COMISIA
EUROPEANĂ

Strasbourg, 20.1.2026
COM(2026) 13 final

2026/0012 (COD)

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]

{SWD(2026) 11-12} - {SEC(2026) 11}

(Text cu relevanță pentru SEE)

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Prezenta propunere face parte dintr-un pachet de măsuri care vizează alinierea cadrului de securitate cibernetică al Uniunii la nevoile părților interesate într-un peisaj din ce în ce mai sofisticat al amenințărilor cibernetice și într-o realitate geopolitică complexă. Entitățile esențiale și importante din sectoarele critice sunt vizate din ce în ce mai mult de atacurile cibernetice[1], în timp ce actorii care reprezintă amenințări la adresa statului valorifică tehnologiile emergente, cum ar fi inteligența artificială (IA), pentru a-și extinde și optimiza în continuare atacurile. În acest context, reziliența infrastructurii critice în fața amenințărilor cibernetice este recunoscută ca un pilon strategic pentru democrațiile noastre și pentru securitatea economică a Uniunii. Atât Strategia europeană privind o uniune a pregătirii[2], cât și Strategia europeană de securitate internă (ProtectEU)[3] au plasat securitatea cibernetică în centrul agendei Uniunii privind reziliența. În mod similar, Comunicarea privind consolidarea securității economice a UE[4] identifică drept obiective prioritare prevenirea accesului la informații și date sensibile care ar putea submina securitatea economică a Uniunii și prevenirea și atenuarea perturbărilor infrastructurii critice a Uniunii care afectează economia Uniunii, iar în cadrul acestora măsurile eficace de securitate cibernetică joacă un rol esențial. În plus, raportul privind viitorul competitivității europene a subliniat că necesitatea de a spori securitatea și de a reduce dependențele este unul dintre principalele domenii de acțiune necesare în Uniune[5]. În comunicarea sa intitulată „O Europă mai simplă și mai rapidă”[6], Comisia și-a anunțat angajamentul față de un program ambițios de promovare a unor politici inovatoare și orientate spre viitor care să consolideze competitivitatea Uniunii și să ușureze sarcinile de reglementare pentru cetățeni, întreprinderi și administrații, menținând, în același timp, cel mai înalt standard în ceea ce privește promovarea valorilor sale.

În acest context, prezenta propunere de directivă de modificare a Directivei (UE) 2022/2555 în ceea ce privește măsurile de simplificare și alinierea la [Propunerea 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)] urmărește să abordeze problema complexității și a diversității politicilor legate de securitatea cibernetică care au un impact asupra posturii de securitate cibernetică a Uniunii, în special prin introducerea de clarificări și prin facilitarea conformității pentru entitățile reglementate.

Ar trebui să se considere că obiectivul prezentei directive face parte din obiectivele generale ale pachetului de revizuire a Regulamentului privind securitatea cibernetică, care implică propunerea de regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a

---

1 ENISA, *ENISA Threat Landscape 2025* (Raportul privind situația amenințărilor pentru 2025).
2 JOIN(2025) 130 final.
3 COM(2025) 148 final.
4 JOIN(2025) 977 final.
5 Comisia Europeană, Viitorul competitivității europene, https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.
6 COM(2025) 47 final.

securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului (UE) 2019/881. Propunerea de regulament urmărește să abordeze: (i) neconcordanța dintre cadrul de politică al Uniunii în materie de securitate cibernetică și nevoile părților interesate într-un peisaj al amenințărilor din ce în ce mai ostil; (ii) stagnarea punerii în aplicare a cadrului european de certificare a securității cibernetice (ECCF); (iii) complexitatea și diversitatea politicilor legate de securitatea cibernetică care au un impact asupra posturii de securitate cibernetică a Uniunii și (iv) creșterea riscurilor la adresa securității lanțurilor de aprovizionare TIC. În ceea ce privește complexitatea și diversitatea politicilor legate de securitatea cibernetică care au un impact asupra poziției cibernetice a Uniunii, pachetul de revizuire a Regulamentului privind securitatea cibernetică propune – ca parte a unei reforme a cadrului european de certificare a securității cibernetice – să se promoveze certificarea ca instrument de asigurare a conformității pentru întreprinderi și să se permită dezvoltarea unui sistem privind postura de securitate cibernetică a entităților pentru a reduce costurile de asigurare a conformității pentru entitățile care fac obiectul Directivei NIS 2 și al altor acte legislative relevante ale Uniunii în materie de securitate cibernetică. Această abordare va simplifica în mod semnificativ obligațiile de reglementare pentru entitățile care fac obiectul mai multor cerințe de conformitate și va asigura o utilizare mai eficace a resurselor în rândul autorităților naționale.

Expunerea de motive a propunerii de Regulament privind securitatea cibernetică 2 prezintă aspectele esențiale care stau la baza propunerii, precum și obiectivele specifice pentru abordarea acestora. Propunerea de directivă va aborda obiectivul specific 4 (SPO4) al evaluării impactului revizuirii Regulamentului privind securitatea cibernetică, și anume stabilirea unor mecanisme și condiții care să contribuie la facilitarea respectării cerințelor în materie de securitate cibernetică și, în acest mod, la o punere în aplicare mai coerentă și mai eficace a acestora. Modificările specifice aduse Directivei NIS 2 vizează simplificarea respectării aspectelor specifice ale cadrului de securitate cibernetică și asigurarea unei puneri în aplicare raționalizate și coerente a acestora, inclusiv în ceea ce privește domeniul de aplicare, definițiile, raportarea privind atacurile de tip ransomware și supravegherea entităților care furnizează servicii transfrontaliere.

Propunerea de directivă de modificare a Directivei (UE) 2022/2555 privind măsurile de simplificare și alinierea la [Regulamentul privind securitatea cibernetică 2] intră în domeniul de aplicare al Programului privind o reglementare adecvată și funcțională (REFIT). Împreună cu revizuirea Regulamentului privind securitatea cibernetică, aceasta contribuie în mod semnificativ la îmbunătățirea clarității, la eliminarea ineficiențelor și la alinierea procedurilor la nivelul cadrelor juridice. Aceasta contribuie la buna funcționare a pieței interne, asigurând în același timp securitatea și autonomia strategică a Uniunii.

