Consiliul
Uniunii Europene

Bruxelles, 14 septembrie 2017
(OR. en)

12183/17

Dosar interinstituțional:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

PROPUNERE

Sursă:	Secretar general al Comisiei Europene, sub semnătura dlui Jordi AYET PUIGARNAU, director
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2017) 477 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

În anexă, se pune la dispoziția delegațiilor documentul COM(2017) 477 final.

Anexă: COM(2017) 477 final

COMISIA
EUROPEANĂ

Bruxelles, 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

(Text cu relevanță pentru SEE)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Temeiurile și obiectivele propunerii

Uniunea Europeană a luat o serie de măsuri pentru a spori reziliența și gradul de pregătire în ceea ce privește securitatea cibernetică. Prima Strategie de securitate cibernetică a UE[1], adoptată în 2013, stabilește obiective strategice și acțiuni concrete menite să permită obținerea rezilienței, reducerea criminalității cibernetice, dezvoltarea politicii și a capabilităților de apărare cibernetică, dezvoltarea resurselor industriale și tehnologice și stabilirea unei politici internaționale coerente a UE în ceea ce privește spațiul cibernetic. În acest context, de la această primă strategie au avut loc evoluții importante, cele mai notabile fiind al doilea mandat al Agenției Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA)[2] și adoptarea **Directivei privind securitatea rețelelor și a sistemelor informatice**[3] (denumită în continuare „Directiva privind securitatea rețelelor și a informațiilor"), care constituie baza prezentei propuneri.

În plus, în **2016, Comisia Europeană a adoptat Comunicarea privind „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator"**[4], în cadrul căreia a anunțat noi măsuri de intensificare a cooperării, informării și schimbului de cunoștințe și de consolidare a rezilienței și pregătirii UE, ținând seama, de asemenea, de perspectiva unor incidente de mare amploare și de posibilitatea unei crize de securitate cibernetică paneuropene. În acest context, Comisia a anunțat că va prezenta **evaluarea** și **revizuirea** Regulamentului (UE) nr. 526/2013 al Parlamentului European și al Consiliului privind ENISA și de abrogare a Regulamentului (CE) nr. 460/2004 (denumit în continuare „Regulamentul ENISA"). Procesul de evaluare ar putea conduce la o eventuală reformă a agenției și la consolidarea capabilităților și capacităților de care dispune aceasta pentru a sprijini statele membre în mod durabil. În acest mod, agenția ar primi un rol mai proeminent și mai operațional în cadrul eforturilor depuse pentru atingerea rezilienței în materie de securitate cibernetică, iar noile responsabilități încredințate agenției în temeiul Directivei privind securitatea rețelelor și a informațiilor ar fi recunoscute în noul său mandat.

Directiva privind securitatea rețelelor și a informațiilor constituie o primă etapă esențială în direcția promovării unei culturi a gestionării riscurilor, deoarece introduce cerințe de securitate care constituie obligații juridice pentru principalii actori economici, în special operatorii care furnizează servicii esențiale (operatorii de servicii esențiale – OSE) și furnizorii anumitor servicii digitale cheie (furnizorii de servicii digitale – FSD). Dat fiind că cerințele de securitate sunt considerate ca fiind esențiale pentru protejarea beneficiilor digitalizării în curs a societății și având în vedere rapida proliferare a dispozitivelor conectate [*the Internet of Things (Internetul obiectelor)* – IoT], comunicarea din 2016 a propus, de

---

1 Comunicare comună a Comisiei Europene și a Serviciului European de Acțiune Externă: „Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat" - JOIN (2013).

2 Regulamentul (UE) nr. 526/2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004.

3 Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

4 Comunicarea Comisiei privind „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator", COM(2016) 0410 final.

asemenea, ideea de a se institui un cadru de certificare de securitate pentru produsele și serviciile TIC în scopul de a spori securitatea pieței unice digitale și încrederea de care se bucură aceasta. Certificarea de securitate cibernetică a TIC capătă o importanță deosebită, având în vedere utilizarea pe scară tot mai largă a tehnologiilor care necesită un nivel ridicat de securitate cibernetică, cum ar fi automobilele conectate și automatizate sau dispozitivele electronice pentru sănătate ori sistemele industriale automate de control .

Aceste măsuri de politică și anunțuri au primit susținere și din partea **Consiliului**, care, în **concluziile** din 2016, a recunoscut că „amenințările și vulnerabilitățile cibernetice continuă să evolueze și să se intensifice, ceea ce va necesita o cooperare continuă, mai strânsă, în special în ceea ce privește gestionarea incidentelor de securitate cibernetică transfrontaliere de mare amploare”. În concluziile menționate mai sus, Consiliul a reafirmat că Regulamentul ENISA constituie unul dintre „elementele esențiale ale unui cadru UE de reziliență cibernetică”[5] și a invitat Comisia să adopte măsuri suplimentare pentru a aborda problematica certificării la nivel european.

Instituirea unui sistem de certificare ar necesita crearea unui sistem adecvat de guvernanță la nivelul UE, inclusiv expertiză solidă furnizată de o agenție independentă a UE. În această privință, prezenta propunere stabilește că ENISA este organismul competent în mod normal, la nivelul UE, în domeniul securității cibernetice care ar trebui să preia un astfel de rol ce constă în a reuni autoritățile naționale competente în domeniul certificării și în a coordona activitatea acestora.

În Comunicarea sa din **mai 2017** intitulată**„Evaluarea la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală”**, Comisia a precizat din nou că va revizui mandatul ENISA până în septembrie 2017. Scopul urmărit este de a defini rolul care îi revine în ecosistemul de securitate cibernetică rezultat în urma schimbărilor și de a elabora măsuri privind standardele, certificarea și etichetarea în materie de securitate cibernetică pentru a spori gradul de siguranță cibernetică al sistemelor bazate pe TIC, inclusiv al obiectelor conectate[6]. **Concluziile Consiliului European** din iunie 2017[7] au salutat intenția Comisiei de a revizui Strategia de securitate cibernetică în septembrie și de a propune acțiuni suplimentare specifice înainte de sfârșitul anului 2017.

Propunerea de regulament prevede un set cuprinzător de măsuri care se bazează pe acțiuni anterioare și promovează obiective specifice care se consolidează reciproc:

- sporirea **capabilităților și a nivelului de pregătire** ale statelor membre și ale întreprinderilor;
- îmbunătățirea **cooperării și a coordonării** dintre statele membre și instituțiile, agențiile și organele UE;
- sporirea **capabilităților la nivelul UE care să completeze acțiunea statelor membre**, în special în cazul unor crize cibernetice transfrontaliere;
- sporirea **gradului de sensibilizare** a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică;

---

5 Concluziile Consiliului privind consolidarea sistemului de reziliență cibernetică al Europei și promovarea unui sector al securității cibernetice competitiv și inovator, 15 noiembrie 2016.

6 Comunicare intitulată„Evaluarea la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală”, COM(2017) 228 final.

7 Reuniune a Consiliului European (22 și 23 iunie 2017) – Concluziile EUCO 8/17.

- sporirea, în ansamblu, a **transparenței asigurării securității cibernetice**[8] a produselor și serviciilor TIC în scopul de a consolida încrederea în piața unică digitală și în inovarea digitală și
- evitarea **fragmentării sistemelor de certificare** în UE și a cerințelor de securitate aferente, precum și a criteriilor de evaluare în toate statele membre și în toate sectoarele.

Următoarea parte a expunerii de motive explică mai în detaliu argumentele care au stat la baza inițiativei în ceea ce privește acțiunile propuse pentru ENISA și certificarea de securitate cibernetică.

[8] Transparența asigurării securității cibernetice înseamnă furnizarea de informații suficiente utilizatorilor cu privire la proprietățile de securitate cibernetică pentru a le permite să determine în mod obiectiv nivelul de securitate al unui anumit produs, serviciu sau proces TIC.

ENISA

ENISA îndeplinește rolul de centru de expertiză consacrat sporirii securității rețelelor și a informațiilor în Uniune și sprijinirii eforturilor depuse de statele membre pentru consolidarea capacităților.

ENISA a fost creată în 2004[9] pentru a contribui la obiectivul general al asigurării unui nivel ridicat de securitate a rețelelor și a informațiilor în UE. În 2013, Regulamentul (UE) nr. 526/2013 a stabilit noul mandat al agenției, pentru o perioadă de șapte ani, până în 2020. Birourile agenției sunt situate în Grecia, sediul administrativ aflându-se la Heraklion (Creta), iar operațiunile principale desfășurându-se la Atena.

Comparativ cu toate celelalte agenții ale UE, ENISA este o agenție mică, ce dispune de un buget și un personal reduse. ENISA are un mandat cu durată fixă.

Agenția sprijină instituțiile europene, statele membre și comunitatea de afaceri **abordând problemele legate de securitatea rețelelor și a informațiilor, răspunzând la acestea și prevenindu-le**. În acest scop, ENISA desfășoară o serie de activități în cadrul celor cinci domenii identificate în strategia sa[10]:

- expertiză: furnizarea de informații și de expertiză cu privire la aspectele-cheie legate de securitatea rețelelor și a informațiilor;
- politici: acordarea de sprijin pentru elaborarea și punerea în aplicare a politicilor în Uniune;
- capacitate: sprijin pentru consolidarea capacităților în întreaga Uniune (de exemplu, prin cursuri de formare, recomandări, activități de sensibilizare);
- comunitate: promovarea comunității securității rețelelor și a informațiilor [de exemplu, prin acordarea de sprijin echipelor de intervenție în caz de incidente de securitate informatică (*Computer Emergency Response Teams* - CERT) și coordonarea exercițiilor cibernetice paneuropene];
- facilitare (de exemplu, stabilirea colaborării cu părțile interesate și relațiile internaționale).

În cursul negocierilor referitoare la Directiva privind securitatea rețelelor și a informațiilor, colegiuitorii UE au hotărât să încredințeze ENISA atribuții importante în punerea în aplicare a acestei directive. Agenția asigură în special secretariatul rețelei CSIRT (instituită pentru a promova cooperarea operațională rapidă și eficace între statele membre cu privire la incidentele de securitate cibernetică specifice, precum și schimbul de informații referitoare la riscuri) și este invitată, de asemenea, să furnizeze asistență grupului de cooperare în îndeplinirea sarcinilor care îi revin. În plus, directiva obligă ENISA să furnizeze asistență statelor membre și Comisiei, oferind expertiză, asigurând consiliere și facilitând schimbul de bune practici.

În conformitate cu Regulamentul ENISA, Comisia a efectuat o evaluare a agenției, care include un studiu independent și o consultare publică. În cadrul evaluării au fost analizate

[9] Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, JO L 77, 13.3.2004, p. 1.

[10] https://www.enisa.europa.eu/publications/corporate/enisa-strategy

relevanța, impactul, eficacitatea, eficiența, coerența și valoarea adăugată europeană a agenției în ceea ce privește îndeplinirea sarcinilor, guvernanța, structura de organizare internă și practicile de lucru în decursul perioadei 2013-2016.

Performanța globală a ENISA a primit aprecieri favorabile din partea majorității respondenților[11] (74 %) în cadrul consultării publice. Mai mult, majoritatea respondenților au considerat că ENISA își îndeplinește diferitele sale obiective (cel puțin 63 % pentru fiecare dintre obiective). Serviciile și produsele ENISA sunt utilizate periodic (lunar sau mai des) de aproape jumătate dintre respondenți (46 %) și sunt apreciate datorită faptului că provin de la un organism de la nivelul UE (83 %), precum și datorită calității lor (62 %).

Cu toate acestea, marea majoritate a respondenților (88 %) consideră că actualele instrumente și mecanisme disponibile la nivelul UE sunt insuficiente sau numai parțial adecvate pentru a răspunde provocărilor în materie de securitate cibernetică. Marea majoritate a respondenților (98 %) au indicat că aceste necesități ar trebui abordate de un organ al UE, iar 99% dintre aceștia au considerat că ENISA este organizația potrivită. În plus, 67,5 % dintre respondenți și-au exprimat opinia conform căreia ENISA ar putea juca un rol în crearea unui cadru armonizat pentru certificarea de securitate a produselor și serviciilor informatice.

Evaluarea globală (nu doar pe baza consultării publice, ci și pe baza unei serii de interviuri individuale, anchete și ateliere specifice suplimentare) a ajuns la următoarele concluzii:

- obiectivele ENISA rămân de actualitate și în ziua de azi. Într-un context marcat de evoluții tehnologice rapide și de amenințări în continuă schimbare și având în vedere riscurile din ce în ce mai grave la care este expusă securitatea cibernetică mondială, este clar că UE are nevoie să promoveze și să consolideze în continuare expertiza tehnică de nivel înalt privind aspectele legate de securitatea cibernetică. Este necesar să se consolideze capacități în statele membre pentru a înțelege amenințările și a răspunde la acestea, iar părțile interesate trebuie să coopereze în diverse domenii tematice și cu diverse instituții;
- în pofida bugetului său redus, agenția a dat dovadă de eficiență operațională în utilizarea resurselor sale și în îndeplinirea sarcinilor care îi revin. Cu toate acestea, existența a două sedii, la Atena și la Heraklion, a generat costuri administrative suplimentare;
- în ceea ce privește eficacitatea, ENISA a și-a îndeplinit parțial obiectivele. Agenția a contribuit cu succes la îmbunătățirea securității rețelelor și a informațiilor în Europa, oferind asistență pentru consolidarea capacității în 28 state membre[12], promovând

[11] La consultare au răspuns 90 de părți interesate din 19 state membre (88 răspunsuri și 2 documente de poziție), printre care se numără autorități naționale din 15 state membre și 8 organizații-umbrelă care reprezintă un număr important de întreprinderi europene.

[12] Respondenții la consultarea publică au fost invitați să își prezinte observațiile cu privire la ceea ce au perceput ei ca fiind principalele realizări ale ENISA în perioada 2013-2016. Respondenții din toate categoriile (în total 55, dintre care 13 din partea autorităților naționale, 20 din partea sectorului privat și 22 din categoria „alți respondenți") au apreciat că principalele realizări ale ENISA sunt: 1) coordonarea exercițiilor Cyber Europe; 2) furnizarea de sprijin pentru CERT/CSIRT prin cursuri de formare și ateliere de promovare a coordonării și a schimburilor; 3) publicațiile ENISA (orientări și recomandări, rapoarte privind situația amenințărilor, strategii de raportare a incidentelor și de gestionare a crizelor etc.), care au fost considerate ca fiind utile pentru a crea cadre naționale de securitate și a le actualiza, precum și ca referință pentru factorii de decizie politică și practicienii din domeniul cibernetic; 4) asistența acordată la promovarea Directivei privind securitatea rețelelor și a informațiilor;

cooperarea dintre statele membre și părțile interesate din domeniul securității rețelelor și a informațiilor, furnizând expertiză, consolidând comunitățile și sprijinind procesul de elaborare a politicilor. În ansamblu, ENISA s-a axat cu diligență pe punerea în aplicare a programului său de lucru și a acționat ca un partener de încredere în relația cu părțile interesate, într-un domeniu a cărui deosebită importanță transfrontalieră nu a fost decât recent recunoscută;

- ENISA a reușit să exercite o influență, cel puțin într-o anumită măsură, în vastul domeniu al securității rețelelor și informațiilor, dar nu a reușit să dezvolte pe deplin un nume de marcă puternic și să câștige o vizibilitate suficientă pentru a fi recunoscută drept „centru de expertiză” în Europa. Acest lucru se explică prin mandatul extins al ENISA, pentru care nu s-au alocat resurse proporțional de mari. În plus, ENISA rămâne singura agenție a UE având un mandat cu durată fixă, fapt care limitează capacitatea acesteia de a dezvolta o viziune pe termen lung și de a sprijini părțile interesate în mod durabil. Acest lucru este, de asemenea, în contradicție cu dispozițiile Directivei privind securitatea rețelelor și a informațiilor, care prevede pentru ENISA sarcini fără dată de finalizare. În sfârșit, evaluarea a constatat că această eficacitate limitată se poate explica parțial prin gradul ridicat de dependență de expertiza externă față de cea internă și prin dificultățile întâmpinate la recrutarea și păstrarea personalului de specialitate;
- în cele din urmă, dar nu mai puțin important, evaluarea a concluzionat că valoarea adăugată adusă de ENISA constă, în primul rând, în capacitatea agenției de a consolida cooperarea în principal între statele membre și în special cu comunitățile corespunzătoare din sectorul securității rețelelor și a informațiilor (îndeosebi între CSIRT). La nivelul UE, nu există niciun alt actor care să acorde sprijin unei game atât de ample de părți interesate din domeniul securității rețelelor și a informațiilor. Cu toate acestea, din cauza necesității de stabili în mod strict gradul de prioritate al activităților sale, programul de lucru al ENISA este orientat în principal în funcție de nevoile statelor membre. Drept urmare, agenția nu ține seama în suficientă măsură de nevoile altor părți interesate, în special ale sectorului. De asemenea, reacția agenției constă în a răspunde nevoilor principalelor părți interesate, ceea ce o împiedică să aibă un impact mai important. Prin urmare, valoarea adăugată adusă de agenție variază în funcție de nevoile divergente ale părților sale interesate și de măsura în care agenția poate să răspundă la acestea (de exemplu, statele membre mari față de statele membre mici; statele membre față de sector).

