Consiliul
Uniunii Europene

Bruxelles, 17 decembrie 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	11 decembrie 2025
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	C(2025) 8407 final
Subiect:	REGULAMENTUL DELEGAT (UE) …/… AL COMISIEI din 11.12.2025 de completare a Regulamentului (UE) 2024/2847 al Parlamentului European și al Consiliului prin specificarea termenelor și condițiilor de aplicare a motivelor legate de securitatea cibernetică în legătură cu întârzierea difuzării notificărilor

În anexă, se pune la dispoziția delegațiilor documentul C(2025) 8407 final.

Anexă: C(2025) 8407 final

COMISIA
EUROPEANĂ

Bruxelles, 11.12.2025
C(2025) 8407 final

REGULAMENTUL DELEGAT (UE) …/… AL COMISIEI

din 11.12.2025

de completare a Regulamentului (UE) 2024/2847 al Parlamentului European și al Consiliului prin specificarea termenelor și condițiilor de aplicare a motivelor legate de securitatea cibernetică în legătură cu întârzierea difuzării notificărilor

(Text cu relevanță pentru SEE)

EXPUNERE DE MOTIVE

1. CONTEXTUL ACTULUI DELEGAT

Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului („Regulamentul privind reziliența cibernetică”) impune producătorilor de produse cu elemente digitale să notifice, prin intermediul unei platforme unice de raportare, orice vulnerabilitate exploatată activ sau orice incident grav care are un impact asupra securității unui produs cu elemente digitale. În temeiul articolului 16 alineatul (2) din regulamentul respectiv, echipa de intervenție în caz de incidente de securitate informatică (CSIRT) desemnată de statul membru drept coordonator care a primit inițial notificarea poate, în circumstanțe excepționale și din motive justificate legate de securitatea cibernetică, să întârzie difuzarea notificării către CSIRT din alte state membre în care a fost pus la dispoziție produsul cu elemente digitale.

Prezentul act delegat este menit, așadar, să completeze Regulamentul privind reziliența cibernetică prin specificarea termenelor și condițiilor de aplicare a motivelor legate de securitatea cibernetică pentru întârzierea difuzării notificărilor. Acest lucru se realizează prin identificarea a trei tipuri de motive pentru care CSIRT care a primit inițial notificarea poate decide că este necesar să întârzie difuzarea ulterioară a acesteia către alte CSIRT. O astfel de decizie de întârziere poate fi luată în trei situații:

- în lumina unei evaluări a naturii informațiilor notificate;
- dacă CSIRT căreia ar trebui să i se difuzeze notificarea nu este în măsură să asigure confidențialitatea informațiilor respective;
- dacă platforma unică de raportare a fost compromisă sau este temporar neoperațională.

Obligațiile de raportare prevăzute la articolul 14 din Regulamentul (UE) 2024/2847 urmează să se aplice de la 11 septembrie 2026.

2. CONSULTĂRI PREALABILE ADOPTĂRII ACTULUI

Rețeaua CSIRT și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) au fost consultate cu privire la diverse proiecte ale prezentului act. La 26 martie 2025 a avut loc o discuție preliminară cu întrebări orientative, cu posibilitatea de a furniza contribuții scrise până la 11 aprilie 2025. Un prim proiect al prezentului act a fost transmis rețelei CSIRT și ENISA la 16 mai 2025, iar la 6 iunie 2025 a avut loc o discuție, cu posibilitatea de a furniza contribuții scrise până la 27 iunie 2025. Un al doilea proiect al prezentului act a fost transmis rețelei CSIRT și ENISA la 23 iulie 2025, cu posibilitatea de a furniza contribuții scrise până la 1 septembrie 2025. Un al treilea proiect al prezentului act a fost transmis rețelei CSIRT și ENISA la 25 septembrie 2025, iar la 9 octombrie 2025 a avut loc o discuție, cu posibilitatea de a furniza contribuții scrise până la 27 octombrie 2025.