- **Coerența cu dispozițiile de politică deja existente în domeniul de politică vizat**

Uniunea și-a extins instrumentele juridice și de politică prin adoptarea unei serii de instrumente juridice și de măsuri de politică: (i) Directiva NIS 2 servește la consolidarea securității cibernetice pentru infrastructura critică; (ii) măsurile de securitate fizică sunt definite în „directiva conexă”, Directiva privind reziliența entităților critice; (iii) Regulamentul privind reziliența cibernetică sporește securitatea cibernetică a produselor; (iv) Regulamentul privind solidaritatea cibernetică creează capacități de răspuns la nivelul UE; (v) Planul de acțiune al UE în materie de securitate cibernetică[7] sprijină cooperarea la nivelul UE în materie de gestionare a crizelor; (vi) setul de instrumente pentru securitatea

[7] COM(2025) 66 final.

cibernetică a rețelelor 5G (setul de instrumente pentru rețelele 5G) sprijină securitatea cibernetică în rețelele 5G; (vii) planul de acțiune european privind securitatea cibernetică a spitalelor și a furnizorilor de servicii medicale[8] contribuie la îmbunătățirea securității cibernetice a acestora și (viii) Academia de competențe în materie de securitate cibernetică[9] abordează provocarea tot mai mare reprezentată de deficitul de talente în materie de securitate cibernetică.

Cadrul juridic în materie de securitate cibernetică menționat mai sus a fost completat de acte legislative sectoriale, și anume Regulamentul privind reziliența operațională digitală pentru sectorul financiar, codul de rețea privind normele sectoriale pentru aspectele de securitate cibernetică ale fluxurilor transfrontaliere de energie electrică pentru subsectorul energiei electrice, normele de securitate a informațiilor (Part-IS[10]) pentru subsectorul transportului aerian.

Prezenta propunere de directivă, la fel ca propunerea de regulament pe care o însoțește, face parte dintr-un set mai amplu de inițiative juridice și de politică adoptate de Uniune pentru a îmbunătăți reziliența entităților la amenințările cibernetice și la adresa securității. Aceasta se axează pe modificări specifice ale Directivei NIS 2, care vizează, printre altele, clarificarea anumitor aspecte privind domeniul de aplicare, definițiile și normele jurisdicționale, reducerea sarcinii de supraveghere a entităților esențiale și a entităților importante și facilitarea supravegherii entităților transfrontaliere prin consolidarea rolului ENISA în sprijinul cooperării operaționale. În plus, împreună cu propunerea de regulament, prezenta propunere creează o sinergie puternică care decurge din dezvoltarea certificării posturii de securitate cibernetică pentru Directiva NIS 2, precum și, eventual, pentru facilitarea respectării altor acte juridice relevante ale Uniunii, cum ar fi Regulamentul general privind protecția datelor (RGPD), fără a aduce atingere cerințelor lor specifice de certificare. Aceste măsuri de simplificare ar trebui să deblocheze resurse pentru a consolida pregătirea operațională în materie de securitate cibernetică a entităților din sectoarele critice ale Uniunii.

- **Coerența cu alte politici ale Uniunii**

Prezenta propunere consolidează cerințele de securitate pentru entitățile care furnizează portofele pentru întreprinderi, astfel cum sunt prevăzute în propunerea de regulament al Parlamentului European și al Consiliului de instituire a portofelelor europene pentru întreprinderi[11]. În plus, Comisia va asigura coerența cu inițiativele viitoare, cum ar fi Regulamentul privind rețelele digitale. Prezenta propunere este aliniată la propunerea de regulament privind simplificarea legislației digitale (Omnibus digital), care conține, printre altele, modificări ale Directivei NIS 2, împreună cu alte acte juridice ale Uniunii. Pachetul omnibus digital propune facilitarea respectării cerințelor de raportare în materie de securitate cibernetică, printre altele în temeiul Directivei NIS 2, prin raportarea prin intermediul unui punct de intrare unic pentru raportarea incidentelor, care urmează să fie dezvoltat și întreținut de ENISA. În plus, propunerea este aliniată la propunerea de regulament al

[8] COM(2025) 10 final.
[9] COM(2023) 207 final.
[10] Regulamentul de punere în aplicare (UE) 2023/203 al Comisiei și Regulamentul delegat (UE) 2022/1645 al Comisiei.
[11] COM(2025) 838 final.

Parlamentului European și al Consiliului privind siguranța, reziliența și sustenabilitatea activităților spațiale în Uniune[12].

În plus, propunerea este în concordanță cu raportul lui Mario Draghi privind viitorul competitivității europene, astfel cum s-a subliniat mai sus.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Temeiul juridic al prezentei directive este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), care urmărește să instituie și să asigure funcționarea pieței interne prin consolidarea măsurilor de apropiere a normelor de drept intern. Prezenta propunere modifică Directiva (UE) 2022/2555, care a fost adoptată în temeiul articolului 114 din TFUE.

• Subsidiaritatea (în cazul competențelor neexclusive)

Principiul subsidiarității impune obligația de a evalua necesitatea și valoarea adăugată a acțiunii Uniunii. Respectarea principiului subsidiarității în acest domeniu a fost deja recunoscută la adoptarea Directivei (UE) 2022/2555, care este modificată prin prezenta propunere.

Prezenta propunere facilitează respectarea legislației Uniunii în materie de securitate cibernetică, reducând costurile de asigurare a conformității și insecuritatea juridică pentru entitățile afectate și facilitând și îmbunătățind rata de conformitate cu cerințele de securitate cibernetică. Aceasta contribuie, de asemenea, la asigurarea unor condiții de concurență echitabile în ceea ce privește abordările în materie de supraveghere și de verificare a conformității în toate statele membre.

• Proporționalitatea

Normele propuse în prezenta directivă nu depășesc ceea ce este necesar pentru îndeplinirea obiectivelor specifice în mod satisfăcător. Alinierea și raționalizarea preconizate ale domeniului, ale măsurilor de securitate și ale obligațiilor de raportare au legătură cu solicitările statelor membre și ale întreprinderilor de îmbunătățire a cadrului actual.