În concluzie, rezultatele consultărilor cu părțile interesate și ale evaluării au evidențiat necesitatea adaptării resurselor și mandatului ENISA, astfel încât aceasta să poată îndeplini un rol adecvat în ceea ce privește răspunsul la provocările prezente și viitoare.

Având în vedere aceste constatări, prezenta propunere revizuiește mandatul actual al ENISA și stabilește un set reînnoit de sarcini și funcții, cu scopul de a sprijini, în mod eficient și cu eficacitate, eforturile depuse de statele membre, instituțiile UE și alte părți interesate pentru a asigura un spațiu cibernetic sigur în Uniunea Europeană. Noul mandat propus urmărește să atribuie agenției un rol mai puternic și mai proeminent, în special în ceea ce privește acordarea de sprijin statelor membre în punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor, contracararea într-un mod mai activ a amenințărilor specifice (capacitate operațională) și dobândirea statutului de centru de expertiză care acordă sprijin

5) eforturile depuse pentru a spori gradul de sensibilizare cu privire la securitatea cibernetică prin intermediul lunii securității cibernetice.

statelor membre și Comisiei cu privire la certificarea de securitate cibernetică. În temeiul acestei propuneri:

- ENISA ar urma să primească un mandat permanent, beneficiind astfel de o bază stabilă pentru viitor. Mandatul, obiectivele și sarcinile ar trebui să facă obiectul unei revizuiri periodice;
- mandatul propus clarifică mai bine rolul ENISA de agenție de securitate cibernetică a UE și de punct de referință în ecosistemul de securitate cibernetică al UE, care acționează în strânsă cooperare cu toate celelalte organisme relevante ale acestui ecosistem;
- organizarea și guvernanța agenției, care au primit aprecieri pozitive în cursul evaluării, ar urma să fie ușor revizuite, în special pentru a asigura că nevoile comunității părților interesate în sens mai larg sunt mai bine reflectate în activitatea agenției;
- domeniul de aplicare propus al mandatului este delimitat, fiind consolidate domeniile în care agenția și-a demonstrat în mod clar valoarea adăugată și fiind adăugate acele domenii noi în care este nevoie de sprijin, având în vedere noile priorități și instrumente de politică, în special Directiva privind securitatea rețelelor și a informațiilor, revizuirea Strategiei de securitate cibernetică a UE și Planul de acțiune al UE privind securitatea cibernetică pentru cooperarea în caz de criză cibernetică și certificarea de securitate în domeniul TIC, care urmează să fie prezentat.
    - **Elaborarea și punerea în aplicare a politicilor UE:** ENISA ar urma să primească sarcina de a contribui în mod proactiv la elaborarea politicii din domeniul securității rețelelor și a informațiilor, precum și la alte inițiative de politici din diferite sectoare (de exemplu, energie, transporturi, finanțe) care prezintă elemente de securitate cibernetică. În acest scop, agenția ar urma să aibă un rol consultativ solid, pe care l-ar putea îndeplini emițând avize independente și realizând lucrări pregătitoare în vederea elaborării și actualizării politicii și legislației. ENISA ar urma să sprijine, de asemenea, politica și legislația UE din domeniile comunicațiilor electronice, identității electronice și serviciilor de încredere, în vederea promovării unui nivel mai ridicat de securitate cibernetică. În faza de punere în aplicare, în special în cadrul grupului de cooperare privind securitatea rețelelor și a informațiilor, ENISA ar urma să ajute statele membre să definească o abordare coerentă a punerii în aplicare a Directivei privind securitatea rețelelor și a informațiilor la nivel transfrontalier și transsectorial, precum și în alte politici și legislații relevante. Pentru a sprijini revizuirea periodică a politicilor și a legislației din domeniul securității cibernetice, ENISA ar urma să prezinte, de asemenea, rapoarte periodice cu privire la stadiul punerii în aplicare a cadrului juridic al UE.
    - **Consolidarea capacităților:** ENISA ar urma să contribuie la îmbunătățirea capabilităților și expertizei autorităților publice de la nivelul UE și de la nivel național, inclusiv în ceea ce privește răspunsul la incidente și supravegherea măsurilor de reglementare referitoare la securitatea cibernetică. De asemenea, ar trebui să se prevadă cerința ca agenția să contribuie la înființarea de centre de schimb și analiză de informații (*Information Sharing and Analysis Centres* - ISACS) în diverse sectoare, furnizând bune practici și orientări privind instrumentele disponibile și procedura și abordând în mod corespunzător aspectele de reglementare legate de schimbul de informații.

- **Cunoștințe și informații, acțiuni de sensibilizare:** ENISA ar urma să devină platforma de informații a UE. Acest lucru ar presupune schimbul de bune practici și inițiative și promovarea acestora la nivelul UE prin punerea în comun a informațiilor referitoare la securitatea cibernetică provenite de la instituțiile, organele și agențiile UE și naționale. De asemenea, agenția ar urma să pună la dispoziție consiliere, orientări și bune practici privind securitatea infrastructurilor critice. În plus, după producerea incidentelor transfrontaliere semnificative de securitate cibernetică, ENISA ar urma să întocmească rapoarte cu scopul de a oferi orientări întreprinderilor și cetățenilor din întreaga UE. Această linie de activitate ar urma să cuprindă, de asemenea, organizarea periodică de activități de sensibilizare, pe baza unei coordonări cu autoritățile statelor membre.

- **Sarcini legate de piață (standardizare, certificare de securitate cibernetică):** ENISA ar urma să îndeplinească o serie de funcții menite să sprijine în mod expres piața internă și să constituie totodată un observator al pieței" securității cibernetice, analizând tendințele relevante de pe piața securității cibernetice, pentru a corela mai bine cererea și oferta, și sprijinind elaborarea politicii UE în materie de standardizare și certificare de securitate cibernetică în domeniul TIC. În special în ceea ce privește standardizarea, aceasta ar facilita instituirea și adoptarea de standarde de securitate cibernetică. De asemenea, ENISA ar urma să îndeplinească sarcinile prevăzute în contextul viitorului cadru de certificare (a se vedea secțiunea de mai jos).

- **Cercetare și inovare:** ENISA ar urma să contribuie cu expertiza de care dispune, acordând consiliere autorităților UE și naționale în ceea ce privește stabilirea priorităților în materie de cercetare și dezvoltare, inclusiv în cadrul parteneriatului public-privat contractual (PPPc) privind securitatea cibernetică. Consilierea furnizată de ENISA cu privire la cercetare ar urma să fie integrată în activitatea noului centru european de cercetare și competențe în materie de securitate cibernetică în temeiul următorului cadru financiar multianual. De asemenea, ENISA ar urma să ia parte, în cazul în care primește o solicitare în acest sens din partea Comisiei, la punerea în aplicare a programelor UE de finanțare a cercetării și inovării.

- **Cooperarea operațională și gestionarea crizelor:** această linie de activitate ar trebui să se bazeze pe consolidarea capabilităților operaționale de prevenire existente, în special prin modernizarea exercițiilor paneuropene de securitate cibernetică (Cyber Europe), organizându-le anual, și pe îndeplinirea unui rol de susținere în cadrul cooperării operaționale în calitate de secretariat al rețelei CSIRT (în conformitate cu dispozițiile Directivei privind securitatea rețelelor și a informațiilor), asigurând, printre altele, buna funcționare a infrastructurii IT și a canalelor de comunicare ale rețelei CSIRT. În acest context, ar urma să fie necesar să se instituie o cooperare structurată cu CERT-EU, cu Centrul european de combatere a criminalității informatice (EC3) și cu alte organisme relevante ale UE. În plus, o cooperare structurată cu CERT-EU, în imediata vecinătate fizică, ar trebui să aibă drept rezultat îndeplinirea unei funcții de asistență tehnică în cazul unor incidente semnificative și de sprijinire a analizei incidentelor. Statele membre care solicită acest lucru ar urma să primească asistență pentru gestionarea incidentelor și sprijin pentru analiza vulnerabilităților, artefactelor și incidentelor, pentru a-și consolida propriile capabilități de prevenire și de răspuns.

- De asemenea, ENISA ar urma să îndeplinească un rol în ceea ce privește **planul de acțiune al UE în materie de securitate cibernetică**, care face parte din acest pachet și constituie recomandarea Comisiei către statele membre privind un răspuns coordonat, la nivelul UE, în caz de incidente și crize cibernetice transfrontaliere de mare amploare[13]. ENISA ar urma să faciliteze cooperarea dintre statele membre în ceea ce privește răspunsul în situații de urgență, prin analizarea și agregarea rapoartelor situaționale naționale pe baza informațiilor puse la dispoziția agenției pe bază de voluntariat de către statele membre și alte entități.

- **Certificarea de securitate cibernetică a produselor și serviciilor TIC**

Pentru a inspira și a menține încrederea în produsele și serviciile TIC și a le asigura securitatea, acestea trebuie să includă în mod direct elemente de securitate care să fie prevăzute încă din primele etape de proiectare și dezvoltare tehnică (securitatea de la stadiul conceperii). Mai mult decât atât, consumatorii și utilizatorii trebuie să poată verifica nivelul de asigurare a securității produselor și serviciilor pe care pe le achiziționează sau le cumpără.

Certificarea, care constă în evaluarea oficială a produselor, serviciilor și proceselor de către un organism independent și acreditat, pe baza unui set definit de criterii și standarde, și în emiterea unui certificat care să indice conformitatea, joacă un rol important în sporirea încrederii în produse și servicii și a securității acestora. Dacă evaluările de securitate prezintă un grad relativ ridicat de tehnicitate, certificarea are drept scop să informeze cumpărătorii și utilizatorii și să le insufle încredere cu privire la proprietățile de securitate a produselor și serviciilor TIC pe care le achiziționează sau le utilizează. După cum s-a indicat mai sus, acest lucru este valabil îndeosebi pentru sistemele noi care folosesc pe scară largă tehnologiile digitale și care necesită un nivel înalt de securitate, precum autovehiculele conectate și automatizate, dispozitivele electronice pentru sănătate, sistemele industriale automate de control[14] sau rețelele inteligente.

În prezent, certificarea de securitate cibernetică a produselor și serviciilor TIC în UE oferă o imagine destul de contrastată. Există o serie de inițiative internaționale, cum ar fi așa-numitele Criterii comune (CC) de evaluare a securității tehnologiei informației (ISO 15408), care constituie un standard internațional de evaluare a securității informatice. Acestea se bazează pe evaluarea efectuată de părți terțe și prevede șapte niveluri de evaluare a asigurării (EAL). CC și Metodologia comună de evaluare a securității tehnologiei informației (CEM), care le însoțește, constituie baza tehnică a unui acord internațional, Înțelegerea privind recunoașterea criteriilor comune (CCRA), care asigură recunoașterea certificatelor CC de toți semnatarii CCRA. Cu toate acestea, în conformitate cu actuala versiune a CCRA, sunt recunoscute reciproc numai evaluările până la EAL 2. În plus, numai 13 state membre au semnat înțelegerea.

---

13 Planul de acțiune se va aplica incidentelor de securitate cibernetică care provoacă perturbări a căror amploare depășește capacitatea oricărui stat membru de a gestiona situația pe cont propriu sau care afectează două sau mai multe state membre, consecințele sau importanța politică fiind atât de ample și de importante încât trebuie să se asigure rapid coordonarea politicilor și răspunsul la nivelul politic al Uniunii.

14 DG JRC a publicat un raport care propune un prim set de cerințe europene comune și de orientări generale privind certificarea de securitate cibernetică a componentelor sistemelor industriale automate de control. Disponibile la: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

Autoritățile de certificare din 12 state membre au încheiat un acord de recunoaștere reciprocă privind certificatele emise în conformitate cu acordul, pe baza criteriilor comune[15]. În plus, în statele membre există deja sau sunt pe cale de a fi instituite o serie de inițiative de certificare în domeniul TIC. Chiar dacă sunt importante, aceste inițiative riscă să conducă la fragmentarea pieței interne și la dificultăți legate de interoperabilitate. Drept urmare, aceeași întreprindere riscă să fie nevoită să parcurgă mai multe proceduri de certificare în diferite state membre pentru a-și putea oferi produsele pe mai multe piețe. De exemplu, un fabricant de contoare inteligente care dorește să își vândă produsele în trei state membre, de exemplu Germania, Franța și Regatul Unit, trebuie să se conformeze în prezent la trei tipuri diferite de sisteme de certificare: CPA (Commercial Product Assurance) în Regatul Unit, CSPN (Certification de Sécurité de Premier Niveau) în Franța și, respectiv, un profil de protecție specific bazat pe Criteriile comune în Germania.

Această situație generează costuri mai mari și constituie o sarcină administrativă considerabilă pentru întreprinderile care își desfășoară activitatea în mai multe state membre. Deși costurile de certificare pot varia în mod semnificativ în funcție de produsul/serviciul în cauză, de nivelul de evaluare a asigurării dorit și/sau de alte componente, în general, acestea sunt destul de ridicate pentru întreprinderi. De exemplu, în cazul certificatului „Smart Meter Gateway" acordat de Oficiul german pentru securitatea informațiilor (BSI), acest cost este de peste 1 milion euro (certificatul oferind cel mai ridicat nivel de testare și de asigurare și vizând nu doar un singur produs, ci întreaga infrastructură din jurul produsului respectiv). În Regatul Unit, costul de certificare a contoarelor inteligente este de aproximativ 150 000 euro. În Franța, acest cost este similar cu cel din Regatul Unit, ridicându-se la aproximativ 150 000 EUR sau chiar mai mult.

Principalele părți interesate publice și private au recunoscut că, în lipsa unui sistem la nivelul UE de certificare de securitate cibernetică, întreprinderile trebuie, în numeroase cazuri, să solicite certificare în mod separat în fiecare stat membru, ceea ce duce la fragmentarea pieței. Cel mai important este însă faptul că, în lipsa unei legislații UE care să asigure armonizarea pentru produsele și serviciile TIC, diferențele de standarde și practici de certificare de securitate cibernetică dintre statele membre riscă să creeze, în practică, 28 de piețe separate ale securității în UE, fiecare dintre acestea stabilind propriile cerințe tehnice, metodologii de testare și proceduri de certificare de securitate cibernetică. Dacă nu se ia nicio măsură adecvată la nivelul UE, aceste abordări divergente de la nivel național sunt de natură să conducă la regres semnificativ în realizarea pieței unice digitale, încetinind sau împiedicând efectele pozitive conexe în ceea ce privește creșterea economică și crearea de locuri de muncă.

Pornind de la aceste evoluții, propunerea de Regulament stabilește un cadru european de certificare de securitate cibernetică („**cadrul**") pentru produsele și serviciile TIC și precizează funcțiile și sarcinile esențiale ale ENISA în domeniul certificării de securitate cibernetică. Prezenta propunere stabilește un cadru general de norme care reglementează sistemele europene de certificare de securitate cibernetică. Propunerea nu introduce sisteme de certificare imediat operaționale, ci creează un sistem (cadru) în vederea instituirii de sisteme de certificare specifice pentru produse/servicii TIC specifice (denumite în continuare „sisteme

[15] Din Grupul înalților funcționari pentru securitatea sistemelor informatice (SOG-IS) fac parte reprezentanți din12 state membre plus Norvegia. SOG-IS a elaborat câteva profiluri de protecție pentru un număr restrâns de produse, cum ar fi semnătura electronică, tahograful digital și cardul inteligent. Participanții colaborează pentru a coordona standardizarea profilurilor de protecție CC și a coordona elaborarea de profiluri de protecție. Statele membre solicită adesea certificarea SOG-IS pentru procedurile naționale de achiziții publice.

europene de certificare de securitate cibernetică"). Crearea unor sisteme europene de certificare de securitate cibernetică în conformitate cu cadrul va permite certificatelor emise în cadrul acestor sisteme să beneficieze de valabilitate și recunoaștere în toate statele membre și va contracara actuala fragmentare a pieței.

Scopul general al unui sistem european de certificare de securitate cibernetică este de a atesta că produsele și serviciile TIC care au fost certificate în conformitate cu sistemul respectiv respectă cerințele de securitate cibernetică specificate. Este vorba, de exemplu, de capacitatea lor de a proteja datele (indiferent dacă sunt stocate, transmise sau prelucrate într-un alt mod) împotriva stocării, prelucrării, accesării, divulgării, distrugerii accidentale sau neautorizate sau a pierderii ori modificării accidentale. Sistemele UE de certificare de securitate cibernetică ar urma să utilizeze standardele existente în ceea ce privește cerințele tehnice și procedurile de evaluare cărora trebuie să se conformeze produsele și nu ar urma să elaboreze ele însele propriile standarde tehnice[16]. De exemplu, o certificare la nivelul UE a unor produse precum cardurile inteligente, care, în prezent, sunt testate în conformitate cu standardele CC internaționale în cadrul sistemului SOG-IS multilateral (descris anterior), ar însemna că acest sistem ar deveni valabil pe întregul teritoriu al UE.