Proiectul de act a făcut obiectul unei consultări publice în perioada 16 octombrie 2025-13 noiembrie 2025, la care s-au primit 34 de răspunsuri de la 31 de respondenți unici (aceste cifre reflectă faptul că un respondent a transmis feedback prin 4 contribuții diferite). 29,41 % din răspunsuri au fost primite de la asociații de întreprinderi, 26,47 % de la companii/întreprinderi, 17,65 % de la cetățeni ai UE, 14,71 % de la autorități publice, 5,88 %

de la organizații neguvernamentale (ONG-uri) și 5,88 % de la instituții academice/de cercetare[1].

La data de 22 octombrie, proiectul a fost discutat, de asemenea, cu Grupul de experți privind securitatea cibernetică a produselor cu elemente digitale (E03967), din care fac parte autorități ale statelor membre, ENISA, experți individuali numiți cu titlu personal și organizații în sensul larg al cuvântului (de exemplu companii, asociații, ONG-uri).

3. ELEMENTELE JURIDICE ALE ACTULUI DELEGAT

Competența de a adopta acte delegate este prevăzută la articolul 14 alineatul (9) din Regulamentul privind reziliența cibernetică, care impune Comisiei să specifice, până la 11 decembrie 2025, termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică în legătură cu întârzierea difuzării notificărilor.

[1] Aceste procente nu reflectă faptul că un respondent a transmis feedback prin 4 contribuții diferite.

REGULAMENTUL DELEGAT (UE) …/… AL COMISIEI

din 11.12.2025

de completare a Regulamentului (UE) 2024/2847 al Parlamentului European și al Consiliului prin specificarea termenelor și condițiilor de aplicare a motivelor legate de securitatea cibernetică în legătură cu întârzierea difuzării notificărilor

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică)[2], în special articolul 14 alineatul (9),

întrucât:

(1) În circumstanțe excepționale și, în special, la cererea producătorului și având în vedere nivelul de sensibilitate al informațiilor notificate și din motive justificate legate de securitatea cibernetică, echipa de intervenție în caz de incidente de securitate informatică (CSIRT) desemnată drept coordonator care a primit inițial notificarea unei vulnerabilități exploatate activ sau a unui incident grav care are un impact asupra securității unui produs cu elemente digitale („CSIRT care a primit inițial notificarea”) poate decide să întârzie pentru o perioadă de timp strict necesară difuzarea notificării prin intermediul platformei unice de raportare către CSIRT desemnate drept coordonatori pe teritoriul cărora producătorul care transmite notificarea a indicat că a fost pus la dispoziție produsul cu elemente digitale („CSIRT relevante”). Este necesar, așadar, să se stabilească termenele și condițiile de aplicare a motivelor menționate mai sus. În cazul în care se aplică astfel de motive, CSIRT care a primit inițial notificarea este autorizată să întârzie difuzarea acesteia către CSIRT relevante pentru o perioadă de timp strict necesară, dar nu este obligată să facă acest lucru. În temeiul articolului 16 alineatul (2) din Regulamentul (UE) 2024/2847, în cazul în care o CSIRT care a primit inițial notificarea decide să invoce astfel de motive, aceasta ar trebui să informeze imediat Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) cu privire la decizia sa de întârziere, la motivele pentru care a luat această decizie, precum și la momentul în care intenționează să difuzeze mai departe notificarea.

(2) În conformitate cu articolul 16 alineatul (2) al doilea paragraf din Regulamentul (UE) 2024/2847, termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică prevăzute în regulamentul menționat nu se aplică accesului ENISA la informațiile notificate. Accesul ENISA la informațiile notificate poate fi restricționat numai în circumstanțe excepționale: atunci când producătorul indică în notificarea sa

[2] JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

că este îndeplinită una dintre cele trei condiții menționate la articolul 16 alineatul (2) al treilea paragraf litera (a), (b) sau (c) din Regulamentul (UE) 2024/2847 și numai în ceea ce privește notificarea vulnerabilității în termen de 72 de ore menționată la articolul 14 alineatul (2) litera (b) din Regulamentul (UE) 2024/2847. În aceste cazuri, singurele informații care trebuie puse simultan la dispoziția ENISA sunt informațiile privind transmiterea unei notificări de către un producător, informații generale privind produsul cu elemente digitale, informații privind natura generală a exploatării și informații privind invocarea unor motive legate de securitate.