• Alegerea instrumentului

Propunerea va modifica actuala Directivă NIS 2 și va raționaliza și mai mult obligațiile impuse întreprinderilor, asigurând astfel un nivel mai ridicat de armonizare în întreaga Uniune. Alegerea instrumentului juridic pentru prezenta propunere este în concordanță cu cea a textului juridic pe care îl modifică, și anume Directiva NIS 2. Prezenta propunere se bazează pe obiectivul Directivei NIS 2 de a oferi statelor membre flexibilitatea necesară pentru a ține seama de particularitățile naționale.

3. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

• Evaluările *ex post*/verificarea adecvării legislației existente

A se vedea expunerea de motive a [propunerii de regulament privind securitatea cibernetică 2].

[12] COM(2025) 335 final.

- **Consultarea cu părțile interesate**

A se vedea expunerea de motive a [propunerii de regulament privind securitatea cibernetică 2].

- **Obținerea și utilizarea cunoștințelor de specialitate**

A se vedea expunerea de motive a [propunerii de regulament privind securitatea cibernetică 2].

- **Evaluarea impactului**

A se vedea expunerea de motive, precum și raportul de evaluare a impactului care însoțește [propunerea de regulament privind securitatea cibernetică 2].

- **Adecvarea reglementărilor și simplificarea**

A se vedea expunerea de motive a [propunerii de regulament privind securitatea cibernetică 2].

- **Drepturile fundamentale**

A se vedea expunerea de motive a [propunerii de regulament privind securitatea cibernetică 2].

4. IMPLICAȚII BUGETARE

Vă rugăm să consultați fișa legislativă și financiară din [propunerea de regulament privind securitatea cibernetică 2].

5. ALTE ELEMENTE

- **Planurile de punere în aplicare și măsurile de monitorizare, evaluare și raportare**

În conformitate cu articolul 40 din Directiva NIS 2, Comisia va revizui funcționarea directivei și va prezenta un raport Parlamentului European și Consiliului o dată la 36 de luni.

- **Explicarea detaliată a dispozițiilor specifice ale propunerii**

Propunerea urmărește să faciliteze respectarea obligațiilor în materie de securitate cibernetică și să deblocheze resurse pentru a consolida pregătirea operațională în materie de securitate cibernetică a entităților din sectoarele critice ale Uniunii.

Propunerea introduce modificări specifice ale Directivei NIS 2 pentru a simplifica aspecte specifice ale cadrului de securitate cibernetică, pentru a spori securitatea juridică și pentru a armoniza punerea în aplicare.

Pentru a facilita demonstrarea de către entități și furnizori a conformității cu Directiva NIS 2, în conformitate cu propunerea de regulament pe care o însoțește prezenta propunere, entitățile reglementate de Directiva NIS 2 vor putea obține certificate în cadrul sistemelor organizaționale de certificare a securității cibernetice dezvoltate în cadrul ECCF.

Pentru a facilita și mai mult respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică pentru entitățile multinaționale care fac obiectul supravegherii de către autoritățile competente din mai multe state membre, ENISA i se încredințează un nou rol de sprijinire a statelor membre în supravegherea entităților respective, de facilitare a asistenței

reciproce și de creare a unei imagini de ansamblu mai bune a entităților care intră în domeniul de aplicare al Directivei NIS 2.

În plus, propunerea prevede adoptarea de către Comisie a unor orientări privind aplicarea cerințelor de securitate a lanțului de aprovizionare pe care entitățile care intră în domeniul de aplicare al Directivei NIS 2 le transferă furnizorilor lor, pentru a asigura securitatea juridică și a preveni transferul nejustificat al obligațiilor asupra entităților care nu intră în domeniul de aplicare al Directivei NIS 2.

Alte modificări specifice ale Directivei NIS 2 includ:

- clarificări privind domeniul de aplicare și definițiile;
- eliminarea din domeniul de aplicare a furnizorilor de servicii DNS de dimensiuni mici și foarte mici;
- introducerea unei armonizări maxime pentru actele de punere în aplicare în temeiul articolului 21 alineatul (5) (specificând măsurile de gestionare a riscurilor în materie de securitate cibernetică) pentru a facilita conformitatea entităților și supravegherea autorităților;
- introducerea unei noi categorii de întreprinderi mici cu capitalizare medie, în conformitate cu Recomandarea Comisiei din 2025 privind definiția întreprinderilor mici cu capitalizare medie[18]; entitățile care se califică drept întreprinderi mici cu capitalizare medie urmează să fie desemnate drept entități importante, reducându-le sarcina de asigurare a conformității și reducând sarcina de supraveghere pentru autoritățile competente;
- cerința ca statele membre să adopte politici de migrare către criptografia post-cuantică (PQC) ca parte a strategiei lor naționale de securitate cibernetică și
- introducerea unei colectări armonizate de date privind atacurile de tip ransomware.

2026/0012 (COD)

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]

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[1],

având în vedere avizul Comitetului Regiunilor[2],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[3] stabilește măsuri care vizează obținerea unui nivel comun ridicat de securitate cibernetică în Uniune, cu scopul de a îmbunătăți funcționarea pieței interne. De la intrarea în vigoare a Directivei (UE) 2022/2555, s-au înregistrat progrese semnificative în ceea ce privește creșterea nivelului de reziliență cibernetică în Uniune. În același timp, au apărut anumite provocări în cursul punerii în aplicare de către statele membre, inclusiv în ceea ce privește domeniul de aplicare al directivei, punerea în aplicare a obligațiilor de gestionare a riscurilor în materie de securitate cibernetică și de raportare a incidentelor și supravegherea entităților transfrontaliere. Pe baza [propunerii de regulament privind securitatea cibernetică 2], ar trebui aduse modificări specifice Directivei (UE) 2022/2555 pentru a aborda aceste provocări, prin simplificarea aspectelor specifice, cu scopul de a spori securitatea juridică și de a asigura punerea în aplicare uniformă a Directivei (UE) 2022/2555.

(2) Pentru a reduce sarcina de asigurare a conformității pentru entități și sarcina de supraveghere pentru autoritățile competente, în Directiva (UE) 2022/2555 ar trebui introdusă o nouă categorie de întreprinderi mici cu capitalizare medie, în conformitate

[1] JO C [...], [...], p. [...].

[2] JO C [...], [...], p. [...].