Propunerea prezintă un set precis de obiective de securitate care urmează să fie luate în considerare la conceperea unui sistem european de certificare de securitate cibernetică specific și, în plus, stabilește în ce ar trebui să constea conținutul minim al unor astfel de sisteme. Aceste sisteme vor trebui să definească, printre altele, o serie de elemente specifice care să stabilească domeniul de aplicare și obiectul certificării de securitate cibernetică. Aceasta include identificarea categoriilor de produse și servicii care fac obiectul sistemului, descrierea detaliată a cerințelor de securitate cibernetică (de exemplu, prin trimitere la standardele sau specificațiile tehnice relevante), criteriile și metodele specifice de evaluare și nivelul de asigurare pe care sistemul respectiv intenționează să-l ofere (și anume, de bază, substanțială sau ridicată).

Sistemele europene de certificare de securitate cibernetică vor fi pregătite de ENISA, pe baza asistenței și consilierii de specialitate acordate de Grupul european pentru certificarea de securitate cibernetică (a se vedea mai jos) și a cooperării cu acesta și vor fi adoptate de Comisie prin intermediul actelor de punere în aplicare. În cazul în care se stabilește că este necesar un sistem de certificare de securitate cibernetică, Comisia va solicita ENISA să pregătească un sistem pentru anumite produse sau servicii TIC. ENISA va lucra la sistemul respectiv în strânsă cooperare cu autoritățile naționale de supraveghere în materie de certificare reprezentate în cadrul Grupului. Statele membre și Grupul pot propune Comisiei să solicite ENISA să pregătească un anumit sistem.

Certificarea poate fi un proces foarte costisitor, putând duce la creșterea prețurilor pentru clienți și consumatori. De asemenea, necesitatea certificării poate varia semnificativ în funcție de contextul specific de utilizare a produselor și serviciilor și de rapiditatea schimbărilor tehnologice. Recurgerea la certificarea europeană de securitate cibernetică ar trebui să aibă loc în continuare numai pe bază de voluntariat, cu excepția cazului în care există dispoziții contrare în legislația Uniunii privind cerințele de securitate aplicabile produselor și serviciilor TIC.

Pentru a se asigura armonizarea și a se evita fragmentarea, sistemele sau procedurile naționale de certificare de securitate cibernetică pentru produsele și serviciile TIC care fac obiectul unui

[16] În cazul standardelor europene, acest lucru se realizează prin intermediul organizațiilor europene de standardizare, iar Comisia Europeană își acordă aprobarea prin publicarea în *Jurnalul Oficial* (a se vedea Regulamentul (UE) nr. 1025/2012).

sistem european de certificare de securitate cibernetică vor înceta să se aplice cu începere de la data stabilită în actul de punere în aplicare prin care a fost adoptat sistemul în cauză. În plus, statele membre ar trebui să nu introducă noi sisteme naționale de certificare pentru produse și servicii TIC care fac deja obiectul unui sistem european de certificare de securitate cibernetică existent.

Odată ce este adoptat un sistem european de certificare de securitate cibernetică, fabricanții de produse TIC sau furnizorii de servicii TIC vor avea posibilitatea de a depune o cerere de certificare a produselor sau serviciilor lor la un organism de evaluare a conformității ales de ei. Organismele de evaluare a conformității ar trebui să fie acreditate de un organism de acreditare dacă respectă anumite cerințe specificate. Acreditarea va fi acordată pe o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, dacă organismul de evaluare a conformității îndeplinește cerințele. Organismele de acreditare vor revoca acreditarea unui organism de evaluare a conformității în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care măsurile luate de un organism de evaluare a conformității încalcă dispozițiile prezentului regulament.

În temeiul propunerii, sarcinile de monitorizare, de supraveghere și de executare le revin statelor membre. Statele membre vor trebui să prevadă o autoritate de supraveghere în materie de certificare. Această autoritate va fi însărcinată să verifice dacă organismele de evaluare a conformității și certificatele emise de organismele de evaluare a conformității stabilite pe teritoriul lor respectă cerințele prezentului regulament și ale sistemelor relevante de certificare de securitate cibernetică. Autoritățile naționale de supraveghere în materie de certificare vor avea competența de a soluționa plângerile depuse de persoane fizice sau juridice în legătură cu certificatele emise de organismele de evaluare a conformității stabilite pe teritoriul lor. În măsura necesară, acestea vor examina subiectul plângerii și vor informa reclamantul cu privire la stadiul și rezultatul investigației, într-un termen rezonabil. În plus, ele vor coopera cu alte autorități de supraveghere în materie de certificare sau cu alte autorități publice, de exemplu prin schimbul de informații cu privire la o posibilă neconformitate a produselor și serviciilor TIC cu cerințele prezentului regulament sau cu sistemele europene de securitate cibernetică specifice.

În cele din urmă, propunerea instituie Grupul european pentru certificarea de securitate cibernetică (denumit în continuare „Grupul”), alcătuit din autoritățile naționale de supraveghere în materie de certificare ale tuturor statelor membre. Principala misiune a grupului constă în a acorda consiliere Comisiei cu privire la chestiuni legate de politica în materie de certificare de securitate cibernetică și în a coopera cu ENISA pentru elaborarea de proiecte de sisteme europene de certificare de securitate cibernetică. ENISA va ajuta Comisia să asigure secretariatul Grupului și va ține o evidență actualizată a sistemelor aprobate în temeiul cadrului european de certificare de securitate cibernetică. De asemenea, ENISA ar urma să coopereze cu organismele de standardizare pentru a se sigura că standardele utilizate în cadrul sistemelor aprobate sunt adecvate și pentru a identifica domeniile în care sunt necesare standarde de securitate cibernetică.

Cadru european de certificare de securitate cibernetică („cadrul”) va oferi mai multe avantaje pentru cetățeni și întreprinderi. În special:

- prin crearea unor sisteme de certificare de securitate cibernetică la nivelul UE pentru produse sau servicii specifice se va pune la dispoziția întreprinderilor un „ghișeu unic” pentru certificarea de securitate cibernetică în UE. Aceste întreprinderi își vor putea certifica produsele lor numai o singură dată și vor obține un certificat valabil în toate statele membre. Ele nu vor fi obligate să depună cereri de recertificare la diferitele organisme naționale de certificare. În acest mod, se vor reduce costurile

suportate de întreprinderi, se vor facilita operațiunile transfrontaliere și, în ultimă instanță, se va reduce și se va evita fragmentarea pieței interne pentru produsele în cauză;

- cadrul stabilește preeminența sistemelor europene de certificare de securitate cibernetică asupra sistemelor naționale: în temeiul acestei reguli, adoptarea unui sistem european de certificare de securitate cibernetică va înlocui toate sistemele naționale paralele existente pentru aceleași produse sau servicii TIC la un anumit nivel de asigurare. Acest lucru va aduce mai multă claritate, limitând actuala proliferare a sistemelor naționale de certificare de securitate cibernetică care se suprapun și riscă să se contrazică;
- propunerea sprijină și completează punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor, furnizând întreprinderilor care fac obiectul directivei un instrument foarte util pentru a demonstra respectarea cerințelor privind securitatea rețelelor și a informațiilor în întreaga Uniune. Atunci când elaborează noi sisteme de certificare de securitate cibernetică, Comisia și ENISA vor acorda o atenție deosebită necesității de a se asigura că cerințele privind securitatea rețelelor și a informațiilor se regăsesc în sistemele de certificare de securitate cibernetică;
- propunerea va sprijini și va facilita elaborarea unei politici europene în materie de securitate cibernetică, prin armonizarea condițiilor și cerințelor de fond privind certificarea de securitate cibernetică a produselor și serviciilor TIC în UE. Sistemele europene de certificare de securitate cibernetică vor face trimitere la standarde sau criterii comune de evaluare și la metodologii comune de testare. Acest lucru va contribui în mod semnificativ, deși indirect, la adoptarea soluțiilor comune de securitate în UE, ceea ce va permite, de asemenea, eliminarea barierelor din calea pieței interne;
- cadrul este conceput astfel încât să se asigure flexibilitatea necesară sistemelor de certificare de securitate cibernetică. În funcție de nevoile specifice în materie de securitate cibernetică, un produs sau un serviciu pot fi certificate la un nivel de securitate mai ridicat sau mai scăzut. La conceperea sistemelor europene de certificare de securitate cibernetică se va avea în vedere această flexibilitate. Prin urmare, aceste sisteme vor trebui să prevadă diferite niveluri de asigurare (și anume de bază, substanțială sau ridicată), astfel încât sistemele să poată fi utilizate în scopuri diferite sau în contexte diferite;
- toate elementele de mai sus vor crește atractivitatea certificării de securitate cibernetică pentru întreprinderi, care vor vedea în aceasta un mijloc eficace de a comunica nivelul de asigurare a securității cibernetice pentru produsele sau serviciile TIC. În măsura în care certificarea de securitate cibernetică devine mai puțin costisitoare, mai eficace și mai atractivă din punct de vedere comercial, întreprinderile vor fi mai motivate să-și certifice produsele împotriva riscurilor de securitate cibernetică, contribuind astfel la difuzarea unor practici de securitate cibernetică mai bune la conceperea produselor și serviciilor TIC (securitatea cibernetică de la stadiul conceperii).

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

Directiva privind securitatea rețelelor și a informațiilor prevede că operatorii din sectoare care sunt vitale pentru economie și societate, precum energia, transporturile, apa, băncile, infrastructurile pieței financiare, asistența medicală și infrastructurile digitale, precum și

furnizorii de servicii digitale (și anume, motoarele de căutare, serviciile de cloud computing și piețele online) sunt obligați să ia măsuri pentru a gestiona în mod corespunzător riscurile de securitate. Noile norme din prezenta propunere completează dispozițiile Directivei privind securitatea rețelelor și a informațiilor și asigură coerența cu acestea, urmărind să consolideze în continuare reziliența cibernetică a UE, prin consolidarea capabilităților, prin cooperare, prin gestionarea riscurilor și prin sensibilizare cu privire la aspectele cibernetice.

În plus, normele privind certificarea de securitate cibernetică asigură întreprinderilor care fac obiectul Directivei privind securitatea rețelelor și a informațiilor un instrument esențial, permițându-le să își certifice produsele și serviciile TIC împotriva riscurilor de securitate cibernetică pe baza unor sisteme de certificare de securitate cibernetică valabile și recunoscute în întreaga UE. De asemenea, aceste norme vor veni în completarea cerințelor de securitate menționate în Regulamentul eIDAS[17] și în Directiva privind echipamentele radio[18].

- **Coerența cu alte domenii de politică a Uniunii**

Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor - „**RGPD**”)[19] cuprinde dispoziții privind instituirea de mecanisme de certificare și introducerea de sigilii și mărci de protecție a datelor pentru a demonstra conformitatea cu regulamentul respectiv a operațiunilor de prelucrare efectuate de operatori și persoanele împuternicite de aceștia. Prezentul regulament nu aduce atingere certificării operațiunilor de prelucrare a datelor în temeiul RGPD, inclusiv în cazul în care aceste operațiuni sunt integrate în produse și servicii.

Propunerea de regulament va asigura compatibilitatea cu Regulamentul (CE) nr. 765/2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței[20], făcând trimitere la normele cadrului respectiv privind organismele naționale de acreditare și organismele de evaluare a conformității. În ceea ce privește autoritățile de supraveghere, propunerea de regulament va obliga statele membre să desemneze autorități naționale de supraveghere în materie de certificare, cu responsabilități de supraveghere, monitorizare și asigurare a respectării normelor. Aceste organisme vor rămâne distincte de organismele de evaluare a conformității, astfel cum se prevede în Regulamentul (CE) nr. 765/2008.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

- **Temeiul juridic**

Temeiul juridic pentru acțiunea UE este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), care se referă la apropierea legislațiilor statelor membre în vederea

---

17 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.

18 Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE.

19 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), (JO L 119, 4.5.2016, p. 1-88).

20 Regulamentul (CE) nr. 765/2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93.

realizării obiectivelor prevăzute la articolul 26 din TFUE, și anume buna funcționare a pieței interne.

Temeiul juridic privind piața internă pentru instituirea ENISA a fost confirmat de Curtea de Justiție (în cauza C-217/04 Regatul Unit/Parlamentul European și Consiliul) și a fost confirmat din nou prin regulamentul din 2013 care a stabilit mandatul actual al agenției. În plus, activitățile menite să atingă obiectivele intensificării cooperării și coordonării dintre statele membre și cele care urmăresc să dezvolte capabilitățile existente la nivelul UE pentru a completa acțiunea statelor membre ar intra în categoria „cooperării operaționale". Aceasta din urmă este identificată în mod expres de Directiva privind securitatea rețelelor și a informațiilor (care are drept temei juridic articolul 114 din TFUE) drept obiectiv care trebuie urmărit în contextul rețelei CSIRT, pentru care „ENISA asigură secretariatul și sprijină activ cooperarea" [articolul 12 alineatul (2)]. În special, articolul 12 alineatul (3) litera (f) precizează în plus că identificarea de noi forme de cooperare operațională face parte din sarcinile rețelei CSIRT, inclusiv în ceea ce privește: (i) categoriile de riscuri și incidente; (ii) alertele timpurii; (iii) asistența reciprocă și (iv) principiile și modalitățile de coordonare, atunci când statele membre răspund la riscuri și incidente transfrontaliere.

- Fragmentarea actuală a sistemelor de certificare pentru produsele și serviciile TIC decurge, de asemenea, din lipsa unui proces-cadru comun, obligatoriu din punct de vedere juridic și eficace care să se aplice statelor membre. Acest lucru împiedică crearea unei piețe interne pentru produsele și serviciile TIC și afectează competitivitatea industriei europene în acest sector. Prezenta propunere urmărește să remedieze fragmentarea existentă și obstacolele conexe din calea pieței interne, prin asigurarea unui cadru comun pentru instituirea de sisteme de certificare de securitate cibernetică valabile în întreaga UE.

Subsidiaritatea (în cazul competențelor neexclusive)

Principiul subsidiarității impune obligația de a evalua necesitatea și valoarea adăugată a acțiunii UE. Respectarea principiului subsidiarității în acest domeniu a fost deja recunoscută în momentul adoptării actualului Regulament ENISA[21].

Securitatea cibernetică este o chestiune de interes comun pentru Uniune. Interdependențele dintre rețelele și sistemele informatice sunt de așa natură încât, în numeroase cazuri, actorii individuali (publici și privați, inclusiv cetățenii), în mod separat, nu sunt în măsură să facă față amenințărilor și să gestioneze riscurile și eventualele efecte ale incidentelor cibernetice. Pe de o parte, având în vedere relațiile de interdependență dintre statele membre, inclusiv în ceea ce privește funcționarea infrastructurilor critice (energie, transporturi și apă, pentru a menționa doar câteva dintre acestea), intervenția publică la nivel european este nu numai benefică, ci și necesară. Pe de altă parte, intervenția UE poate avea un „efect de propagare" pozitiv, datorită schimbului de bune practici între statele membre, ceea ce poate avea ca rezultat consolidarea securității cibernetice a Uniunii.

Pentru a rezuma toate aceste considerații, din contextul actual și din perspectiva scenariilor viitoare reiese că, pentru **a spori reziliența cibernetică colectivă** a Uniunii, **acțiunile individuale ale statelor membre ale UE și o abordare fragmentară a securității cibernetice** nu vor fi suficiente.

---

[21] Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004.

Acțiunea la nivelul UE este considerată necesară și pentru a pune capăt fragmentării actualelor sisteme de certificare de securitate cibernetică. Aceasta ar permite fabricanților să beneficieze pe deplin de piața internă, datorită importantelor economii obținute în ceea ce privește costurile de testare și de reproiectare. Deși actualul Acord de recunoaștere reciprocă (ARR) al Grupului înalților funcționari pentru securitatea sistemelor informatice (SOG-IS) a obținut rezultate importante în acest sens, acesta a dat dovadă, de asemenea, de limitări importante care îi afectează capacitatea de a furniza soluții durabile pe termen lung pentru valorificarea întregului potențial al pieței interne.

Valoarea adăugată a unei acțiuni la nivelul UE, în special în scopul de a consolida cooperarea între statele membre, dar și între comunitățile din sectorul securității rețelelor și a informațiilor, a fost recunoscută de Concluziile Consiliului din 2016[22] și reiese, de asemenea, în mod clar din evaluarea ENISA.

- **Proporționalitatea**

Măsurile propuse nu depășesc ceea ce este necesar atingerii obiectivelor lor de politică. În plus, domeniul de aplicare al intervenției UE nu împiedică nicio altă acțiune națională în domeniul securității naționale. Prin urmare, acțiunea UE este justificată din rațiuni de subsidiaritate și proporționalitate.