(3) Accesul la informațiile notificate permite CSIRT să aibă o imagine de ansamblu a mediului de securitate de pe teritoriul lor și să instituie măsuri de atenuare, sporind nivelul general de securitate cibernetică în Uniune. Prin urmare, aplicarea unor restricții suplimentare privind difuzarea notificărilor în lumina naturii informațiilor notificate ar trebui să fie posibilă numai în cazurile în care, având în vedere caracterul sensibil al informațiilor notificate, riscurile de securitate cibernetică rezultate din difuzarea ulterioară depășesc beneficiile în materie de securitate pentru Uniune, iar riscurile respective nu pot fi atenuate în mod adecvat prin introducerea de restricții privind gestionarea și partajarea ulterioară a notificării prin intermediul unor protocoale adecvate utilizate în cadrul rețelei CSIRT, cum ar fi protocolul „Traffic Light Protocol” (TLP) sau protocolul „Permissible Actions Protocol” (PAP). Acest lucru se poate întâmpla, de exemplu, în cazul în care un producător a informat CSIRT care a primit inițial notificarea că preconizează să furnizeze în scurt timp o măsură de atenuare (cum ar fi o corecție). De asemenea, acest lucru se poate întâmpla atunci când CSIRT care a primit inițial notificarea decide să partajeze numai părți dintr-o notificare, iar aceste părți sunt totuși suficiente pentru ca CSIRT relevante să se asigure că sunt în măsură să instituie măsuri adecvate de atenuare a riscurilor. În plus, pentru a încuraja cooperarea în ceea ce privește identificarea și divulgarea vulnerabilităților între producători, CSIRT și cercetătorii din domeniul securității, acest lucru se poate întâmpla și atunci când CSIRT acționează ca intermediar de încredere pentru o procedură în curs de divulgare coordonată a vulnerabilităților, astfel cum se menționează la articolul 12 alineatul (1) din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[3]. În acest caz, atunci când CSIRT decide să întârzie difuzarea unei notificări și în conformitate cu articolul 16 alineatul (6) din Regulamentul (UE) 2024/2847, CSIRT trebuie să o întârzie pentru o perioadă care nu depășește ceea ce este strict necesar și până când părțile implicate în divulgarea coordonată a vulnerabilităților își dau consimțământul pentru divulgarea respectivă.

(4) Informațiile incluse în notificare vor ajuta CSIRT să își îndeplinească sarcinile în contextul atenuării riscurilor și al gestionării incidentelor. Cu toate acestea, în cazuri rare, astfel de informații ar putea fi suficiente pentru a permite crearea unei tehnici de exploatare fără cercetări suplimentare, chiar și de către actori cu competențe și resurse limitate. Dacă actori răuvoitori ar avea acces la aceste informații, securitatea cibernetică a Uniunii ar fi puternic afectată, dată fiind ușurința exploatării. Acest lucru s-ar putea întâmpla, de exemplu, atunci când versiunea vulnerabilă a unui software diferă doar marginal de versiunile anterioare, nevulnerabile. În astfel de situații, în cazul în care consideră că riscurile de securitate cibernetică rezultate din difuzarea

[3] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80).

ulterioară nu pot fi atenuate în mod adecvat prin impunerea de restricții privind gestionarea și partajarea ulterioară, CSIRT care a primit inițial notificarea poate decide să întârzie difuzarea până când va fi disponibilă o măsură eficace de atenuare a riscurilor, cum ar fi o actualizare de securitate sau instrucțiuni pentru utilizatori.