[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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

cu Recomandarea (UE) 2025/1099 a Comisiei[4]. Entitățile de tipul celor menționate în anexa I la Directiva (UE) 2022/2555, care se califică drept întreprinderi mici cu capitalizare medie în temeiul recomandării respective, ar trebui, ca regulă generală, să fie desemnate drept entități importante. În plus, pentru a sprijini obiectivul Comisiei de a reduce costurile administrative cu 25 % în total și cu 35 % pentru întreprinderile mici și mijlocii, furnizorilor de servicii din cadrul sistemului de nume de domenii ar trebui să li se aplice regula generală privind plafonarea dimensiunii prevăzută în Directiva (UE) 2022/2555, conform căreia toate entitățile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei[5] sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) de la articolul respectiv intră în domeniul de aplicare al Directivei (UE) 2022/2555.

(3) În cursul punerii în aplicare a Directivei (UE) 2022/2555, au existat provocări în ceea ce privește interpretarea dispozițiilor referitoare la domeniul său de aplicare. Prin urmare, anumite dispoziții legate de domeniul de aplicare privind furnizorii de servicii medicale, producătorii de energie electrică, întreprinderile din sectorul hidrogenului și entitățile din sectorul chimic ar trebui clarificate pentru a asigura securitatea juridică și a reduce sarcina de asigurare a conformității atât pentru entități, cât și pentru autoritățile naționale.

(4) Pentru a asigura proporționalitatea în ceea ce privește producătorii de energie electrică în sensul articolului 2 punctul 38 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului[6], numai producătorii de energie electrică cu o capacitate totală de producție de peste 1 MW ar trebui să fie considerați entități esențiale sau entități importante în temeiul Directivei (UE) 2022/2555, cu condiția să respecte regula privind plafonarea dimensiunii. Aceasta ar trebui să includă producătorii de energie electrică în cazul în care o singură instalație de producere a energiei electrice depășește 1 MW, precum și producătorii de energie electrică care exploatează mai multe instalații de producere care, împreună, au o capacitate de producție mai mare de 1 MW. O astfel de abordare permite un echilibru între necesitatea de a include entitățile în cazul cărora interferența cu rețeaua și sistemul lor informatic ar putea implica o pierdere, imposibilitate a controlului sau un control extern al capacității de producție care este relevantă în sine pentru securitatea și stabilitatea rețelei de energie electrică și necesitatea de a nu impune o sarcină administrativă disproporționată întreprinderilor în temeiul Directivei (UE) 2022/2555.

(5) Portofelele europene pentru identitatea digitală, astfel cum sunt prevăzute în Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[7], reprezintă o componentă esențială a infrastructurii digitale a Uniunii, care permite

---

4 Recomandarea (UE) 2025/1099 a Comisiei din 21 mai 2025 privind definiția întreprinderilor mici cu capitalizare medie (JO L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).

5 Recomandarea 2003/361/CE a Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36, ELI: http://data.europa.eu/eli/reco/2003/361/oj).

6 Directiva (UE) 2019/944 din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125; ELI: http://data.europa.eu/eli/dir/2019/944/oj).

7 Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

identificarea și autentificarea securizată și schimbul de documente electronice, inclusiv de atestări electronice ale atributelor. Având în vedere rolul lor esențial pentru public și pentru furnizarea de servicii publice și private, orice incident de securitate cibernetică care afectează portofelele respective ar putea avea un impact amplu. Pentru a asigura furnizarea serviciilor lor, furnizorii de portofele europene pentru identitatea digitală ar trebui să aibă obligația de a pune în aplicare măsuri tehnice, operaționale și organizatorice adecvate pentru a gestiona riscurile de securitate cibernetică, a preveni incidentele și a răspunde la acestea, precum și de a coopera cu autoritățile competente în conformitate cu Directiva (UE) 2022/2555. Prin urmare, aceștia ar trebui să fie incluși printre entitățile care intră sub incidența directivei respective, indiferent de dimensiunea lor, și să fie clasificați drept entități esențiale. Portofelele europene pentru întreprinderi oferă funcționalități și servicii similare adaptate nevoilor operatorilor economici și ale organismelor din sectorul public, pe baza cadrului UE pentru identitatea digitală, și sunt la fel de esențiale pentru securitatea și integritatea economiei digitale. În consecință, furnizorii de portofele europene pentru întreprinderi instituite în conformitate cu [Propunerea de regulament privind instituirea portofelelor europene pentru întreprinderi][8] ar trebui să facă obiectul acelorași cerințe și obligații în materie de securitate cibernetică ca furnizorii de portofele europene pentru identitatea digitală, pentru a asigura un nivel consecvent și ridicat de securitate în întregul ecosistem al identității digitale.

(6) Infrastructura submarină de transmitere a datelor include nu numai cablurile, ci și orice infrastructură legată de exploatarea acestora. O astfel de infrastructură include stațiile de debarcare și părțile terestre ale cablului submarin care se conectează la acestea, cum ar fi rutele terestre de la gura de vizitare de pe plajă până la stația de debarcare, centrul de date sau punctul de prezență. Infrastructura submarină de transmitere a datelor este exploatată, de obicei, de entități care intră deja sub incidența Directivei (UE) 2022/2555, inclusiv de furnizori de rețele și servicii publice de comunicații electronice sau de furnizori de servicii de cloud computing. Cu toate acestea, infrastructura submarină de transmitere a datelor poate fi exploatată și de alte tipuri de entități care nu intră în prezent în domeniul de aplicare al Directivei (UE) 2022/2555, cum ar fi infrastructura submarină de transmitere a datelor exploatată de furnizori de rețele de comunicații electronice care nu sunt publice sau de entități care concesionează exploatarea infrastructurii submarine de transmitere a datelor, integral sau parțial, furnizorilor de rețele publice de comunicații electronice. Având în vedere riscurile tot mai mari pentru infrastructura submarină de transmitere a datelor și caracterul lor critic ridicat care rezultă din acestea, este necesar să se asigure că toate tipurile de operatori de infrastructuri submarine de transmitere a datelor intră sub incidența Directivei (UE) 2022/2555. Alte infrastructuri critice maritime, cum ar fi cablurile electrice submarine, precum și conductele de gaze, hidrogen și petrol sunt, de regulă, deja reglementate de Directiva (UE) 2022/2555, deoarece sunt exploatate de operatorii de transport și de sistem din subsectoarele energiei electrice, gazelor, hidrogenului și petrolului.