- **Alegerea instrumentului**

Prezenta propunere revizuiește Regulamentul (UE) nr. 526/2013 care stabilește actualul mandat și actualele sarcini ale ENISA. În plus, dat fiind rolul important jucat de ENISA în crearea și gestionarea unui cadru UE de certificare de securitate cibernetică, noul mandat al ENISA și cadrul menționat anterior sunt stabilite în mod optim în cadrul unui singur instrument juridic, și anume regulamentul.

3. REZULTATE ALE EVALUĂRILOR EX POST, CONSULTĂRILOR PĂRȚILOR INTERESATE ȘI EVALUĂRII IMPACTULUI

Evaluările ex post/verificarea adecvării legislației existente

Comisia, în conformitate cu foaia de parcurs a evaluării[23], a analizat **relevanța, impactul, eficacitatea, eficiența, coerența și valoarea adăugată** a agenției în ceea ce privește îndeplinirea sarcinilor, guvernanța, structura de organizare internă și practicile de lucru în decursul perioadei 2013-2016. Principalele constatări pot fi sintetizate după cum urmează (pentru mai multe detalii, a se consulta documentul de lucru al serviciilor Comisiei referitor la acest subiect, care însoțește evaluarea impactului).

- **Relevanța:** în contextul evoluțiilor tehnologice și al unor amenințări aflate în plină transformare și având în vedere nevoia acută de sporire a securității cibernetice în UE, obiectivele ENISA s-au dovedit a fi relevante. Într-adevăr, statele membre și organele UE se bazează pe experiența sa considerabilă în chestiunile de securitate cibernetică. Mai mult decât atât, este necesar să se consolideze capacități în statele membre pentru a înțelege mai bine amenințările și a răspunde mai bine la acestea, iar

[22] Concluziile Consiliului privind consolidarea sistemului de reziliență cibernetică al Europei și promovarea unui sector al securității cibernetice competitiv și inovator, 15 noiembrie 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

părțile interesate trebuie să coopereze în diverse domenii tematice și cu diverse instituții. Securitatea cibernetică continuă să fie o prioritate politică esențială a UE, pe care ENISA trebuie să o concretizeze; cu toate acestea, ENISA a fost concepută ca agenție a UE cu un mandat cu durată fixă, ceea ce: (i) nu permite planificarea pe termen lung și acordarea unui sprijin durabil statelor membre și instituțiilor UE; (ii) poate conduce la apariția unui vid juridic, întrucât dispozițiile Directivei privind securitatea rețelelor și a informațiilor care stabilesc sarcinile încredințate ENISA au caracter permanent[24]; (iii) nu este coerent cu viziunea conform căreia ENISA se integrează într-un ecosistem UE consolidat al securității cibernetice.

- **Eficacitatea**: În general, ENISA și-a îndeplinit obiectivele și a pus în aplicare sarcinile care i-au fost încredințate. Agenția a contribuit la sporirea securității rețelelor și a informațiilor în Europa prin activitățile sale principale (consolidarea capacităților, furnizarea de expertiză, crearea de comunități și sprijinirea politicilor). Cu toate acestea, pentru fiecare dintre aceste activități, s-a demonstrat că există posibilități de îmbunătățire. Potrivit concluziilor evaluării, ENISA a stabilit cu eficacitate relații solide și bazate pe încredere cu unele dintre părțile interesate, în special cu statele membre și cu comunitatea CSIRT. Intervențiile în domeniul consolidării capacităților au fost percepute drept eficace, în special pentru statele membre cu mai puține resurse. Una dintre acțiunile sale remarcabile a constituit-o promovarea unei cooperări extinse, părțile interesate fiind, în marea lor majoritate, de acord cu privire la rolul pozitiv pe care l-a jucat ENISA în crearea de legături. Cu toate acestea, ENISA a întâmpinat greutăți în încercarea de a exercita o influență considerabilă asupra domeniului vast al securității rețelelor și a informațiilor. Aceste dificultăți se explică și prin resursele umane și financiare relativ limitate de care a dispus agenția pentru îndeplinirea unui mandat foarte amplu. De asemenea, evaluarea a concluzionat că ENISA nu și-a îndeplinit decât parțial obiectivul de a furniza expertiză, din cauza problemelor legate de recrutarea specialiștilor (a se consulta, de asemenea, secțiunea referitoare la eficiență, de mai jos).
- **Eficiența**: În pofida bugetului său redus – printre cele mai scăzute în comparație cu cele ale altor agenții ale UE – agenția a reușit să contribuie la obiectivele vizate, dând dovadă, în ansamblu, de eficiență în utilizarea resurselor sale. Evaluarea a concluzionat că procesele au fost, în general, eficiente și că delimitarea clară a responsabilităților în cadrul organizației a avut drept rezultat buna îndeplinire a sarcinilor. Eficiența agenției a fost pusă la încercare în principal de dificultățile legate de recrutarea și păstrarea specialiștilor cu înaltă calificare. Potrivit concluziilor, o posibilă explicație constă într-o combinație de factori, printre care pot fi menționate dificultățile generale întâmpinate de întregul sector public atunci când se află în concurență cu sectorul privat în încercarea de a angaja experți cu înaltă specializare, tipul de contracte (cu durată determinată) pe care îl poate oferi în cele mai multe cazuri agenția și nivelul relativ scăzut de atractivitate al locului în care se află ENISA, legat, de exemplu, de dificultatea de a-și găsi un loc de muncă cu care se confruntă soții angajaților. Repartizarea sediului între Atena și Heraklion a necesitat eforturi suplimentare de coordonare și a generat costuri suplimentare, însă transferul la Atena, în 2013, a departamentului care desfășoară operațiunile principale a mărit eficiența operațională a agenției.

[24] Trimitere la articolele 7, 9, 11, 12, 19 din Directiva privind securitatea rețelelor și a sistemelor informatice („Directiva privind securitatea rețelelor și a informațiilor”).

- **Coerența**: În general, activitățile ENISA au fost coerente cu politicile și activitățile părților interesate, la nivel național și la nivelul UE, însă este nevoie de o abordare mai coordonată la nivelul UE în ceea ce privește securitatea cibernetică. Potențialul de cooperare între ENISA și alte organe ale UE nu a fost valorificat pe deplin. Mandatul actual a devenit mai puțin coerent în prezent ca urmare a evoluției peisajului juridic și politic al UE.
- **Valoarea adăugată europeană**: Valoarea adăugată a ENISA constă, în primul rând, în capacitatea agenției de a consolida cooperarea, în special între statele membre, dar și cu comunitățile corespunzătoare din sectorul securității rețelelor și a informațiilor. Nu există niciun alt actor la nivelul UE care să sprijine cooperarea dintre părți interesate atât de diverse în domeniul securității rețelelor și a sistemelor informatice. Valoarea adăugată adusă de agenție a variat în funcție de nevoile și resursele divergente ale părților interesate (de exemplu, statele membre mari față de statele membre mici; statele membre față de sector) și în funcție de necesitatea de a stabili gradul de prioritate al activităților agenției în funcție de programul de lucru. Evaluarea a concluzionat că o eventuală desființare a ENISA ar fi echivalentă, pentru toate statele membre, cu o ocazie ratată. Nu va fi posibil să se asigure același nivel de dezvoltare de comunități și de cooperare între statele membre în domeniul securității cibernetice. În lipsa unei agenții a UE mai centralizate, peisajul ar deveni mai fragmentar, deoarece vidul creat prin desființarea ENISA ar fi acoperit de cooperarea bilaterală sau regională.

În ceea ce privește în mod specific rezultatele anterioare și viitoare ale ENISA, în urma consultării din 2017 se conturează tendințele prezentate în continuare[25].

- Rezultatele globale ale activității ENISA din perioada 2013-2016 au primit aprecieri pozitive din partea majorității respondenților (74 %). Mai mult, majoritatea respondenților au considerat că ENISA își îndeplinește diferitele sale obiective (cel puțin 63 % pentru fiecare dintre obiective). Serviciile și produsele ENISA sunt utilizate periodic (lunar sau mai des) de aproape jumătate dintre respondenți (46 %) și sunt apreciate datorită faptului că provin de la un organism de la nivelul UE (83 %), precum și datorită calității lor (62 %).
- Respondenții au identificat o serie de carențe și de provocări pentru viitorul securității cibernetice în UE, principalele cinci dintre acestea (dintr-o listă care cuprindea un număr de 16) fiind următoarele: cooperarea dintre statele membre; capacitatea de a preveni, a detecta și a soluționa atacurile cibernetice de mare amploare; cooperarea între statele membre în ceea ce privește aspectele legate de securitatea cibernetică; cooperarea și schimbul de informații între diferitele părți interesate, inclusiv cooperarea dintre sectorul public și cel privat; protecția infrastructurilor critice împotriva atacurilor cibernetice.

[25] La consultare au răspuns 90 de părți interesate din 19 state membre (88 răspunsuri și 2 documente de poziție), inclusiv autoritățile naționale din 15 state membre, printre care Franța, Italia, Irlanda și Grecia și 8 organizații-umbrelă care reprezintă un număr semnificativ de organizații europene, cum ar fi Federația Bancară Europeană, Digital Europe (care reprezintă sectorul tehnologiei digitale în Europa) și Asociația Europeană a Operatorilor de Rețele de Telecomunicații (ETNO). Consultarea publică privind ENISA a fost completată de o serie de alte surse, cum ar fi: (i) interviuri aprofundate cu aproximativ 50 de actori-cheie din comunitatea securității cibernetice; (ii) o anchetă efectuată în rândul membrilor rețelei CSIRT; (i) o anchetă efectuată în rândul membrilor consiliului de administrație, ai comitetului executiv și ai Grupului permanent al părților interesate al ENISA.

- Marea majoritate a respondenților (88 %) consideră că actualele instrumente și mecanisme existente la nivelul UE sunt insuficiente sau numai parțial adecvate pentru soluționarea acestor probleme. Marea majoritate a respondenților (98 %) au declarat că un organ al UE ar trebui să răspundă acestor nevoi, iar 99% dintre aceștia au considerat că ENISA este organizația potrivită.

Consultările cu părțile interesate

- Comisia a organizat o consultare publică pentru reexaminarea ENISA între 12 aprilie și 5 iulie 2016 și a primit 421 de răspunsuri[26]. Conform rezultatelor, 67,5 % dintre respondenți și-au exprimat opinia conform căreia ENISA ar putea juca un rol în crearea unui cadru armonizat pentru certificarea de securitate a produselor și serviciilor IT.

Rezultatele consultării din 2016 referitoare la PPPc privind securitatea cibernetică[27] indică, în secțiunea referitoare la certificare, că:

- 50,4 % (121 din 240) dintre respondenți nu știu dacă sistemele naționale de certificare sunt recunoscute reciproc în toate statele membre ale UE. 25,8 % (62 din 240) au răspuns „Nu”, în timp ce 23,8 % (57 din 240) au răspuns „Da”.
- 37,9 % dintre respondenți (91 din 240) consideră că sistemele de certificare existente nu sprijină nevoile industriei europene. Pe de altă parte, 17, 5 % (42 din 240) – în special societăți multinaționale care își desfășoară activitatea pe piața europeană – au susținut contrariul.
- 49,6 % (119 din 240) dintre respondenți afirmă că nu este ușor să se demonstreze echivalența între standarde, sisteme de certificare și etichete. 37,9 % (91 din 240) au răspuns „Nu știu”, în timp ce numai 12,5 % (30 din 240) au răspuns „Da”.

Obținerea și utilizarea expertizei

Comisia s-a bazat pe consiliere de specialitate externă, și anume:

- Studiu privind evaluarea ENISA (Ramboll/Carsa 2017; SMART nr. 2016/0077),
- Studiu privind certificarea și etichetarea de securitate a TIC – Colectarea de probe și evaluarea de impact (PriceWaterhouseCoopers 2017; SMART nr. 2016/0029).

Evaluarea impactului

- În raportul de evaluare a impactului privind această inițiativă s-a stabilit că trebuie soluționate următoarele probleme principale:
- fragmentarea politicilor și a abordărilor în materie de securitate cibernetică din statele membre;

[26] 162 de contribuții de la cetățeni, 33 de la organizațiile societății civile și de consumatori; 186 de la întreprinderi și 40 de la autorități publice, inclusiv autoritățile competente însărcinate cu punerea în aplicare a Directivei asupra confidențialității și comunicațiilor electronice.

[27] La secțiunea privind certificarea au răspuns 240 de părți interesate din administrații publice naționale, întreprinderi mari, IMM-uri, microîntreprinderi și organisme de cercetare.

- dispersarea resurselor și fragmentarea abordărilor privind securitatea cibernetică la nivelul instituțiilor, agențiilor și organelor UE și
- sensibilizarea și informarea insuficiente ale cetățenilor și întreprinderilor, la care se adaugă apariția unui număr tot mai mare de sisteme de certificare naționale și sectoriale multiple.

În cadrul raportului au fost evaluate următoarele opțiuni posibile în ceea ce privește mandatul ENISA:

- menținerea statu-quoului, ceea ce înseamnă prelungirea unui mandat care va continua să aibă o durată determinată (opțiunea de referință);
- expirarea mandatului actual al ENISA fără reînnoire și desființarea ENISA (nicio intervenție politică);
- o „ENISA reformată” și
- o agenție UE pentru securitate cibernetică care să dispună de capabilități operaționale depline.

În cadrul raportului au fost evaluate următoarele opțiuni posibile în ceea ce privește certificarea de securitate cibernetică:

- nicio intervenție politică (opțiunea de referință);
- măsuri nelegislative („fără caracter obligatoriu”);
- un act legislativ al UE care să creeze un sistem obligatoriu pentru toate statele membre pe baza sistemului SOG-IS și
- un cadru general al UE de certificare de securitate cibernetică în domeniul TIC.

În urma analizei s-a concluzionat că opțiunea preferată constă într-o „ENISA reformată” asociată cu un cadru general al UE de certificare a securității cibernetice în domeniul TIC.

S-a apreciat că opțiunea preferată este cea mai eficace pentru a permite UE să îndeplinească obiectivele stabilite, și anume: sporirea capabilităților de securitate cibernetică, creșterea gradului de pregătire, de cooperare, de sensibilizare și de transparență și evitarea fragmentării pieței. De asemenea, această opțiune a fost evaluată ca fiind cea mai coerentă cu prioritățile de politică ale Strategiei de securitate cibernetică a UE și ale politicilor conexe (de exemplu, Directiva privind securitatea rețelelor și a informațiilor), precum și cu Strategia privind piața unică digitală. În plus, în urma procesului de consultare a reieșit că opțiunea preferată se bucură de sprijinul majorității părților interesate. Mai mult decât atât, analiza efectuată în cadrul evaluării impactului a arătat că opțiunea preferată ar permite atingerea obiectivelor printr-o utilizare rezonabilă a resurselor.

Comitetul de analiză a reglementării al Comisiei a emis inițial un aviz negativ la data de 24 iulie, urmat de un aviz pozitiv la 25 august 2017, în urma prezentării unei noi evaluări. Versiunea modificată a raportului de evaluare a impactului a inclus elemente justificative suplimentare, concluziile finale ale evaluării ENISA și explicații suplimentare cu privire la opțiunile de politică și la impactul acestora. Anexa 1 la raportul final de evaluare a impactului sintetizează modul în care au fost abordate observațiile formulate de comitet în cadrul celui cel de-al doilea aviz. Raportul a fost actualizat în special pentru a prezenta într-un mod mai detaliat situația securității cibernetice în UE, inclusiv măsurile care sunt incluse în Comunicarea comună „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE” [JOIN(2017) 450] și care prezintă o importanță deosebită pentru ENISA: planul de acțiune al UE în materie de securitate cibernetică și Centrul european de

cercetare și competență în materie de securitate cibernetică, căruia agenția îi va prezenta informările sale privind necesitățile UE în materie de cercetare.

Raportul explică modul în care reforma agenției, inclusiv noile sarcini, îmbunătățirea condițiilor de angajare și cooperarea structurată cu organele UE din domeniu, ar ajuta agenția să devină un angajator mai atractiv și să rezolve problemele legate de recrutarea de specialiști. Anexa 6 la raport prezintă, de asemenea, o estimare revizuită a costurilor asociate opțiunilor de politică privind ENISA. În ceea ce privește subiectul certificării, raportul a fost revizuit astfel încât să ofere o explicație mai detaliată, inclusiv sub formă de prezentare grafică, privind opțiunea preferată și să prezinte estimări privind costurile noului cadru de certificare care vor trebui acoperite de statele membre și de Comisie . S-au adus explicații suplimentare cu privire la argumentele pe baza cărora ENISA a fost selectată ca actor-cheie al cadrului, și anume datorită expertizei sale în domeniu și faptului că este singura agenție de securitate cibernetică de la nivelul UE. În cele din urmă, secțiunile privind certificarea au fost revizuite astfel încât să clarifice unele aspecte legate de diferențele față de actualul sistem SOG-IS, să descrie beneficiile care pot fi aduse de diferitele opțiuni de politică și să explice faptul că tipul de produse și de servicii TIC care fac obiectul unui sistem european de certificare vor fi definite în cadrul sistemului aprobat respectiv.

Adecvarea reglementărilor și simplificarea

Nu se aplică.