(5) În cazul în care o CSIRT relevantă nu este în măsură să protejeze în mod adecvat informațiile notificate, informațiile sensibile ar putea fi accesate de actori răuvoitori, iar vulnerabilitățile ar putea fi exploatate în întreaga piață unică. Prin urmare, atunci când există motive serioase de îngrijorare cu privire la capacitatea unei CSIRT relevante de a asigura confidențialitatea informațiilor notificate, CSIRT care a primit inițial notificarea poate decide să întârzie difuzarea notificării numai către CSIRT relevantă respectivă până când vor fi fost disipate respectivele motive de îngrijorare. Acest lucru se poate întâmpla în situațiile în care o CSIRT relevantă a fost afectată de un incident de securitate cibernetică care îi reduce capacitatea de a funcționa în condiții securizate sau atunci când există dovezi ori informații că s-au detectat deficiențe semnificative ale capacităților CSIRT, cum ar fi constrângeri grave în materie de resurse care îi compromit capacitatea de a-și îndeplini funcțiile sau utilizarea unui software depășit sau vulnerabil.

(6) Pentru a împiedica accesul actorilor răuvoitori la informații sensibile, în cazul în care platforma unică de raportare instituită în temeiul articolului 16 din Regulamentul (UE) 2024/2847 a fost compromisă de un incident de securitate cibernetică, CSIRT care a primit inițial notificarea ar trebui să întârzie difuzarea prin intermediul platformei unice de raportare până la restabilirea capacității platformei de a asigura confidențialitatea informațiilor notificate.

(7) În conformitate cu articolul 16 alineatul (2) primul paragraf din Regulamentul (UE) 2024/2847, CSIRT care a primit inițial notificarea nu trebuie să difuzeze o notificare către nicio altă CSIRT relevantă dacă producătorul indică faptul că produsul cu elemente digitale este pus la dispoziție numai pe piața statului membru al CSIRT care a primit inițial notificarea.

(8) Comisia a consultat și a solicitat opiniile părților interesate relevante în cursul pregătirii proiectului de act delegat și a consultat Grupul de experți privind securitatea cibernetică a produselor cu elemente digitale.

(9) În conformitate cu articolul 14 alineatul (9) din Regulamentul (UE) 2024/2847, Comisia a cooperat strâns cu rețeaua CSIRT instituită în temeiul articolului 15 din Directiva (UE) 2022/2555 și cu ENISA la pregătirea proiectului de act delegat,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Obiect

Prezentul regulament specifică termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică menționate la articolul 16 alineatul (2) din Regulamentul (UE) 2024/2847 care permit CSIRT desemnate drept coordonator care a primit inițial o notificare în conformitate cu articolul 14 alineatele (1) și (3) și cu articolul 15 alineatele (1) și (2) din regulamentul respectiv să întârzie difuzarea notificării către CSIRT desemnate drept coordonatori pe teritoriul cărora producătorul a indicat că a fost pus la dispoziție produsul cu elemente digitale.

Articolul 2

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „CSIRT care a primit inițial notificarea” înseamnă CSIRT desemnată drept coordonator care a primit inițial notificarea în conformitate cu articolul 14 alineatele (1) și (3) și cu articolul 15 alineatele (1) și alineatul (2) din Regulamentul (UE) 2024/2847;

(2) „CSIRT relevantă” înseamnă CSIRT desemnată drept coordonator pe teritoriul căreia producătorul a indicat că a fost pus la dispoziție produsul cu elemente digitale.

Articolul 3

Termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică care decurg din natura informațiilor raportate

CSIRT care a primit inițial notificarea poate decide să întârzie, pentru o perioadă de timp limitată la strictul necesar, difuzarea notificărilor sau a unor părți ale acestora către CSIRT relevante în cazurile în care, având în vedere caracterul sensibil al informațiilor notificate, riscurile de securitate cibernetică pe care le prezintă difuzarea depășesc beneficiile sale în materie de securitate, iar riscurile respective nu pot fi atenuate prin introducerea de restricții privind gestionarea sau partajarea ulterioară a notificării prin protocoale adecvate, cum ar fi „Traffic Light Protocol” (TLP) sau „Permissible Actions Protocol” (PAP), și în cazul în care este îndeplinită cel puțin una dintre următoarele condiții:

(a) producătorul a informat CSIRT care a primit inițial notificarea că se preconizează punerea la dispoziție, în termen de 72 de ore, a unei măsuri eficace de atenuare a riscurilor, cum ar fi o actualizare de securitate sau instrucțiuni pentru utilizatori; dacă în acest interval de timp nu este pusă la dispoziție o măsură eficace de atenuare a riscurilor, CSIRT care a primit inițial notificarea difuzează notificarea către CSIRT relevante;

(b) având în vedere natura vulnerabilității exploatate activ notificate, informațiile incluse în notificare sunt considerate suficiente pentru a crea o tehnică de exploatare, în special atunci când vulnerabilitatea poate fi identificată și exploatată cu ușurință de actori cu competențe și resurse limitate; odată ce este pusă la dispoziție o măsură eficace de atenuare a riscurilor, cum ar fi o actualizare de securitate sau instrucțiuni pentru utilizatori, CSIRT care a primit inițial notificarea difuzează notificarea către CSIRT relevante;

(c) CSIRT care a primit inițial notificarea este în măsură să comunice CSIRT relevante informații suficiente pentru a se asigura că CSIRT relevante pot institui măsuri adecvate de atenuare a riscurilor; odată ce este pusă la dispoziție o măsură eficace de atenuare a riscurilor, cum ar fi o actualizare de securitate sau instrucțiuni pentru utilizatori, CSIRT care a primit inițial notificarea difuzează notificarea integrală către CSIRT relevante;

(d) CSIRT care a primit inițial notificarea vulnerabilității exploatate activ a fost informată cu privire la aceasta în cadrul unei divulgări coordonate a vulnerabilităților pentru care CSIRT respectivă acționează ca intermediar de încredere în conformitate cu articolul 12 alineatul (1) din Directiva (UE) 2022/2555; într-un astfel de caz și în conformitate cu articolul 16 alineatul (6) din Regulamentul (UE) 2024/2847, CSIRT care a primit inițial notificarea difuzează notificarea către CSIRT relevante atunci

când întârzierea difuzării nu mai este strict necesară și când părțile implicate în divulgarea coordonată a vulnerabilităților și-au dat consimțământul pentru divulgare.

Articolul 4

Termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică în raport cu o anumită CSIRT

CSIRT care a primit inițial notificarea poate decide să întârzie pentru o perioadă de timp strict necesară difuzarea notificărilor sau a unor părți ale acestora către o anumită CSIRT relevantă în cazurile în care:

(a) CSIRT relevantă a fost afectată de un incident de securitate cibernetică care pune sub semnul întrebării capacitatea sa de a asigura confidențialitatea informațiilor notificate;

(b) aceasta are motive suficiente să creadă că CSIRT relevantă nu are capacități adecvate pentru a asigura confidențialitatea informațiilor notificate.

În cazurile menționate la primul paragraf litera (a), CSIRT care a primit inițial notificarea poate întârzia difuzarea până când CSIRT relevantă informează rețeaua CSIRT menționată la articolul 15 din Directiva 2022/2555 că a fost restabilită capacitatea sa de a asigura confidențialitatea notificărilor.

În cazurile menționate la primul paragraf litera (b), CSIRT care a primit inițial notificarea poate întârzia difuzarea către CSIRT relevantă până când CSIRT respectivă furnizează dovezi că a remediat deficiențele identificate.

Articolul 5

Termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică în raport cu platforma unică de raportare

CSIRT care a primit inițial notificarea poate decide să întârzie difuzarea notificărilor prin intermediul platformei unice de raportare instituite prin articolul 16 din Regulamentul (UE) 2024/2847 atunci când ENISA a informat rețeaua CSIRT, în conformitate cu articolul 16 alineatul (4) din regulamentul respectiv, că platforma unică de raportare a fost afectată de un incident de securitate cibernetică care pune sub semnul întrebării capacitatea sa de a asigura confidențialitatea informațiilor notificate. În astfel de cazuri, CSIRT care a primit inițial notificarea poate întârzia difuzarea prin intermediul platformei unice de raportare până când ENISA informează rețeaua CSIRT că a fost restabilită capacitatea platformei de a asigura confidențialitatea notificărilor.

Articolul 6

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 11.12.2025

Pentru Comisie
Președinta
Ursula VON DER LEYEN