(7) Pentru a permite entităților care furnizează servicii în mai multe state membre să beneficieze de abordări în materie de supraveghere mai coerente și mai puțin împovărătoare în întreaga piață internă, aceste entități ar trebui să fie în măsură să demonstreze respectarea obligațiilor specifice sau a tuturor obligațiilor de gestionare a riscurilor în materie de securitate cibernetică prevăzute în Directiva (UE) 2022/2555

[8] COM(2025) 838 final.

prin obținerea unui certificat privind postura de securitate cibernetică în cadrul unui sistem european de certificare a securității cibernetice. Dezvoltarea unui astfel de sistem va beneficia de adoptarea unor acte de punere în aplicare privind cerințele tehnice și metodologice, precum și cerințele sectoriale referitoare la măsurile de gestionare a riscurilor în materie de securitate cibernetică în temeiul Directivei (UE) 2022/2555, care se bazează pe o armonizare maximă.

(8) Având în vedere dependența tot mai mare a societății și a economiei noastre de tehnologiile digitale, este necesar să se ia măsuri de atenuare a amenințării cuantice. Posibilitatea unor atacuri de tipul „*harvest now - decrypt later*” (colectarea datelor în vederea decriptării ulterioare), care pot apărea deja în prezent, și riscurile viitoare induse de atacurile cuantice asupra falsificării semnăturilor, precum și eliminarea planificată a anumitor implementări ale algoritmilor și eliminarea completă a algoritmilor criptografici cu cheie publică actuali sporesc urgența inițierii de acțiuni pentru migrarea către criptografia post-cuantică (PQC). Prin urmare, statele membre ar trebui să aibă obligația de a adopta politici pentru migrarea către PQC ca parte a strategiei lor naționale de securitate cibernetică. Astfel de politici ar trebui să faciliteze accelerarea planificării strategice și crearea de măsuri și instrumente de sprijin pentru a evalua expunerea activelor criptografice la riscurile prezentate de calculatoarele cuantice. În plus, acestea ar trebui să contribuie la crearea unui plan de migrare și la testarea introducerii PQC în aplicațiile și rețelele digitale, promovând în același timp apariția și adoptarea unor soluții PQC europene verificate și evaluate în mod oficial, care să respecte cadrele de conformitate în ceea ce privește produsele și serviciile. Politicile respective ar trebui să se alinieze la obiectivele de etapă stabilite în actele juridice ale Uniunii și în politicile Uniunii, precum și la documentele adoptate de Grupul de cooperare NIS, în special la Foaia de parcurs coordonată pentru punerea în aplicare a tranziției către PQC, adoptată de Grupul de cooperare NIS în iunie 2025, realizând astfel migrarea către PQC până în 2030 pentru cazurile de utilizare critică și până în 2035 pentru cazurile de utilizare de nivel mediu și scăzut.

(9) În temeiul articolului 21 alineatul (2) litera (d) din Directiva (UE) 2022/2555, entitățile esențiale și entitățile importante trebuie să asigure un nivel adecvat de securitate a lanțului lor de aprovizionare. În practică, această obligație a determinat multe entități să solicite informații ample de la furnizorii lor prin intermediul unor chestionare, formate și procese eterogene. Deși astfel de cereri urmăresc să sprijine diligența necesară și gestionarea riscurilor, ele pot crea, de asemenea, o sarcină administrativă semnificativă pentru furnizorii entităților esențiale și ai entităților importante, în special atunci când informații similare trebuie furnizate în mod repetat sub forme diferite. Pentru a reduce această sarcină și pentru a promova o abordare coerentă, proporțională și eficientă a evaluărilor securității lanțului de aprovizionare, Comisia ar trebui să elaboreze orientări pentru a recomanda un nivel adecvat de detaliere, o structură și un format pentru aceste cereri de informații. Aceste orientări ar trebui să faciliteze armonizarea, să reducă suprapunerile inutile și să sprijine atât entitățile, cât și furnizorii acestora în respectarea efectivă a obligațiilor care le revin în temeiul Directivei (UE) 2022/2555.

(10) Atacurile de tip ransomware în care programele malware criptează date și sisteme și solicită o plată de răscumpărare pentru a le decripta rămân una dintre principalele amenințări la adresa entităților esențiale și importante. Armonizarea și îmbunătățirea colectării de date privind atacurile de tip ransomware de la entitățile esențiale și de la entitățile importante afectate ar oferi informații echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) și autorităților naționale, permițându-le să

se asigure că viitoarele intervenții de tip ransomware sunt adecvate și eficace, să sprijine entitățile în creșterea rezilienței lor și în prevenirea atacurilor viitoare, precum și să compileze informațiile și dovezile de care au nevoie agențiile de aplicare a legii pentru a perturba și a dezmembra grupurile care lansează atacuri de tip ransomware și pentru a sancționa agenții operativi ai acestora. Având în vedere caracterul potențial sensibil al informațiilor care urmează să fie partajate cu privire la atacurile de tip ransomware, în special dacă o entitate a plătit o răscumpărare și, în caz afirmativ, ce sumă și cui, astfel de informații ar trebui transmise numai echipelor CSIRT sau, după caz, autorităților competente, la cererea acestora. În scopul unui astfel de schimb de informații, entitățile esențiale și entitățile importante sunt încurajate să numească o persoană care să acționeze ca punct de contact și să asigure confidențialitatea și credibilitatea schimbului de informații. În contextul Inițiativei internaționale de combatere a atacurilor de tip ransomware, Uniunea a aprobat o declarație de politică internațională fără caracter obligatoriu prin care instituțiile relevante aflate sub autoritatea guvernelor naționale participante nu ar trebui să plătească cererile de extorcare de tip ransomware.

(11) Respectarea obligațiilor de raportare a informațiilor relevante cu privire la incidentele de tip ransomware nu ar trebui să conducă la impunerea unor obligații suplimentare în temeiul Directivei (UE) 2022/2555, la care entitatea nu ar fi fost supusă dacă nu ar fi raportat informațiile. În acest scop, în limitele ordinii lor juridice naționale, statele membre ar trebui să abordeze posibilele riscuri care decurg din răspunderea sporită legată de raportarea informațiilor relevante cu privire la incidentele de tip ransomware.