Impactul asupra drepturilor fundamentale

Securitatea cibernetică are un rol esențial în ceea ce privește protejarea vieții private și a datelor cu caracter personal ale persoanelor fizice, în conformitate cu articolele 7 și 8 din Carta drepturilor fundamentale a UE. Este evident că producerea de incidente cibernetice prezintă riscuri la adresa vieții private și a protecției datelor cu caracter personal. Securitatea cibernetică este, prin urmare, o condiție necesară pentru respectarea vieții private și pentru confidențialitatea datelor noastre personale. Din această perspectivă, întrucât urmărește consolidarea securității cibernetice în Europa, propunerea aduce o completare importantă la legislația existentă care protejează dreptul fundamental la protecția vieții private și a datelor cu caracter personal. De asemenea, securitatea cibernetică este esențială pentru protejarea confidențialității comunicațiilor noastre electronice și, prin urmare, pentru exercitarea libertății de exprimare și de informare și a altor drepturi conexe, precum libertatea de gândire, de conștiință și de religie.

4. IMPLICAȚII BUGETARE

A se vedea fișa financiară

5. ELEMENTE DIVERSE

- **Planurile de implementare și mecanismele de monitorizare, evaluare și raportare**

Comisia va monitoriza punerea în aplicare a regulamentului și va prezenta Parlamentului European, Consiliului și Comitetului Economic și Social European un raport privind evaluarea sa o dată la cinci ani. Aceste rapoarte vor fi publice și vor prezenta în detaliu punerea în aplicare efectivă și asigurarea respectării prezentului regulament.

- **Explicații detaliate cu privire la prevederile specifice ale propunerii**

Titlul I din regulament cuprinde dispozițiile generale: obiectul (articolul 1), definițiile (articolul 2), inclusiv trimiteri la definiții relevante din alte instrumente ale UE, cum ar fi Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva privind securitatea rețelelor și a informațiilor), Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 și Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului privind standardizarea europeană.

Titlul II din regulament cuprinde principalele dispoziții referitoare la ENISA, Agenția UE pentru Securitate Cibernetică.

Capitolul I de la același titlu descrie mandatul (articolul 3), obiectivele (articolul 4) și sarcinile agenției (articolele 5-11).

Capitolul II prezintă în linii mari organizarea ENISA și include principalele dispoziții privind structura sa (articolul 12). Se referă la componența, regulile de vot și funcțiile consiliului de administrație (secțiunea 1, articolele 13-17), la comitetul executiv (secțiunea 2, articolul 18) și la directorul executiv (secțiunea 3 articolul 19). Acesta include, de asemenea, dispoziții privind componența și rolul grupului permanent al părților interesate (secțiunea 4, articolul 20). În cele din urmă, dar nu în ultimul rând, secțiunea 5 de la același capitol prezintă în detaliu regulamentul de funcționare al agenției, inclusiv în ceea ce privește programarea operațiunilor sale, conflictele de interese, transparența, confidențialitatea și accesul la documente (articolele 21-25).

Capitolul III se referă la întocmirea și structura bugetului agenției (articolele 26 și 27), precum și la normele care reglementează execuția bugetului (articolele 28 și 29). Acesta include, de asemenea, dispoziții care facilitează combaterea fraudei, a corupției și a altor activități ilegale (articolul 30).

Capitolul IV se referă la dotarea cu personal a agenției. Acesta cuprinde dispoziții generale privind Statutul funcționarilor și Regimul aplicabil celorlalți agenți, precum și normele care reglementează privilegiile și imunitățile (articolele 31 și 32). De asemenea, capitolul IV detaliază normele privind angajarea și numirea directorului executiv al agenției (articolul 33). În cele din urmă, dar nu în ultimul rând, aceasta include dispoziții care prevăd condițiile în care agenția poate face apel la experți naționali detașați sau la alte categorii de personal care nu sunt angajați ai agenției (articolul 34).

În sfârșit, capitolul V cuprinde dispozițiile generale referitoare la agenție. Acesta descrie statutul juridic (articolul 35) și include dispoziții care reglementează aspecte legate de răspundere, de regimul lingvistic, de protecția datelor cu caracter personal (articolele 36-38), precum și normele de securitate privind protejarea informațiilor clasificate și a informațiilor sensibile neclasificate (articolul 40). Acesta descrie normele care reglementează cooperarea agenției cu țări terțe și cu organizații internaționale (articolul 39). În cele din urmă, dar nu în ultimul rând, aceasta conține, de asemenea, dispoziții privind sediul agenției și condițiile de funcționare, precum și privind exercitarea controlului administrativ de către Ombudsman (articolele 41 și 42).

Titlul III din regulament stabilește cadrul european de certificare de securitate cibernetică („**cadrul**”) pentru produsele și serviciile TIC cu titlu de *lex generalis* (articolul 1). Acesta definește obiectivul general al sistemelor europene de certificare de securitate cibernetică, care constă în a oferi asigurarea că produsele și serviciile TIC sunt conforme cu cerințele de

securitate cibernetică specificate în ceea ce privește capacitatea acestora de a rezista, la un anumit nivel de asigurare, la acțiuni care compromit disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori funcțiile sau serviciile oferite de respectivele produse și servicii (articolul 43). În plus, acesta enumeră obiectivele de securitate pe care sistemele europene de certificare de securitate cibernetică trebuie să le urmărească (articolul 45), cum ar fi, printre altele, capacitatea de a proteja datele împotriva divulgării, distrugerii sau modificării accidentale sau neautorizate sau împotriva accesului accidental sau neautorizat la acestea, și stabilește conținutul (și anume, elementele) sistemelor europene de certificare de securitate cibernetică, cum ar fi, de exemplu, specificațiile detaliate privind domeniului lor de aplicare, obiectivele de securitate, criteriile de evaluare etc. (articolul 47).

Titlul III stabilește, de asemenea, efectele juridice principale ale sistemelor europene de certificare de securitate cibernetică, și anume (i) obligația de punere în aplicare a sistemului la nivel național și caracterul voluntar al certificării; (ii) efectul de invalidare pe care îl au sistemele europene de certificare de securitate cibernetică asupra sistemelor naționale existente pentru aceleași produse sau servicii (articolele 48 și 49).

Acest titlu stabilește, de asemenea, procedura de adoptare a sistemelor europene de certificare de securitate cibernetică și rolurile care revin în acest sens Comisiei, ENISA și Grupului european pentru certificarea de securitate cibernetică – „Grupul” – (articolul 44). În cele din urmă, acest titlu stabilește dispozițiile care reglementează organismele de evaluare a conformității, inclusiv cerințele, competențele și sarcinile acestora, autoritățile naționale de supraveghere în materie de certificare, precum și sancțiunile.

Același titlu prevede, de asemenea, instituirea grupului, în calitate de organism esențial, alcătuit din reprezentanți ai autorităților naționale de supraveghere în materie de certificare. Se stabilește că funcția sa principală constă în a coopera cu ENISA la pregătirea sistemelor europene de certificare de securitate cibernetică și în a furniza consiliere Comisiei cu privire la probleme generale sau specifice legate de politica de certificare de securitate cibernetică.

Titlul IV din regulament cuprinde dispozițiile finale care descriu exercitarea delegării, cerințele privind evaluarea, abrogarea și succesiunea, precum și intrarea în vigoare.

2017/0225 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ŞI 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[28],

având în vedere avizul Comitetului Regiunilor[29],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Rețelele și sistemele informatice și rețelele și serviciile de telecomunicații îndeplinesc un rol vital pentru societate și au devenit coloana vertebrală a creșterii economice. Tehnologia informației și comunicațiilor stă la baza sistemelor complexe care sprijină activitățile societății, asigură funcționarea economiei în sectoare-cheie cum ar fi sănătatea, energia, finanțele și transporturile și, mai ales, susține funcționarea pieței interne.

(2) În prezent, rețelele și sistemele informatice sunt utilizate la scară generală de către cetățenii, întreprinderile și administrațiile din întreaga Uniune. Digitizarea și conectivitatea sunt pe cale să devină caracteristici principale ale unui număr tot mai mare de produse și servicii, preconizându-se că, odată cu apariția internetului obiectelor (IoT), în UE, în următorul deceniu, vor intra în folosință milioane, dacă nu chiar miliarde de dispozitive digitale conectate. Deși numărul dispozitivelor conectate la internet este în creștere, securitatea și reziliența nu sunt incluse suficient de la nivelul de proiect, ceea ce conduce la o securitate cibernetică insuficientă. În acest context, din cauză că certificarea nu este utilizată decât într-o măsură limitată, utilizatorii, indiferent dacă sunt persoane fizice sau organizații, nu dispun de suficiente informații cu privire la caracteristicile de securitate cibernetică ale produselor și serviciilor TIC, ceea ce erodează încrederea în soluțiile digitale.

(3) Creșterea gradului de digitizare și conectivitate conduce la agravarea riscurilor la adresa securității cibernetice, societatea, în general, devenind astfel mai vulnerabilă la

[28] JO C , , p. .
[29] JO C , , p. .

amenințările cibernetice, iar pericolele cu care se confruntă persoanele fizice, inclusiv persoanele vulnerabile precum copiii, fiind extrem de mari. Pentru a atenua acest risc cu care se confruntă societatea, trebuie să se ia toate măsurile necesare pentru îmbunătățirea securității cibernetice în UE, astfel încât să se ofere o mai bună protecție a rețelelor și sistemelor informatice, a rețelelor de telecomunicații, a produselor, serviciilor și dispozitivelor digitale utilizate de către cetățeni, administrații și întreprinderi – de la IMM-uri la operatorii de infrastructuri critice – împotriva amenințărilor cibernetice.

(4) În condițiile în care atacurile cibernetice sunt în creștere, o economie și o societate conectată care sunt mai vulnerabile la amenințările și atacurile cibernetice necesită dispozitive de protecție mai puternice. Cu toate acestea, deși atacurile cibernetice sunt adesea transfrontaliere, răspunsurile oferite de politicile autorităților de securitate cibernetică și de aplicare a legii sunt predominant naționale. Incidentele de securitate cibernetică de mare amploare sunt de natură să perturbe furnizarea serviciilor esențiale pe întregul teritoriu al UE. Din acest motiv, trebuie să se asigure un răspuns și o gestionare eficace a crizelor la nivelul UE, care să se bazeze pe politicile specifice și pe instrumentele mai generale de solidaritate europeană și asistență reciprocă. În plus, pentru factorii de decizie politică, sector și utilizatori este important, prin urmare, să existe o evaluare periodică a situației în materie de securitate cibernetică și reziliență în Uniune, pornind de la date fiabile la nivelul Uniunii, precum și de la o prognoză sistematică a evoluțiilor, provocărilor și amenințărilor viitoare, atât la nivelul Uniunii, cât și la nivel mondial.

(5) Având în vedere intensificarea provocărilor în materie de securitate cibernetică cu care se confruntă Uniunea, este necesar un set cuprinzător de măsuri care să se bazeze pe acțiunile anterioare ale Uniunii și să promoveze obiective care se consolidează reciproc. Printre acestea se numără necesitatea de a spori și mai mult capabilitățile și gradul de pregătire ale statelor membre și ale întreprinderilor, precum și de a îmbunătăți cooperarea și coordonarea între statele membre și instituțiile, agențiile și organele UE. Mai mult decât atât, amenințările cibernetice nu se opresc la frontiere, motiv pentru care este necesară dezvoltarea capabilităților de la nivelul Uniunii care ar putea completa acțiunea statelor membre, în special în cazul incidentelor și crizelor de securitate cibernetică transfrontaliere de mare amploare. De asemenea, sunt necesare eforturi suplimentare pentru a spori gradul de sensibilizare a cetățenilor și întreprinderilor cu privire la aspectele legate de securitatea cibernetică. În plus, oferirea de informații transparente cu privire la nivelul de securitate al produselor și serviciilor TIC ar urma să permită pieței unice digitale să se bucure de o încredere și mai mare. Acest lucru poate fi facilitat printr-o certificare la nivelul UE care să prevadă cerințe comune în materie de securitate cibernetică și criterii de evaluare aplicabile pe toate piețele naționale și în toate sectoarele.

(6) În 2004, Parlamentul European și Consiliul au adoptat Regulamentul (CE) nr. 460/2004[30] privind instituirea ENISA, cu scopul de a contribui la obiectivele de asigurare a unui nivel ridicat al securității rețelelor și a informațiilor în Uniune și la dezvoltarea unei culturi a securității rețelelor și a informațiilor, în beneficiul cetățenilor, al consumatorilor, al întreprinderilor și al administrațiilor publice. În 2008,

[30] Regulamentul (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (JO L 77, 13.3.2004, p. 1).

Parlamentul European și Consiliul au adoptat Regulamentul (CE) nr. 1007/2008[31], prelungind mandatul agenției până în martie 2012. Regulamentul (UE) nr. 580/2011[32] a prelungit din nou mandatul agenției până la 13 septembrie 2013. În 2013, Parlamentul European și Consiliul au adoptat Regulamentul (UE) nr. 526/2013[33] privind ENISA și de abrogare a Regulamentului (CE) nr. 460/2004, prin care mandatul agenției a fost prelungit până în iunie 2020.

(7) Uniunea a luat deja măsuri importante pentru a asigura securitatea cibernetică și a crește încrederea în tehnologiile digitale. În 2013, a fost adoptată Strategia de securitate cibernetică a Uniunii Europene, menită să orienteze politicile prin care Uniunea răspunde la amenințările și riscurile în materie de securitate cibernetică. În cadrul eforturilor depuse pentru a proteja mai bine europenii în mediul online, în 2016 Uniunea a adoptat primul act legislativ în domeniul securității cibernetice, și anume Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune („Directiva privind securitatea rețelelor și a informațiilor”). Directiva privind securitatea rețelelor și a informațiilor a instituit cerințe privind capabilitățile naționale în domeniul securității cibernetice, a creat primele mecanisme de intensificare a cooperării strategice și operaționale între statele membre și a introdus obligații privind măsurile de securitate și notificările incidentelor în sectoare vitale pentru economie și societate, cum ar fi energia, transporturile, apa, băncile, infrastructurile pieței financiare, asistența medicală, infrastructurile digitale, precum și furnizorii de servicii digitale esențiale (motoarele de căutare, serviciile de cloud computing și piețele online). ENISA a primit un rol esențial de sprijinire a punerii în aplicare a directivei menționate mai sus. În plus, combaterea eficace a criminalității cibernetice se numără printre prioritățile importante ale Agendei europene privind securitatea, contribuind la obiectivul general de obținere a unui nivel ridicat de securitate cibernetică.

(8) Este recunoscut faptul că, de la adoptarea Strategiei de securitate cibernetică a UE, în 2013, și de la ultima revizuire a mandatului agenției, contextul general de politici a cunoscut schimbări semnificative, legate, de asemenea, de apariția unui mediu mondial mai incert și mai puțin sigur. În acest context, în cadrul noii politici de securitate cibernetică a Uniunii, este necesar să se revizuiască mandatul ENISA pentru a defini rolul care îi revine în ecosistemul de securitate cibernetică rezultat în urma acestor evoluții și pentru a oferi asigurarea că agenția contribuie în mod eficace la răspunsul Uniunii la provocările în materie de securitate cibernetică ce își au originea în această transformare radicală a naturii amenințărilor, pentru care, astfel cum se recunoaște în evaluarea agenției, mandatul actual nu este suficient.

(9) Agenția instituită prin prezentul regulament ar trebui să succeadă ENISA astfel cum a fost instituită prin Regulamentul (UE) nr. 526/2013. Agenția ar trebui să ducă la

---

31 Regulamentul (CE) nr. 1007/2008 al Parlamentului European și al Consiliului din 24 septembrie 2008 de modificare a Regulamentului (CE) nr. 460/2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, în ceea ce privește durata de funcționare a acesteia (JO L 293, 31.10.2008, p. 1).

32 Regulamentul (UE) nr. 580/2011 al Parlamentului European și al Consiliului din 8 iunie 2011 de modificare a Regulamentului (CE) nr. 460/2004 privind instituirea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor, în ceea ce privește durata de funcționare a acesteia (JO L 165, 24.6.2011, p. 3).

33 Regulamentul (UE) nr. 526/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) și de abrogare a Regulamentului (CE) nr. 460/2004 (JO L 165, 18.6.2013, p. 41).

îndeplinire sarcinile care îi sunt conferite prin prezentul regulament și prin actele juridice ale Uniunii din domeniul securității cibernetice, printre altele prin furnizarea de expertiză și consiliere și prin exercitarea rolului de centru de informare și de cunoștințe al Uniunii. Ea ar trebui să promoveze schimbul de bune practici între statele membre și părțile interesate din sectorul privat, oferind sugestii în materie de politici Comisiei Europene și statelor membre, acționând ca punct de referință pentru inițiativele de politică sectorială ale Uniunii în ceea ce privește aspectele legate de securitatea cibernetică, încurajând cooperarea operațională între statele membre, precum și între statele membre și instituțiile, agențiile și organele UE.

