându-se astfel un grad mai mare de armonizare.

Opțiuni pentru securitatea lanțului de aprovizionare TIC

Opțiunea D.1: *Adoptarea unei abordări bazate pe instrumente juridice neobligatorii pentru a aborda riscurile în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC* – Această opțiune nu ar prevedea o intervenție de reglementare la nivelul UE. În schimb, Comisia ar crește numărul evaluărilor coordonate ale riscurilor și al seturilor de instrumente voluntare.

Opțiunea D.2: *Intervenție de reglementare* ad-hoc *care codifică setul de instrumente pentru 5G* – Această opțiune ar presupune codificarea măsurilor din setul de instrumente pentru 5G. Aceasta ar introduce o obligație pentru statele membre de a se asigura că nu sunt utilizate componente de la furnizorii cu grad ridicat de risc în activele esențiale ale rețelei.

Opțiunea D.3: *Un cadru de reglementare cuprinzător și orizontal pentru abordarea riscurilor în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC* – Această opțiune ar institui un cadru de reglementare orizontal, neutru din punct de vedere tehnologic și sectorial pentru a aborda riscurile non-tehnice în materie de securitate cibernetică din lanțurile de aprovizionare TIC.

După analize ample, pachetul de politici preferat include: opțiunea A.2 - reformarea mandatului ENISA; opțiunea B.2 – reformarea ECCF prin revizuirea procedurii și extinderea domeniului său de aplicare pentru a facilita simplificarea procesului de respectare a legislației, opțiunea C.2 – intervenție țintită: simplificarea în continuare a procesului de respectare a legislației relevante a Uniunii în materie de securitate cibernetică și opțiunea D.3 – un cadru cuprinzător și orizontal pentru abordarea riscurilor în materie de securitate cibernetică la nivelul lanțurilor de aprovizionare TIC.

Această combinație oferă un răspuns echilibrat la provocările identificate în materie de politici, sporind în mod semnificativ eficacitatea, eficiența și coerența în întreaga UE.

Principalele impacturi

Analiza cost-beneficiu: Tranziția către cadrul de reglementare propus va genera costuri atât pentru ENISA – estimate la până la 161,3 milioane EUR pe o perioadă de cinci ani – pentru a-și îndeplini noile sarcini, cât și pentru autoritățile publice din întreaga UE – de până la 80 de milioane EUR pe o perioadă de cinci ani – pentru supraveghere (luând în considerare economiile de costuri relevante). În ceea ce privește întreprinderile, pe o perioadă de tranziție de cinci ani, eliminarea treptată a anumitor echipamente cu risc ridicat ar putea genera costuri anuale cuprinse între 3,4 și 4,3 miliarde EUR pentru operatorii de rețele de telefonie mobilă, în timp ce investițiile în furnizori de încredere ar putea crește simultan cu până la 2 miliarde EUR pe an. În plus, se preconizează că prin raționalizarea și simplificarea obligațiilor de conformare se vor stimula realizarea de economii de costuri pentru întreprinderi de până la 14,6 miliarde EUR. De asemenea, îmbunătățirea posturii de securitate cibernetică generală și a suveranității tehnologice a UE, precum și stimularea inovării și a competitivității ar urma să genereze beneficii semnificative pentru cetățeni, autoritățile publice și întreprinderi, beneficii care se preconizează că vor compensa în mare măsură, pe termen lung, cheltuielile inițiale.

Competitivitatea: Prin reducerea fragmentării pieței și armonizarea reglementărilor, opțiunile preferate sporesc egalitatea concurențială în întreaga UE, oferind întreprinderilor căi mai clare de conformare la cadrul legislativ și de stimulare a inovării.

Verificarea coerenței cu politicile climatice: Evaluarea a analizat impactul potențial al fiecărei opțiuni asupra mediului. S-a acordat o atenție deosebită eficienței energetice, emisiilor legate de călătorii și consolidării infrastructurii. Opțiunile preferate A.2, B.2 și C.2 au un impact limitat asupra mediului, în timp ce D.3 ține seama de neutralitatea din punctul de vedere al mediului, ținând cont de ciclul de viață al produsului și perioadele de tranziție pentru înlocuirea activelor esențiale. Acest lucru este în conformitate cu angajamentul UE privind dezvoltarea durabilă.

Digital în mod implicit: Faptul că propunerea pune accentul pe raționalizarea proceselor digitale demonstrează angajamentul UE față de o abordare de tipul „digitalizarea pe primul loc”, asigurând un schimb de date și un proces decizional mai rapide și mai fiabile. Opțiunea D.3 ar putea avea, de asemenea, un impact ridicat asupra digitalizării, deoarece ar implica înlocuirea componentelor de la entități stabilite în țări terțe sau controlate de entități din țări terțe ce prezintă motive de îngrijorare în materie de securitate cibernetică.

Simplificarea și reducerea sarcinii: Opțiunile preferate contribuie la simplificare prin introducerea unor clarificări ale domeniului de aplicare și a unor măsuri de raționalizare a procesului de respectare a legislației și de supraveghere, reducând sarcinile administrative. Se ține seama de principiul numărului constant, asigurându-se compensarea noilor obligații prin reduceri echivalente.

Concluzie

Prezenta evaluare a impactului prezintă o strategie cuprinzătoare de consolidare a securității cibernetice a UE, de abordare a ineficiențelor în materie de reglementare și de pregătire a

peisajului digital pentru provocările viitoare. Aceasta recomandă o abordare bazată pe colaborare și coeziune, care să fundamenteze reformele de politică pe cadrele existente, adaptându-le în același timp la noile realități tehnologice. Prin aceste măsuri, UE urmărește să asigure o economie digitală rezilientă, competitivă și durabilă.