(12) Având în vedere dimensiunea transfrontalieră a multor entități esențiale și importante de pe piața internă și necesitatea de a asigura coerența și de a promova convergența și eficiența în ceea ce privește abordările în materie de supraveghere, ENISA ar trebui să sprijine statele membre în efectuarea asistenței reciproce pentru entitățile esențiale și entitățile importante care furnizează servicii în mai multe state membre sau care furnizează servicii în unul sau mai multe state membre și ale căror rețele și sisteme informatice sunt situate în unul sau mai multe alte state membre. În acest scop, statele membre ar trebui să transmită informații suplimentare registrului entităților ținut de ENISA. Pe baza informațiilor conținute în registrul entităților esențiale și al entităților importante, ENISA ar trebui să efectueze o analiză cuprinzătoare a riscurilor transfrontaliere în materie de securitate cibernetică legate de entitățile esențiale și de cele importante. Analiza ar trebui să se bazeze pe o metodologie elaborată împreună cu Comisia și cu Grupul de cooperare NIS. Metodologia respectivă ar putea ține seama de măsura în care entitățile esențiale și importante își implementează serviciile la nivel transfrontalier pe scară largă, se bazează pe servicii transfrontaliere, sunt expuse unui risc de concentrare la nivelul lanțului de aprovizionare, pot fi identificate ca sursă de risc de concentrare la nivelul lanțului de aprovizionare, sunt expuse unor incidente care ar putea avea efecte perturbatoare semnificative asupra serviciilor transfrontaliere sau se bazează pe rețele și sisteme informatice pentru furnizarea serviciilor lor, care sunt situate în diferite state membre și în afara Uniunii. Pe baza raportului de analiză a riscurilor, ENISA ar trebui să recomande autorităților competente relevante să înființeze echipe comune de examinare pentru a sprijini supravegherea entităților cu un grad mai ridicat de risc pentru buna funcționare a pieței interne în caz de incidente și să asiste autoritățile competente în executarea acțiunilor comune de supraveghere, la cererea acestora.

(13) Întrucât obiectivul prezentei directive, și anume simplificarea punerii în aplicare a măsurilor pentru un nivel comun ridicat de securitate cibernetică în Uniune, nu poate fi

realizat în mod satisfăcător de către statele membre, dar, având în vedere efectele acțiunii, poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezenta directivă nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(14) Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor au fost consultate în conformitate cu articolul 42 alineatul (2) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[9] și au emis un aviz comun la [data],

ADOPTĂ PREZENTA DIRECTIVĂ:

Articolul 1
Modificări aduse Directivei (UE) 2022/2555

Directiva (UE) 2022/2555 se modifică după cum urmează:

(1) Articolul 2 se modifică după cum urmează:

(a) la alineatul (2), litera (a) se modifică după cum urmează:

(i) punctul (iii) se înlocuiește cu următorul text:

„(iii) registrele de nume de domenii de prim nivel;”;

(ii) se adaugă următoarele puncte (iv) și (v):

„(iv) furnizorii de portofele europene pentru identitatea digitală, astfel cum se prevede în Regulamentul (UE) nr. 910/2014;

(v) furnizorii de portofele europene pentru întreprinderi instituite în conformitate cu Regulamentul (UE) [...]*.

_____

* Regulamentul (UE) [...] [Propunere de regulament privind instituirea portofelelor europene pentru întreprinderi].”;

(b) se introduce următorul alineat (3a):

„(3a) Indiferent de dimensiunea lor, prezenta directivă se aplică entităților identificate ca proprietari, administratori și operatori de infrastructuri strategice cu dublă utilizare în temeiul Regulamentului (UE) [...]**.

_____

** Regulamentul (UE) [...] [Propunere de regulament al Parlamentului European și al Consiliului de instituire a unui cadru de măsuri pentru facilitarea transportului de echipamente, bunuri și personal militar în întreaga Uniune].”

[9] Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

(2) Articolul 3 se modifică după cum urmează:

(a) alineatul (1) se modifică după cum urmează:

(i) literele (a) și (b) se înlocuiesc cu următorul text:

„(a) entitățile de tipul celor menționate în anexa I care depășesc plafoanele pentru întreprinderile mici cu capitalizare medie;

(b) prestatorii de servicii de încredere calificați, furnizorii de portofele europene pentru identitatea digitală, furnizorii de portofele europene pentru întreprinderi și de registre de nume de domenii de prim nivel, indiferent de dimensiunea acestora;”;

(ii) se adaugă următoarea literă (h):

„(h) entitățile identificate ca proprietari, administratori și operatori de infrastructuri strategice cu dublă utilizare în temeiul Regulamentului (UE) [...] [Propunere de regulament al Parlamentului European și al Consiliului de instituire a unui cadru de măsuri pentru facilitarea transportului de echipamente, bunuri și personal militar în întreaga Uniune].”;

(b) la alineatul (4), primul paragraf se înlocuiește cu următorul text:

„În scopul întocmirii listei menționate la alineatul (3), statele membre solicită entităților menționate la respectivul alineat să prezinte autorităților competente cel puțin următoarele informații:

(a) denumirea entității;

(b) sectorul, subsectorul relevant și tipul de entitate menționate în anexa I sau II, după caz;

(c) adresa entității sau, după caz, adresa sediului principal al entității și a celorlalte sedii legale ale sale din Uniune sau, dacă nu este stabilită în Uniune, adresa reprezentantului său desemnat în temeiul articolului 26 alineatul (3);

(d) datele de contact actualizate, inclusiv adresele de e-mail, numerele de telefon, identificatorul unic și adresele digitale ale portofelului european pentru întreprinderi al entității, după caz, și ale reprezentantului său desemnat în temeiul articolului 26 alineatul (3), după caz;

(e) statele membre în care entitatea furnizează servicii și

(f) gamele de adrese IP ale entității.”

(3) Articolul 5 se înlocuiește cu următorul text:

„*Articolul 5*

Armonizarea minimă

Fără a aduce atingere articolului 21 alineatul (5) al cincilea paragraf, prezenta directivă nu împiedică statele membre să adopte sau să mențină dispoziții care asigură un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.”