(10) În cadrul Deciziei 2004/97/CE, Euratom, adoptată cu ocazia reuniunii Consiliului European din 13 decembrie 2003, reprezentanții statelor membre au decis că ENISA își va avea sediul într-un oraș din Grecia care urma să fie stabilit de guvernul elen. Statul membru gazdă al agenției ar trebui să asigure cele mai bune condiții posibile pentru funcționarea optimă și în mod eficient a agenției. Pentru îndeplinirea adecvată și eficientă a sarcinilor sale, pentru recrutarea și menținerea personalului, precum și pentru consolidarea eficienței activităților sale de relaționare este indispensabil ca agenția să aibă un amplasament adecvat care, printre altele, să ofere conexiuni de transport și facilități adecvate pentru soții/soțiile și copiii care însoțesc membrii personalului agenției. Dispozițiile necesare ar trebui stabilite într-un acord încheiat între agenție și statul membru gazdă, după obținerea aprobării consiliului de administrație al agenției.

(11) Având în vedere agravarea provocărilor în materie de securitate cibernetică cu care se confruntă Uniunea, ar fi necesară o sporire a resurselor financiare și umane alocate agenției, care să corespundă consolidării rolului și sarcinilor sale, precum și poziției sale critice în ecosistemul de organizații care apără ecosistemul digital european.

(12) Agenția ar trebui să dezvolte și să mențină un nivel ridicat de expertiză și să funcționeze ca punct de referință, instaurând încrederea în piața unică grație independenței sale, calității consilierii acordate și informațiilor diseminate, transparenței procedurilor și metodelor sale de operare, precum și eforturilor depuse în îndeplinirea sarcinilor sale. Agenția ar trebui să contribuie în mod proactiv la eforturile depuse la nivel național și la nivelul UE, îndeplinindu-și totodată sarcinile în deplină cooperare cu instituțiile, organele, oficiile și agențiile Uniunii și cu statele membre. În plus, agenția ar trebui să se bazeze pe informațiile primite de la sectorul privat și alte părți interesate relevante și pe cooperarea cu acestea. Este necesar să se stabilească printr-o serie de sarcini modul în care agenția trebuie să își realizeze obiectivele, permițându-i în același timp să funcționeze flexibil.

(13) Agenția ar trebui să furnizeze asistență Comisiei sub formă de consiliere, avize și analize cu privire la toate chestiunile de competența Uniunii legate de elaborarea, actualizarea și revizuirea politicilor și legislației din domeniul securității cibernetice, inclusiv al protecției infrastructurilor critice și al rezilienței cibernetice. Agenția ar trebui să acționeze ca punct de referință în ceea ce privește consilierea și expertiza pentru inițiativele de politică și legislative sectoriale ale Uniunii în cazul în care intervin chestiuni legate de securitatea cibernetică.

(14) Sarcina fundamentală a agenției este de a promova punerea în aplicare coerentă a cadrului juridic relevant, în special punerea în aplicare eficace a Directivei privind securitatea rețelelor și a informațiilor, care este esențială pentru sporirea rezilienței cibernetice. Având în vedere evoluția rapidă a naturii amenințărilor la adresa securității cibernetice, este clar că statele membre trebuie să fie sprijinite printr-o

abordare mai cuprinzătoare, bazată pe mai multe politici, a consolidării rezilienței cibernetice.

(15) Agenția ar trebui să furnizeze asistență statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii, venind în sprijinul eforturilor depuse de acestea pentru a crea și a consolida capabilitățile și pregătirea necesare pentru a preveni, a detecta și a reacționa la problemele și incidentele de securitate cibernetică și în ceea ce privește securitatea rețelelor și a sistemelor informatice. În special, agenția ar trebui să sprijine dezvoltarea și consolidarea CSIRT naționale, astfel încât acestea să ajungă la un nivel comun ridicat de maturitate în Uniune. Agenția ar trebui, de asemenea, să acorde asistență la elaborarea și actualizarea strategiilor Uniunii și ale statelor membre în materie de securitate a rețelelor și a sistemelor informatice, în special în ceea ce privește securitatea cibernetică, și să promoveze diseminarea lor și monitorizarea progreselor înregistrate în punerea în aplicare a acestora. Totodată, agenția ar trebui să ofere organismelor publice cursuri și materiale de formare, și, dacă este cazul, să asigure„formarea formatorilor” pentru a ajuta statele membre să își creeze propriile capabilități de formare.

(16) Agenția ar trebui să furnizeze asistență grupului de cooperare instituit prin Directiva privind securitatea rețelelor și a informațiilor pentru a-l ajuta să își îndeplinească sarcinile, în special oferind expertiză, asigurând consiliere și facilitând schimbul de bune practici, în principal în ceea ce privește identificarea operatorilor de servicii esențiale de către statele membre, inclusiv în legătură cu dependența transfrontalieră în ceea ce privește riscurile și incidentele.

(17) Pentru a încuraja cooperarea între sectorul public și cel privat și cooperarea în cadrul acestuia din urmă, în special pentru a sprijini protecția infrastructurilor critice, agenția ar trebui să faciliteze instituirea de centre sectoriale de schimb și analiză de informații (*Information Sharing and Analysis Centres* - ISAC), propunând bune practici și orientări privind instrumentele disponibile și procedura și furnizând orientări privind modul în care trebuie abordate problemele de reglementare legate de schimbul de informații.

(18) Agenția ar trebui să agrege și să analizeze rapoartele naționale primite de la CSIRT și CERT-UE, stabilind norme, limbaje și terminologii comune pentru schimbul de informații. Agenția ar trebui, de asemenea, să atragă participarea sectorului privat, în cadrul Directivei privind securitatea rețelelor și a informațiilor care a prevăzut bazele schimbului voluntar de informații tehnice la nivel operațional, creând rețeaua CSIRT.

(19) Agenția ar trebui să contribuie la răspunsul la nivelul UE în caz de crize și incidente transfrontaliere de securitate cibernetică de mare amploare. Această funcție ar trebui să includă colectarea de informații relevante și exercitarea rolului de facilitare între rețeaua CSIRT și comunitatea tehnică, precum și cu factorii de decizie responsabili cu gestionarea situațiilor de criză. În plus, agenția ar putea sprijini din punct de vedere tehnic administrarea incidentelor, facilitând schimbul de soluții tehnice relevante între statele membre și contribuind la comunicarea publică. Agenția ar trebui să sprijine acest proces testând modalitățile de desfășurare a acestei cooperări prin intermediul exercițiilor anuale de securitate cibernetică.

(20) Pentru îndeplinirea sarcinilor sale operaționale, agenția ar trebui să apeleze la expertiza de care dispune CERT-UE, prin intermediul unei cooperări structurate, în imediata vecinătate fizică. Cooperarea structurată va facilita sinergiile necesare și consolidarea expertizei ENISA. Dacă este cazul, între cele două organizații ar trebui

încheiate acorduri specifice pentru a se stabili modalitățile practice de punere în aplicare a acestei cooperări.

(21) În conformitate cu sarcinile sale operaționale, agenția ar trebui să aibă posibilitatea de a oferi sprijin statelor membre, de exemplu prin furnizarea de consiliere sau asistență tehnică sau prin asigurarea analizelor amenințărilor și incidentelor. Recomandarea Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare invită statele membre să coopereze cu bună credință și să facă schimb de informații între ele și cu ENISA cu privire la incidentele și crizele de securitate cibernetică de mare amploare, fără întârzieri nejustificate. Aceste informații ar trebui să constituie pentru ENISA un ajutor suplimentar în îndeplinirea sarcinilor sale operaționale.

(22) Ca parte a cooperării periodice la nivel tehnic desfășurate pentru a sprijini cunoașterea de către Uniune a situației, agenția ar trebui să pregătească periodic Raportul asupra situației tehnice a incidentelor și amenințărilor de securitate cibernetică în UE, pe baza informațiilor disponibile în mod public, a propriei analize și a rapoartelor care i-au fost transmise de CSIRT ale statelor membre (în mod voluntar) sau de punctele unice de contact instituite prin Directiva privind securitatea rețelelor și a informațiilor, de Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol și CERT-UE și, după caz, de Centrul de analiză a informațiilor al Uniunii Europene (INTCEN) din cadrul Serviciului European de Acțiune Externă (SEAE). Raportul ar trebui să fie pus la dispoziția structurilor relevante ale Consiliului, Comisiei, Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate și ale rețelei CSIRT.

(23) Anchetele tehnice ex-post privind incidentele care au consecințe importante într-unul sau mai multe state membre, realizate cu sprijinul agenției sau întreprinse de aceasta la cererea sau cu acordul statelor membre afectate ar trebui să se axeze asupra prevenirii viitoarelor incidente și să fie efectuate fără a aduce atingere eventualelor proceduri judiciare sau administrative destinate stabilirii culpei sau răspunderii.

(24) Statele membre afectate ar trebui să furnizeze agenției informațiile și asistența necesare în scopul anchetei fără a aduce atingere articolului 346 din Tratatul privind funcționarea Uniunii Europene sau altor rațiuni de ordine publică.

(25) Statele membre pot invita întreprinderile afectate de incident să coopereze furnizând agenției informațiile și asistența necesare, fără a aduce atingere dreptului lor de a proteja informații sensibile din punct de vedere comercial.

(26) Pentru a înțelege mai bine provocările din domeniul securității cibernetice și a oferi consiliere strategică pe termen lung statelor membre și instituțiilor Uniunii, este necesar ca agenția să analizeze riscurile actuale și pe cele emergente. În acest scop, agenția ar trebui să colecteze informațiile relevante în cooperare cu statele membre și, după caz, cu organismele de statistică și cu alte entități, să efectueze analize privind tehnologiile emergente și să furnizeze evaluări tematice privind impactul societal, juridic, economic și în materie de reglementare al inovațiilor tehnologice asupra securității rețelelor și informațiilor, în special asupra securității cibernetice. În plus, agenția ar trebui să sprijine statele membre și instituțiile, agențiile și organele Uniunii în ceea ce privește identificarea tendințelor emergente și prevenirea problemelor legate de securitatea cibernetică, prin efectuarea de analize ale amenințărilor și incidentelor.

(27) Pentru a spori reziliența Uniunii, agenția ar trebui să vizeze excelența în materie de securitate a infrastructurii de internet și a infrastructurilor critice, furnizând consiliere,

orientări și bune practici. În vederea asigurării unui acces mai ușor la informații mai bine structurate privind riscurile de securitate cibernetică și potențialele măsuri corective, agenția ar trebui să creeze și să întrețină „platforma de informare” a Uniunii, un portal de tip ghișeu unic care să permită publicului să obțină informațiile despre securitatea cibernetică ce provin de la instituțiile, agențiile și organismele UE și naționale.

(28) Agenția ar trebui să contribuie la sensibilizarea publicului cu privire la riscurile legate de securitatea cibernetică și să furnizeze, în atenția cetățenilor și organizațiilor, orientări privind bunele practici care trebuie adoptate de utilizatorii individuali. De asemenea, agenția ar trebui să contribuie la promovarea celor mai bune practici și soluții în rândul persoanelor fizice și organizațiilor, prin colectarea și analiza informațiilor aflate la dispoziția publicului referitoare la incidentele semnificative și prin întocmirea de rapoarte cu scopul de a furniza orientări întreprinderilor și cetățenilor și de a îmbunătăți nivelul global de pregătire și reziliență. În plus, agenția ar trebui să organizeze, în cooperare cu instituțiile, organele, oficiile și agențiile statelor membre și ale Uniunii, activități de informare periodice și campanii publice de educație pentru utilizatorii finali, având ca scop promovarea unor comportamente individuale online mai sigure și sensibilizarea cu privire la eventualele pericole din spațiul cibernetic, inclusiv actele de criminalitate cibernetică, cum ar fi atacurile de tip *phishing*, rețelele *botnet*, fraudele financiare și bancare, precum și promovarea consilierii de bază privind autentificarea și protecția datelor. Agenția ar trebui să joace un rol central în accelerarea sensibilizării utilizatorilor finali cu privire la securitatea dispozitivelor.

(29) Pentru a sprijini întreprinderile din sectorul securității cibernetice, precum și utilizatorii de soluții de securitate cibernetică agenția ar trebui să înființeze un „observator al pieței” și să asigure întreținerea acestuia, efectuând analize periodice ale principalelor tendințe ale pieței securității cibernetice, atât la nivelul cererii, cât și la nivelul ofertei, și diseminând aceste tendințe.

(30) Pentru a asigura îndeplinirea în totalitate a obiectivelor sale, agenția ar trebui să colaboreze cu instituțiile, agențiile și organismele relevante, inclusiv cu CERT-UE, Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol, Agenția Europeană de Apărare (AEA), Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă (eu-LISA), Agenția Europeană de Siguranță a Aviației (AESA) și orice altă agenție a UE implicată în securitatea cibernetică. Agenția ar trebui, de asemenea, să colaboreze cu autoritățile care îndeplinesc sarcini de protecție a datelor pentru a face schimb de cunoștințe de specialitate și de bune practici și pentru a oferi consiliere privind aspectele legate de securitatea cibernetică ce ar putea avea un impact asupra activității acestora. Reprezentanții autorităților naționale și ale Uniunii responsabile de aplicarea legii și de protecția datelor ar trebui să fie eligibili pentru a fi reprezentați în grupul permanent al părților interesate din cadrul agenției. În activitatea sa de colaborare cu organele responsabile de aplicarea legii, cu privire la aspectele de securitate a rețelelor și a informațiilor care ar putea avea un impact asupra activității acestora, agenția ar trebui să respecte canalele de informații și rețelele existente.

(31) Agenția, în calitate de membru care, în plus, asigură secretariatul rețelei CSIRT, ar trebui să sprijine echipele de intervenție în caz de incidente de securitate informatică (CSIRT) ale statelor membre și CERT-UE în ceea ce privește cooperarea operațională care are drept obiect toate sarcinile relevante ale rețelei CSIRT, astfel cum sunt definite prin Directiva privind securitatea rețelelor și a informațiilor. De asemenea,

agenția ar trebui să promoveze și să sprijine cooperarea dintre CSIRT relevante în caz de incidente, atacuri sau întreruperi la nivelul rețelelor sau al infrastructurilor gestionate sau protejate de CSIRT și care implică sau pot implica cel puțin două CERT, ținând seama în mod corespunzător de procedurile standard de operare ale rețelei CSIRT.

(32) Pentru ca Uniunea să fie mai bine pregătită să răspundă la incidentele de securitate cibernetică, agenția ar trebui să organizeze exerciții anuale de securitate cibernetică la nivelul Uniunii și, la cererea acestora, să ajute statele membre și instituțiile, agențiile și organele UE să organizeze exerciții.

(33) Agenția ar trebui să își dezvolte și să își mențină în continuare expertiza în materie de certificare de securitate cibernetică, pentru a sprijini politicile Uniunii din acest domeniu. Aceasta ar trebui să promoveze adoptarea certificării de securitate cibernetică în Uniune. În acest scop, ea ar trebui, printre altele, să contribuie la instituirea și întreținerea unui cadru de certificare de securitate cibernetică la nivelul Uniunii, astfel încât asigurarea securității cibernetice a produselor și serviciilor TIC să devină mai transparentă, iar piața internă digitală să se bucure, astfel, de o mai mare încredere.

(34) Politicile de securitate cibernetică eficiente ar trebui să se bazeze pe metode de evaluare a riscurilor bine puse la punct, atât în sectorul public cât și în sectorul privat. Metodele de evaluare a riscurilor sunt utilizate la diferite niveluri, fără a exista o practică comună în ceea ce privește aplicarea lor eficientă. Promovarea și dezvoltarea celor mai bune practici pentru evaluarea riscurilor și pentru soluții interoperabile de gestionare a riscurilor în cadrul organizațiilor din sectorul public și privat vor spori nivelul de securitate cibernetică din Uniune. În acest scop, agenția ar trebui să sprijine cooperarea dintre părțile interesate la nivelul Uniunii, facilitând eforturile acestora referitoare la elaborarea și adoptarea de standarde europene și internaționale în ceea ce privește gestionarea riscurilor și securitatea măsurabilă a produselor, sistemelor, rețelelor și serviciilor electronice, care, împreună cu software-ul, formează rețelele și sistemele informatice.

(35) Agenția ar trebui să încurajeze statele membre și furnizorii de servicii să-și ridice standardele generale de securitate, astfel încât toți utilizatorii de internet să poată lua măsurile necesare pentru a-și asigura securitatea cibernetică personală. În particular, furnizorii de servicii și fabricanții de produse ar trebui să retragă sau să recicleze produsele și serviciile care nu îndeplinesc standardele de securitate cibernetică. În cooperare cu autoritățile competente, ENISA poate difuza informații privind nivelul de securitate cibernetică al produselor și serviciilor oferite pe piața internă și emite avertismente prin care să oblige furnizorii și fabricanții să îmbunătățească securitatea, inclusiv cibernetică, a produselor și serviciilor lor.