(4) La articolul 6,

se adaugă următoarele puncte 42 și 43:

„42. «întreprindere mică cu capitalizare medie» înseamnă o întreprindere mică cu capitalizare medie astfel cum este definită în anexa la Recomandarea (UE) 2025/1099 a Comisiei***;

(43) «infrastructură submarină de transmitere a datelor» înseamnă cabluri submarine care transmit date, infrastructura aferentă și alte instalații sau elemente asociate cu transmiterea datelor.

_____

*** Recomandarea (UE) 2025/1099 a Comisiei din 21 mai 2025 privind definiția întreprinderilor mici cu capitalizare medie (JO L, 2025/1099, 28.5.2025, ELI: http://data.europa.eu/eli/reco/2025/1099/oj).”

(5) La articolul 7 alineatul (2) se adaugă următoarea literă (k):

„(k) pentru tranziția către criptografia post-cuantică, ținând seama de termenele de tranziție și de cerințele relevante prevăzute în actele juridice și politicile aplicabile ale Uniunii.”

(6) La articolul 15 alineatul (2), prima teză se înlocuiește cu următoarea teză:

„Rețeaua echipelor CSIRT este formată din reprezentanți ai echipelor CSIRT desemnate sau instituite în temeiul articolului 10, din Centrul de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile Uniunii (CERT-UE) și ENISA.”

(7) Articolul 21 alineatul (5) se modifică după cum urmează:

(a) al doilea paragraf se înlocuiește cu următorul text:

„Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice și metodologice, precum și a cerințelor sectoriale, după caz, ale măsurilor menționate la alineatul (2) în ceea ce privește entitățile esențiale și entitățile importante, altele decât cele menționate la primul paragraf de la prezentul alineat. Comisia evaluează periodic dacă actele de punere în aplicare menționate la prezentul paragraf se adoptă pentru anumite sectoare sau tipuri de entități pentru a îmbunătăți funcționarea pieței interne. Atunci când pregătește aceste evaluări, Comisia se axează în special pe caracterul transfrontalier al sectoarelor sau al tipurilor de entități și desfășoară un proces de consultare deschis, transparent și cuprinzător cu părțile interesate relevante și cu statele membre.”;

(b) se adaugă următorul al cincilea paragraf:

„În cazul în care Comisia adoptă actele de punere în aplicare menționate la primul și al doilea paragraf de la prezentul alineat, statele membre nu trebuie să impună entităților care intră în domeniul de aplicare al respectivelor acte de punere în aplicare nicio cerință tehnică, metodologică sau sectorială suplimentară legată de măsurile menționate la articolul 21 alineatul (2) din Directiva (UE) 2022/2555.”

(8) La articolul 23 se introduc următoarele alineate (12) și (13):

„(12) Atunci când adoptă un act de punere în aplicare în temeiul alineatului (11) primul paragraf, Comisia include cerințe ca următoarele informații în ceea ce privește atacurile de tip ransomware să fie transmise în temeiul alineatului (1):

(a) dacă entitatea a detectat un atac de tip ransomware;

(b) vectorul de atac al atacului de tip ransomware;

(c) dacă au fost puse în aplicare măsuri de atenuare.

(13) Statele membre se asigură că, în cazul unui incident semnificativ cauzat de un atac de tip ransomware, entitățile în cauză informează, la cererea echipei CSIRT sau, după caz, a autorității competente, prin intermediul unui canal de comunicare furnizat de echipa CSIRT sau, după caz, de autoritatea competentă:

(a) dacă entitatea a primit o cerere de răscumpărare și, după caz, de la cine;

(b) dacă s-a plătit o răscumpărare și, în caz afirmativ, ce sumă a fost plătită și cărui destinatar sau beneficiar, inclusiv criptoactivul și prestatorul de servicii de criptoactive, după caz."

(9) La articolul 24, se adaugă următoarele alineate (4), (5) și (6):

„(4) Pentru a demonstra conformitatea cu articolul 21, statele membre pot solicita entităților esențiale și entităților importante să obțină un certificat privind postura de securitate cibernetică în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 75 din Regulamentul (UE) XXX/XXX**** [Propunere de regulament privind securitatea cibernetică 2].

(5) În cazul în care postura de securitate cibernetică a unei entități esențiale sau a unei entități importante este certificată în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 74 din Regulamentul (UE) XXX/XXX**** [Propunerea de regulament privind securitatea cibernetică 2] și în cazul în care certificatul demonstrează conformitatea cu cerințele prevăzute într-un act de punere în aplicare adoptat în temeiul articolului 21 alineatul (5) din prezenta directivă sau în dreptul intern de transpunere a articolului 21 alineatele (1) și (2) din prezenta directivă, autoritățile competente nu trebuie să supună entitatea unor măsuri suplimentare în temeiul articolului 32 alineatul (2) litera (b) sau al articolului 33 alineatul (2) litera (b), după caz, în ceea ce privește cerințele care fac obiectul certificatului.

(6) O certificare în temeiul alineatului (4) nu afectează responsabilitatea entității esențiale sau a entității importante de a se conforma prezentei directive.

_____

**** Regulamentul (UE) XXX/XXX [Propunere de regulament privind securitatea cibernetică 2]."

(10) Articolul 26 se modifică după cum urmează:

(a) la alineatul (1) se adaugă următoarea literă (d):

„(d) transportatorii aerieni, în privința cărora se consideră că se află sub jurisdicția statului membru a cărui autoritate competentă pentru acordarea licențelor a acordat licența de operare entității în temeiul Regulamentului (CE) nr. 1008/2008 al Parlamentului European și al Consiliului***** sau, în cazul în care licența de operare sau echivalentul acesteia nu a fost acordat(ă) în conformitate cu regulamentul respectiv, se află sub jurisdicția statului membru în care își au sediul principal în Uniune în temeiul alineatului (2).

_____

***** Regulamentul (CE) nr. 1008/2008 al Parlamentului European și al Consiliului din 24 septembrie 2008 privind normele comune pentru operarea

serviciilor aeriene în Comunitate (reformare) (JO L 293, 31.10.2008, p. 3, ELI: http://data.europa.eu/eli/reg/2008/1008/oj)”;

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) În cazul în care o entitate esențială sau o entitate importantă nu este stabilită în Uniune, dar oferă servicii în Uniune, aceasta desemnează un reprezentant în Uniune. Reprezentantul se stabilește în unul dintre statele membre în care se oferă serviciile. O astfel de entitate se consideră a fi sub jurisdicția statului membru în care este stabilit reprezentantul. În cazul în care o astfel de entitate este o entitate menționată la alineatul (1) litera (a), se consideră că aceasta se află sub jurisdicția statului membru în care își prestează serviciile. În absența unui reprezentant în Uniune desemnat în temeiul prezentului alineat, orice stat membru în care entitatea prestează servicii poate introduce acțiuni în justiție împotriva entității pentru încălcarea prezentei directive.”

(11) Articolul 27 se modifică după cum urmează:

(a) alineatul (1) se înlocuiește cu următorul text:

„(1) ENISA creează și menține un registru al entităților esențiale și al entităților importante, precum și al entităților care furnizează servicii de înregistrare a numelor de domenii, pe baza informațiilor primite de la punctele unice de contact în conformitate cu alineatul (4). La cerere, ENISA permite autorităților competente accesul la informații privind furnizorii de servicii DNS, registrele de nume TLD, entitățile care furnizează servicii de înregistrare a numelor de domenii, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, precum și furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și transportatorii aerieni stocați în registrul respectiv, asigurându-se, în același timp, că este protejată confidențialitatea informațiilor, după caz.”;

(b) alineatul (2) se elimină;

(c) alineatele (3), (4) și (5) se înlocuiesc cu următorul text:

„(3) Statele membre se asigură că entitățile esențiale și importante notifică autorității competente orice modificare a informațiilor pe care le-au transmis în temeiul articolului 3 alineatul (4), fără întârziere și, în orice caz, în termen de două săptămâni de la data modificării.

(4) La primirea informațiilor menționate la articolul 3 alineatul (4), punctul unic de contact al statului membru în cauză le transmite către ENISA fără întârzieri nejustificate.

(5) După caz, informațiile menționate la articolul 3 alineatul (4) primul paragraf se transmit prin mecanismul național menționat la articolul 3 alineatul (4) al patrulea paragraf.”

(12) Se introduce următorul articol 37a:

„Articolul 37a

Rolul ENISA în asistența reciprocă

(1) ENISA asistă statele membre în furnizarea de asistență reciprocă în sensul articolului 37 și contribuie la facilitarea unor astfel de procese de cooperare pentru entitățile esențiale și entitățile importante care furnizează servicii în mai multe state membre sau care furnizează servicii în unul sau mai multe state membre și ale căror rețele și sisteme informatice sunt situate în unul sau mai multe alte state membre.

(2) În scopurile prevăzute la alineatul (1), până la... [15 luni de la intrarea în vigoare a prezentului regulament], ENISA efectuează o analiză cuprinzătoare a riscurilor transfrontaliere în materie de securitate cibernetică legate de entitățile esențiale și entitățile importante care furnizează servicii în mai multe state membre sau care furnizează servicii în unul sau mai multe state membre și ale căror rețele și sisteme informatice sunt situate în unul sau mai multe alte state membre. Analiza evaluează amploarea posibilelor consecințe transfrontaliere și asupra pieței interne ale incidentelor care afectează aceste entități esențiale și importante. În scopul acestei analize, ENISA elaborează o metodologie în cooperare cu Comisia și cu grupul de cooperare. Pe baza analizei, ENISA elaborează un raport cuprinzător de evaluare a riscurilor transfrontaliere în materie de securitate cibernetică, care se actualizează anual.

(3) Pe baza raportului cuprinzător de evaluare a riscurilor transfrontaliere în materie de securitate cibernetică, ENISA:

(a) după caz, recomandă autorităților competente relevante să înființeze echipe comune de examinare pentru a sprijini supravegherea anumitor entități;

(b) elaborează orientări pentru acțiunile comune de supraveghere;

(c) la cererea autorităților competente ale statelor membre în cauză, stabilește modalitățile practice de realizare a acțiunilor comune de supraveghere;

(d) la cererea autorităților competente ale statelor membre în cauză și sub rezerva propriilor resurse și proporțional cu acestea, participă la acțiuni comune de supraveghere;

(e) la cererea autorităților competente ale statelor membre în cauză, acordă asistență pentru evaluarea nivelului de punere în aplicare de către o entitate esențială sau o entitate importantă a măsurilor de gestionare a riscurilor în materie de securitate cibernetică prevăzute la articolul 21.

(4) În sensul alineatului (3) litera (e) de la prezentul articol, autoritățile competente ale statelor membre în cauză furnizează ENISA, dacă este disponibilă, o listă a măsurilor de gestionare a riscurilor în materie de securitate cibernetică luate de entitatea esențială sau de entitatea importantă în conformitate cu articolul 21, o listă a acțiunilor de supraveghere sau de asigurare a respectării legii desfășurate, precum și documentația relevantă, inclusiv dovezi privind punerea în aplicare a politicilor de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate, pe care autoritățile competente le-au întreprins în temeiul articolelor 32 și 33 în ceea ce privește entitatea respectivă.

(5) În cazul în care un stat membru primește asistență reciprocă, astfel cum se menționează la articolul 37 alineatul (1) primul paragraf litera (c), punctul unic de contact informează ENISA că a avut loc asistența reciprocă. După caz, punctul unic de contact indică incidentul transfrontalier menționat la articolul 23 alineatul (6) care a fost legat de cazul de asistență reciprocă.”

(13) Anexele I și II se modifică în conformitate cu anexa la prezenta directivă.

Articolul 2

Transpunere

1. Până la... [12 luni de la intrarea în vigoare a prezentei directive], statele membre adoptă și publică măsurile necesare pentru a se conforma prezentei directive. Statele membre informează de îndată Comisia cu privire la aceasta.

   Statele membre aplică măsurile respective începând cu … [ziua următoare datei menționate la primul paragraf].

2. Atunci când statele membre adoptă măsurile menționate la alineatul (1), acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

Articolul 3

Intrarea în vigoare

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

Articolul 4

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Strasbourg,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președinta	*Președintele*
[...]	*[...]*