(36) Agenția ar trebui să ia în considerare pe deplin activitățile în curs de cercetare, dezvoltare și evaluare tehnologică, în special cele desfășurate în cadrul diferitelor inițiative de cercetare ale Uniunii, în scopul de a consilia instituțiile, organele, oficiile și agențiile Uniunii și, după caz, statele membre, la solicitarea acestora, cu privire la necesitățile în materie de cercetare în domeniul securității rețelelor și a informațiilor, în special în ceea ce privește securitatea cibernetică.

(37) Problemele legate de securitatea cibernetică au o dimensiune mondială. Este necesară consolidarea cooperării internaționale pentru îmbunătățirea standardelor de securitate, inclusiv prin definirea de norme de comportament comune, schimburi de informații și promovarea unei colaborări internaționale mai rapide ca reacție la problemele de

securitate a rețelelor și a informațiilor, precum și a unei abordări comune la nivel mondial a acestor probleme. În acest scop, agenția ar trebui să sprijine continuarea implicării și cooperării Uniunii cu țări terțe și cu organizații internaționale, furnizând, după caz, expertiza și analiza necesară instituțiilor, organelor, oficiilor și agențiilor Uniunii.

(38) Agenția ar trebui să fie în măsură să răspundă solicitărilor ad-hoc de consiliere și asistență care îi sunt adresate de către instituțiile, agențiile și organele statelor membre și ale UE, care se încadrează în obiectivele agenției.

(39) Este necesar să se aplice anumite principii privind guvernanța agenției pentru a se respecta declarația comună și abordarea comună convenite în iulie 2012 de Grupul de lucru interinstituțional privind agențiile descentralizate ale UE, al căror scop este de a raționaliza activitățile agențiilor și de a le îmbunătăți performanțele. Declarația comună și abordarea comună ar trebui să se reflecte, după caz, și în programele de activitate, evaluările și practicile administrative și de raportare ale agenției.

(40) Consiliul de administrație, alcătuit din reprezentanți ai statelor membre și ai Comisiei, ar trebui să traseze direcția generală a activităților agenției și să se asigure că aceasta își îndeplinește sarcinile în conformitate cu prezentul regulament. Consiliului de administrație ar trebui să i se încredințeze competențele necesare pentru întocmirea bugetului, verificarea execuției acestuia, adoptarea normelor financiare adecvate, stabilirea unor proceduri de lucru transparente pentru luarea deciziilor de către agenție, adoptarea documentului unic de programare al agenției, adoptarea propriului regulament de procedură, numirea directorului executiv, luarea deciziei cu privire la prelungirea sau încetarea mandatului directorului executiv.

(41) Pentru buna funcționare în condiții de eficacitate a agenției, Comisia și statele membre ar trebui să se asigure că persoanele care urmează să fie numite în consiliul de administrație au nivelul adecvat de competență și experiență profesională în domeniile funcționale. Comisia și statele membre ar trebui, de asemenea, să depună eforturi pentru a limita rotația reprezentanților lor în consiliul de administrație, cu scopul de a asigura continuitatea activității acestuia.

(42) Pentru buna funcționare a agenției este necesar ca numirea directorului executiv să fie făcută pe baza meritelor și aptitudinilor sale administrative și manageriale atestate, precum și a competenței și experienței relevante în domeniul securității cibernetice și, de asemenea, este necesar ca directorul executiv să își ducă la îndeplinire atribuțiile în deplină independență. Directorul executiv ar trebui să elaboreze o propunere privind programul de activitate al agenției, după consultări prealabile cu Comisia, și să ia toate măsurile necesare pentru a asigura îndeplinirea corespunzătoare a programului de activitate al agenției. Directorul executiv ar trebui să întocmească un raport anual care să fie prezentat consiliului de administrație, să elaboreze un proiect de declarație de venituri și cheltuieli estimate ale agenției și să execute bugetul. În plus, directorul executiv ar trebui să aibă opțiunea de a înființa grupuri de lucru ad-hoc pentru a aborda aspecte specifice, în special de natură științifică, tehnică, juridică sau socioeconomică. Directorul executiv ar trebui să se asigure că selecționarea membrilor grupurilor de lucru ad-hoc se realizează în conformitate cu cele mai înalte standarde de competență, ținând cont în mod corespunzător de o reprezentare echilibrată – după caz, în funcție de problemele specifice – între administrațiile publice ale statelor membre, instituțiile Uniunii și sectorul privat, inclusiv industria, utilizatorii și experții universitari în domeniul securității rețelelor și a informațiilor.

(43) Comitetul executiv ar trebui să contribuie la funcționarea eficace a consiliului de administrație. În cadrul lucrărilor sale pregătitoare legate de deciziile consiliului de administrație, comitetul executiv ar trebui să examineze în detaliu informațiile relevante, să analizeze opțiunile disponibile și să ofere consiliere și soluții pentru pregătirea deciziilor relevante ale consiliului de administrație.

(44) Agenția ar trebui să aibă drept organism consultativ un grup permanent al părților interesate, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Grupul permanent al părților interesate, instituit de consiliul de administrație la propunerea directorului executiv, ar trebui să se concentreze pe probleme relevante pentru părțile interesate și să le aducă în atenția agenției. Componența grupului permanent al părților interesate și sarcinile încredințate acestuia, care urmează să fie consultat în special în legătură cu proiectul de program de activitate, ar trebui să asigure faptul că părțile interesate sunt reprezentate într-o măsură suficientă în ceea ce privește activitatea agenției .

(45) Agenția ar trebui să dispună de norme de prevenire și gestionare a conflictelor de interese. De asemenea, agenția ar trebui să aplice dispozițiile relevante ale Uniunii privind accesul public la documente, prevăzute în Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[34]. Prelucrarea datelor cu caracter personal de către agenție ar trebui să intre sub incidența Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date[35]. Agenția ar trebui să se conformeze dispozițiilor aplicabile instituțiilor Uniunii, precum și dispozițiilor legislațiilor naționale privind gestionarea informațiilor, în special a informațiilor sensibile neclasificate și a informațiilor UE clasificate.

(46) Pentru a garanta autonomia și independența deplină a agenției și a-i permite să îndeplinească sarcini suplimentare și noi, inclusiv sarcini urgente neprevăzute, ar trebui alocat agenției un buget suficient și autonom, ale cărui venituri să provină în principal din contribuția Uniunii și din contribuții ale țărilor terțe care iau parte la activitățile agenției. Majoritatea angajaților agenției ar trebui să fie implicați direct în punerea în aplicare operațională a mandatului agenției. Statul membru gazdă sau oricare alt stat membru ar trebui să poată contribui în mod voluntar la veniturile agenției. Procedura bugetară a Uniunii ar trebui să rămână aplicabilă în ceea ce privește toate subvențiile plătibile din bugetul general al Uniunii. De asemenea, Curtea de Conturi ar trebui să auditeze conturile agenției pentru a asigura transparența și responsabilitatea.

(47) Evaluarea conformității înseamnă procesul prin care se arată dacă s-au îndeplinit cerințele specificate pentru un produs, un proces, un serviciu, un sistem, o persoană sau un organism. În sensul prezentului regulament, certificarea ar trebui să fie considerată ca fiind un tip de evaluare a conformității care să aibă drept obiect caracteristicile de securitate cibernetică ale unui produs, unui proces, unui serviciu, unui sistem sau ale unei combinații a acestora („produsele și serviciile TIC”), efectuată de o parte terță independentă, alta decât fabricantul sau furnizorul de servicii. În sine,

---

[34] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

[35] JO L 8, 12.1.2001, p. 1.

certificarea nu poate garanta că produsele și serviciile TIC certificate îndeplinesc condițiile de securitate cibernetică. Este vorba, mai degrabă, de o procedură și o metodologie tehnică menite să ateste faptul că produsele și serviciile TIC au fost testate și că îndeplinesc anumite cerințe de securitate cibernetică prevăzute în alte dispoziții, de exemplu specificate în cadrul standardelor tehnice.

(48) Certificarea de securitate cibernetică este importantă pentru sporirea securității produselor și a serviciilor TIC și a încrederii de care se bucură acestea. Piața unică digitală și mai ales economia bazată pe date și internetul obiectelor pot prospera numai dacă publicul larg are încredere în faptul că aceste produse și servicii oferă un anumit nivel de asigurare a securității cibernetice. Autovehiculele conectate și automatizate, dispozitivele medicale electronice, sistemele industriale automatizate de control sau rețelele inteligente sunt numai câteva exemple de sectoare în care certificarea este deja utilizată la scară largă sau poate fi utilizată în viitorul apropiat. Certificarea de securitate cibernetică este esențială și în sectoarele reglementate prin Directiva privind securitatea rețelelor și a informațiilor.

(49) În comunicarea sa din 2016 intitulată „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator”, Comisia a subliniat faptul că sunt necesare produse și soluții de securitate cibernetică caracterizate prin calitate superioară, accesibilitatea prețului și interoperabilitate. Oferta de produse și servicii TIC din cadrul pieței unice rămâne foarte fragmentată din punct de vedere geografic. Această fragmentare se explică prin faptul că industria securității cibernetice din Europa s-a dezvoltat de-a lungul timpului în principal pe baza cererii guvernamentale naționale. În plus, lipsa de soluții interoperabile (standarde tehnice), de practici și de mecanisme de certificare la nivelul UE este una dintre lacunele care afectează piața unică în domeniul securității cibernetice. Pe de o parte, acest lucru îngreunează competitivitatea întreprinderilor europene la nivel național, european și mondial, iar pe de altă parte, reduce posibilitățile de alegere a tehnologiilor de securitate cibernetică viabile și utilizabile la care au acces persoanele fizice și întreprinderile. În mod similar, în cadrul evaluării la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală, Comisia a evidențiat necesitatea ca produsele și sistemele conectate să fie sigure și a apreciat că prin crearea unui cadru european de securitate pentru TIC, care să stabilească norme privind modul de organizare a certificării de securitate a TIC în Uniune, internetul s-ar putea bucura în continuare de încredere și, totodată, actuala fragmentare a pieței securității cibernetice ar putea fi contracarată.

(50) În prezent, certificarea de securitate cibernetică a produselor și serviciilor TIC nu este utilizată decât într-o măsură limitată. Atunci când există, certificarea se aplică în principal la nivelul statelor membre sau în cadrul sistemelor instituite de sector. În acest context, un certificat emis de o autoritate națională de securitate cibernetică nu este, în principiu, recunoscut de celelalte state membre. Prin urmare, este posibil ca întreprinderile să fie nevoite să își certifice produsele și serviciile în fiecare dintre statele membre în care își desfășoară activitatea, pentru a putea participa, de exemplu, la procedurile de achiziții publice naționale. În plus, deși apar noi sisteme, nu pare să existe o abordare coerentă și holistică a aspectelor orizontale ale securității cibernetice, de exemplu în domeniul internetului obiectelor. Sistemele existente prezintă importante deficiențe și diferențe în ceea ce privește produsele vizate, nivelurile de asigurare, criteriile de fond și utilizarea efectivă.

(51) În trecut s-au depus eforturi pentru ca certificatele să beneficieze de o recunoaștere reciprocă în Europa, dar acestea nu au fost decât parțial încununate de succes. Cel mai

important exemplu în acest sens îl constituie Acordul de recunoaștere reciprocă (ARR) al Grupului înalților funcționari pentru securitatea sistemelor informatice (SOG-IS). Deși reprezintă cel mai important model de cooperare și de recunoaștere reciprocă din domeniul certificării de securitate, ARR al SOG-IS are importante deficiențe legate de costurile sale ridicate și de domeniul de aplicare limitat. Până în prezent, au fost create numai câteva profiluri de protecție pentru produsele digitale, de exemplu pentru semnătura electronică, tahografele digitale și cardurile inteligente. Principalul inconvenient constă în faptul că SOG-IS nu cuprinde decât o parte din statele membre ale Uniunii. Din această cauză, ARR al SOG-IS a avut o eficacitate restrânsă din perspectiva pieței interne.

(52) Având în vedere cele de mai sus, este necesar să se instituie un cadru european de certificare de securitate cibernetică prin care să se stabilească principalele cerințe orizontale pentru sistemele europene de certificare de securitate cibernetică ce urmează să fie create și să se permită recunoașterea și utilizarea în toate statele membre a certificatelor pentru produse și servicii TIC. Cadrul european ar trebui să aibă o dublă finalitate: pe de o parte, acesta ar trebui să contribuie la creșterea încrederii în produsele și serviciile TIC care au fost certificate în conformitate cu aceste sisteme, pe de altă parte, cadrul ar trebui să evite multiplicarea de certificări naționale de securitate cibernetică ce se contrazic sau se suprapun și să permită astfel reducerea costurilor pentru întreprinderile care își desfășoară activitatea pe piața unică digitală. Aceste sisteme ar trebui să fie nediscriminatorii și să se bazeze pe standarde internaționale și/sau ale Uniunii, cu excepția cazului în care aceste standarde sunt ineficace sau inadecvate pentru îndeplinirea obiectivelor legitime ale UE în această privință.

(53) Comisia ar trebui să fie împuternicită să adopte sisteme europene de certificare de securitate cibernetică în ceea ce privește grupuri specifice de produse și servicii TIC. Aceste sisteme ar trebui să fie puse în aplicare și supervizate de către autoritățile naționale de supraveghere în materie de certificare, iar certificatele emise în cadrul acestor sisteme ar trebui să fie valabile și recunoscute în întreaga Uniune. Sistemele de certificare gestionate de către industrie sau alte organizații private nu ar trebui să fie incluse în domeniul de aplicare al prezentului regulament. Cu toate acestea, organismele care gestionează sisteme de acest tip pot propune Comisiei să le ia în considerare ca bază pentru aprobarea lor ca sistem european.

(54) Dispozițiile prezentului regulament ar trebui să se aplice fără a aduce atingere legislației Uniunii care prevede norme specifice privind certificarea produselor și serviciilor TIC. În special, Regulamentul general privind protecția datelor (RGPD) cuprinde dispoziții privind instituirea de mecanisme de certificare și introducerea de sigilii și mărci de protecție a datelor pentru a demonstra conformitatea cu regulamentul respectiv a operațiunilor de prelucrare efectuate de operatori și de persoanele împuternicite de aceștia. Aceste mecanisme de certificare și sigilii și mărci de protecție a datelor ar trebui să le permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor al produselor și serviciilor în cauză. Prezentul regulament nu aduce atingere certificării operațiunilor de prelucrare a datelor în temeiul RGPD, inclusiv în cazul în care aceste operațiuni sunt integrate în produse și servicii.

(55) Sistemele europene de certificare de securitate cibernetică ar trebui să aibă drept scop asigurarea conformității cu cerințele specificate a produselor și serviciilor TIC certificate în temeiul unui astfel de sistem. Aceste cerințe se referă la capacitatea de a rezista, la un anumit nivel de asigurare, la acțiuni care au scopul de a compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate ori

transmise sau prelucrate ori funcțiile sau serviciile oferite de aceste produse, procese, servicii și sisteme sau accesibile prin intermediul lor, în sensul prezentului regulament. În prezentul regulament nu pot fi detaliate cerințele de securitate cibernetică referitoare la toate produsele și serviciile TIC. Produsele și serviciile TIC și necesitățile conexe în materie de securitate cibernetică sunt atât de variate încât este foarte dificil să se elaboreze cerințe generale de securitate cibernetică cu valabilitate universală. Prin urmare, este necesar să se adopte o noțiune largă și generală a securității cibernetice în scopul certificării, completată printr-o serie de obiective de securitate cibernetică specifice, care trebuie să fie luate în considerare atunci când se concep sisteme europene de certificare de securitate cibernetică. Modalitățile prin care aceste obiective vor fi atinse de produse și servicii TIC specifice ar trebui să fie detaliate și mai precis, într-o etapă ulterioară, la nivelul fiecărui sistem de certificare adoptat de Comisie, de exemplu prin trimitere la standarde sau la specificații tehnice.

(56) Comisia ar trebui să fie împuternicită să adreseze ENISA solicitarea de a pregăti propuneri de sisteme pentru produse sau servicii TIC specifice. Pe baza propunerii de sistem prezentate de ENISA, Comisia ar trebui să fie împuternicită după aceea să adopte sistemul european de certificare de securitate cibernetică prin intermediul unor acte de punere în aplicare. Ținând seama de scopul general și de obiectivele de securitate identificate în prezentul regulament, sistemele europene de certificare de securitate cibernetică adoptate de Comisie ar trebui să specifice un set minim de elemente referitoare la obiectul, domeniul de aplicare și funcționarea fiecărui sistem. Acestea ar trebui să includă, printre altele, domeniul de aplicare și obiectul certificării de securitate cibernetică, inclusiv categoriile de produse și servicii TIC care fac obiectul acesteia, specificații detaliate cu privire la cerințele de securitate cibernetică, de exemplu prin trimitere la standarde sau la specificații tehnice, criteriile specifice și metodele de evaluare, precum și nivelul asigurării vizate: de bază, substanțială și/sau ridicată.

(57) Recurgerea la certificarea europeană de securitate cibernetică ar trebui să rămână voluntară, cu excepția cazului în care există dispoziții contrare în legislația Uniunii sau în cea națională. Cu toate acestea, în scopul îndeplinirii obiectivelor prezentului regulament și pentru a se evita fragmentarea pieței interne, sistemele sau procedurile naționale de certificare de securitate cibernetică pentru produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate cibernetică ar trebui să înceteze să mai producă efecte de la data stabilită de Comisie în actul de punere în aplicare. În plus, statele membre ar trebui să nu introducă noi sisteme naționale de certificare pentru produse și servicii TIC care fac deja obiectul unui sistem european de certificare de securitate cibernetică existent.

(58) Odată ce este adoptat un sistem european de certificare de securitate cibernetică, fabricanții de produse TIC sau furnizorii de servicii TIC ar trebui să aibă posibilitatea de a depune o cerere de certificare a produselor sau serviciilor lor la un organism de evaluare a conformității ales de ei. Organismele de evaluare a conformității ar trebui să fie acreditate de către un organism de acreditare dacă respectă anumite cerințe specificate, stabilite în prezentul regulament. Acreditarea ar trebui să fie acordată pentru o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, dacă organismul de evaluare a conformității îndeplinește cerințele. Organismele de acreditare ar trebui să revoce acreditarea unui organism de evaluare a conformității în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care măsurile luate de un organism de evaluare a conformității încalcă dispozițiile prezentului regulament.

(59) Este necesar să se prevadă obligația ca toate statele membre să desemneze o autoritate de supraveghere în materie de certificare de securitate cibernetică care să verifice dacă organismele de evaluare a conformității și certificatele emise de organismele de evaluare a conformității stabilite pe teritoriul lor respectă cerințele prezentului regulament și ale sistemelor relevante de certificare de securitate cibernetică. Autoritățile naționale de supraveghere în materie de certificare ar trebui să se ocupe de plângerile depuse de persoane fizice sau juridice în legătură cu certificatele emise de organismele de evaluare a conformității stabilite pe teritoriul lor, să investigheze, în măsura în care este oportun, subiectul plângerii și să informeze reclamantul cu privire la progresele și rezultatul investigației, într-un termen rezonabil. În plus, acestea ar trebui să coopereze cu alte autorități naționale de supraveghere în materie de certificare sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor și serviciilor TIC cu cerințele prezentului regulament sau ale sistemelor de securitate cibernetică specifice.

(60) Pentru a asigura aplicarea coerentă a cadrului european de certificare de securitate cibernetică, ar trebui să se instituie un grup european pentru certificarea de securitate cibernetică (denumit în continuare „Grupul”), alcătuit din autorități naționale de supraveghere în materie de certificare. Principalele sarcini ale Grupului ar trebui să constea în a furniza consiliere și asistență Comisiei în activitatea sa pentru a asigura coerența în punerea în aplicare și asigurarea respectării cadrului european de certificare de securitate cibernetică, în a acorda asistență agenției și în a coopera îndeaproape cu aceasta la pregătirea propunerilor de sisteme europene de certificare de securitate cibernetică, în a recomanda Comisiei să solicite agenției să pregătească o propunere de sistem european de certificare de securitate cibernetică și în a adopta avize adresate Comisiei cu privire la întreținerea și revizuirea sistemelor europene de certificare de securitate cibernetică existente.

(61) În vederea sporirii gradului de sensibilizare și pentru a facilita acceptarea viitoarelor sisteme UE de securitate cibernetică, Comisia Europeană poate emite orientări generale sau sectoriale în materie de securitate cibernetică, de exemplu cu privire la bunele practici de securitate cibernetică sau la comportamentul responsabil în materie de securitate cibernetică, subliniind efectul pozitiv al utilizării de produse și servicii TIC certificate.

(62) Sprijinul acordat de agenție pentru certificarea de securitate cibernetică ar trebui să includă și colaborarea cu Comitetul de securitate al Consiliului și cu organismul național relevant, în ceea ce privește aprobarea produselor criptografice în vederea utilizării în rețele clasificate.

(63) Pentru a detalia suplimentar criteriile de acreditare a organismelor de evaluare a conformității, ar trebui să i se delege Comisiei competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE). Comisia ar trebui să desfășoare consultări adecvate în cursul lucrărilor sale pregătitoare, inclusiv la nivel de experți. Aceste consultări ar trebui să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul ar trebui să primească toate documentele în același timp cu experții din statele membre, iar experții acestor instituții să aibă acces în mod sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(64) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentului regulament, Comisia ar trebui învestită cu competențe de executare în situațiile stabilite de prezentul regulament. Competențele respective ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011.

(65) Procedura de examinare ar trebui utilizată pentru adoptarea actelor de punere în aplicare privind sistemele europene de certificare de securitate cibernetică pentru produse și servicii TIC, privind modalitățile de desfășurare a anchetelor întreprinse de agenție, precum și privind circumstanțele, formatele și procedurile pe care trebuie să le respecte autoritățile naționale de supraveghere în materie de certificare pentru a transmite Comisiei notificări privind organismele acreditate de evaluare a conformității.

(66) Funcționarea agenției ar trebui să facă obiectul unei evaluări independente. Evaluarea ar trebui să țină seama de îndeplinirea, de către agenție, a obiectivelor sale, de practicile sale de lucru și de relevanța sarcinilor sale. De asemenea, evaluarea ar trebui să stabilească impactul, eficacitatea și eficiența cadrului european de certificare de securitate cibernetică.

(67) Regulamentul (UE) nr. 526/2013 ar trebui abrogat.

(68) Deoarece obiectivele prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre, dar pot fi realizate 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 enunțat la articolul menționat, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestui obiectiv,

ADOPTĂ PREZENTUL REGULAMENT:

TITLUL I
DISPOZIȚII GENERALE

Articolul 1
Obiect și domeniu de aplicare

În vederea asigurării bunei funcționări a pieței interne, urmărind în același timp atingerea, în Uniune, a unui nivel ridicat de securitate cibernetică, de reziliență cibernetică și de încredere, prezentul regulament:

(a) stabilește obiectivele, sarcinile și aspectele organizaționale ale ENISA, „Agenția UE pentru securitate cibernetică”, denumită în continuare „agenția” și

(b) stabilește un cadru pentru instituirea de sisteme europene de certificare de securitate cibernetică, cu scopul de a asigura un nivel adecvat de securitate cibernetică a produselor și serviciilor TIC în Uniune. Acest cadru se aplică fără a aduce atingere dispozițiilor specifice privind certificarea voluntară sau obligatorie din alte acte ale Uniunii.

Articolul 2
Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

(1) „securitatea cibernetică” cuprinde toate activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor acestora și a persoanelor afectate împotriva amenințărilor cibernetice;

(2) „rețea și sistem informatic” înseamnă un sistem în sensul articolului 4 punctul 1 din Directiva (UE) 2016/1148;

(3) „strategie națională privind securitatea rețelelor și a sistemelor informatice” înseamnă un cadru în sensul articolului 4 punctul 3 din Directiva (UE) 2016/1148;

(4) „operator de servicii esențiale” înseamnă o entitate publică sau privată, astfel cum este definită la articolul 4 punctul 4 din Directiva (UE) 2016/1148;

(5) „furnizor de servicii digitale” înseamnă orice persoană juridică furnizoare a unui serviciu digital, astfel cum este definită la articolul 4 punctul 6 din Directiva (UE) 2016/1148;

(6) „incident” înseamnă orice eveniment definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148;

(7) „administrarea incidentului” înseamnă orice procedură definită la articolul 4 punctul 8 din Directiva (UE) 2016/1148;

(8) „amenințare cibernetică” înseamnă orice circumstanță potențială sau orice eveniment potențial care poate avea un impact negativ asupra rețelelor și a sistemelor informatice, precum și asupra utilizatorilor acestora și a persoanelor afectate;

(9) „sistem european de certificare de securitate cibernetică” înseamnă setul cuprinzător de norme, de cerințe tehnice, de standarde și de proceduri definite la nivelul Uniunii, care se aplică certificării produselor și serviciilor tehnologiei informației și comunicațiilor (TIC) ce se încadrează în domeniul de aplicare al sistemului în cauză;

(10) „certificat european de securitate cibernetică” înseamnă un document eliberat de un organism de evaluare a conformității prin care se atestă că un anumit produs sau serviciu TIC îndeplinește cerințele specifice prevăzute în cadrul unui sistem european de certificare de securitate cibernetică;

(11) „produs și serviciu TIC” înseamnă orice element sau grup de elemente al (ale) rețelelor și al (ale) sistemelor informatice;

(12) „acreditare” înseamnă acreditarea definită la articolul 2 punctul 10 din Regulamentul (CE) nr. 765/2008;

(13) „organism național de acreditare” înseamnă un organism național de acreditare, astfel cum este definit la articolul 2 punctul 11 din Regulamentul (CE) nr. 765/2008;

(14) „evaluarea conformității” înseamnă evaluarea conformității definită la articolul 2 punctul 12 din Regulamentul (CE) nr. 765/2008;

(15) „organism de evaluare a conformității” înseamnă organismul de evaluare a conformității definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008;

(16) „standard” înseamnă un standard, astfel cum este definit la articolul 2 punctul 1 din Regulamentul (UE) nr. 1025/2012;

TITLUL II
ENISA – „Agenția UE pentru securitate cibernetică”

CAPITOLUL I
MANDAT, OBIECTIVE ȘI SARCINI

Articolul 3
Mandat

1. Agenția îndeplinește sarcinile care îi sunt încredințate prin prezentul regulament în scopul de a contribui la asigurarea unui nivel ridicat de securitate cibernetică în Uniune.

2. Agenția duce la îndeplinire sarcinile care îi sunt conferite prin acte legislative ale Uniunii care stabilesc măsuri de apropiere a actelor cu putere de lege și a actelor administrative care au legătură cu securitatea cibernetică ale statelor membre.

3. Obiectivele și sarcinile agenției nu aduc atingere competențelor statelor membre în domeniul securității cibernetice și, în orice caz, nu aduc atingere activităților aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.

Articolul 4
Obiective

1. Agenția este un centru de expertiză în materie de securitate cibernetică, datorită independenței sale, calității științifice și tehnice a consilierii și asistenței acordate și a informațiilor furnizate, transparenței procedurilor și metodelor sale de funcționare, precum și diligenței cu care își îndeplinește sarcinile.

2. Agenția oferă asistență instituțiilor, agențiilor și organelor Uniunii, precum și statelor membre, la elaborarea și punerea în aplicare a politicilor legate de securitatea cibernetică.

3. Agenția sprijină consolidarea capacităților și procesul de pregătire în întreaga Uniune, furnizând asistență Uniunii, statelor membre și părților interesate din sectorul public și privat în vederea sporirii protecției rețelelor și sistemelor informatice, dezvoltării de aptitudini și competențe în domeniul securității cibernetice și obținerii rezilienței cibernetice.

4. Agenția promovează cooperarea și coordonarea la nivelul Uniunii între statele membre, instituțiile, agențiile și organele Uniunii și părțile interesate relevante, inclusiv sectorul privat, cu privire la chestiuni legate de securitatea cibernetică.

5. Agenția sporește capabilitățile de securitate cibernetică la nivelul Uniunii pentru a completa acțiunea statelor membre în materie de prevenire a amenințărilor cibernetice și de reacție la acestea, în special în cazul incidentelor transfrontaliere.

6. Agenția promovează recurgerea la certificare, inclusiv prin contribuția pe care și-o aduce la instituirea și întreținerea unui cadru de certificare de securitate cibernetică la nivelul Uniunii în conformitate cu titlul III din prezentul regulament, astfel încât

asigurarea securității cibernetice a produselor și serviciilor TIC să devină mai transparentă, iar piața internă digitală să se bucure, astfel, de o mai mare încredere.

7. Agenția promovează un nivel ridicat de sensibilizare a cetățenilor și întreprinderilor cu privire la aspectele legate de securitatea cibernetică.

Articolul 5

Sarcini legate de elaborarea și punerea în aplicare a politicii și dreptului Uniunii

Agenția contribuie la elaborarea și punerea în aplicare a politicii și dreptului Uniunii:

1. acordând asistență și consiliere, în special sub formă de avize independente și de lucrări pregătitoare, cu privire la elaborarea și revizuirea politicii și legislației Uniunii în domeniul securității cibernetice, precum și prin inițiative politice și legislative sectoriale în cazul în care sunt implicate aspecte legate de securitatea cibernetică;

2. acordând asistență statelor membre pentru punerea în aplicare în mod coerent a politicii și dreptului Uniunii privind securitatea cibernetică, în special în ceea ce privește Directiva (UE) 2016/1148, inclusiv prin intermediul avizelor, orientărilor, consilierii și bunelor practici referitoare la teme precum gestionarea riscurilor, raportarea incidentelor și schimbul de informații, precum și facilitând schimbul de bune practici între autoritățile competente în această privință;

3. contribuind la activitatea grupului de cooperare instituit în temeiul articolului 11 din Directiva (UE) 2016/1148, prin furnizarea de expertiză și de asistență;

4. sprijinind:

   (1) elaborarea și punerea în aplicare a politicii Uniunii în domeniul identității electronice și al serviciilor de încredere, în special furnizând consiliere și orientări tehnice, precum și facilitarea schimbului de bune practici între autoritățile competente;

   (2) promovarea unui nivel sporit de securitate a comunicațiilor electronice, inclusiv prin furnizarea de expertiză și de consiliere, precum și prin facilitarea schimbului de bune practici între autoritățile competente;

5. sprijinind revizuirea periodică a activităților legate de politicile Uniunii prin furnizarea unui raport anual privind stadiul punerii în aplicare a cadrului juridic aplicabil în ceea ce privește:

   (a) notificările incidentelor transmise de statele membre prin punctul unic de contact grupului de cooperare în temeiul articolului 10 alineatul (3) din Directiva (UE) 2016/1148;

   (b) notificările referitoare la încălcarea securității sau pierderea integrității în ceea ce privește furnizorii de servicii de încredere, transmise agenției de organismele de supraveghere, în temeiul articolului 19 alineatul (3) din Regulamentul (UE) nr. 910/2014;

   (c) notificările privind încălcarea securității primite de la întreprinderile care pun la dispoziție rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului, transmise agenției de autoritățile competente,

în temeiul articolului 40 din [Directiva de instituire a Codului european al comunicațiilor electronice].

Articolul 6

Sarcini legate de consolidarea capacităților

1. Agenția acordă asistență:

(a) statelor membre, în ceea ce privește eforturile lor de a îmbunătăți prevenirea, detectarea și analiza problemelor și incidentelor în materie de securitate cibernetică și capacitatea de răspuns la acestea, prin furnizarea cunoștințelor și a expertizei necesare;

(b) instituțiilor, organelor, oficiilor și agențiilor Uniunii, în ceea ce privește eforturile acestora de a îmbunătăți prevenirea, detectarea și analiza problemelor și incidentelor în materie de securitate cibernetică și capacitatea de răspuns la acestea, printr-un sprijin adecvat acordat Centrului de răspuns la incidente de securitate cibernetică pentru instituțiile, organele și agențiile UE (CERT-UE);

(c) statelor membre, la solicitarea acestora, în ceea ce privește dezvoltarea echipelor naționale de intervenție în caz de incidente de securitate informatică (CSIRT), în temeiul articolului 9 alineatul (5) din Directiva (UE) 2016/1148;

(d) statelor membre, la solicitarea acestora, în ceea ce privește elaborarea strategiilor naționale privind securitatea rețelelor și a sistemelor informatice, în temeiul articolului 7 alineatul (2) din Directiva (UE) 2016/1148; de asemenea, agenția promovează difuzarea acestor strategii în întreaga Uniune și urmărirea progreselor înregistrate în punerea lor în aplicare, pentru a promova bunele practici;

(e) instituțiilor Uniunii, în ceea ce privește elaborarea și revizuirea strategiilor Uniunii referitoare la securitatea cibernetică, promovarea difuzării acestora, precum și urmărirea progreselor înregistrate în punerea lor în aplicare;

(f) echipelor naționale și ale Uniunii de intervenție în caz de incidente de securitate informatică (CSIRT), în ceea ce privește creșterea nivelului capabilităților proprii, inclusiv prin promovarea dialogului și a schimbului de informații, pentru a garanta că, având în vedere stadiul actual al tehnologiei, fiecare CSIRT dispune de un set comun de capabilități minime și funcționează în conformitate cu cele mai bune practici;

(g) statelor membre, prin organizarea exercițiilor anuale la scară largă în materie de securitate cibernetică la nivelul Uniunii menționate la articolul 7 alineatul (6) și prin formularea de recomandări de politici bazate pe procesul de evaluare a exercițiilor și pe învățămintele desprinse în urma acestora;

(h) organismelor publice relevante, prin oferirea de cursuri de formare privind securitatea cibernetică, în cooperare cu părțile interesate acolo unde este cazul;

(i) grupului de cooperare, prin schimbul de bune practici, în special în ceea ce privește identificarea operatorilor de servicii esențiale de către statele membre, inclusiv în legătură cu dependența transfrontalieră legată de riscuri și incidente, în temeiul articolului 11 alineatul (3) litera (l) din Directiva (UE) 2016/1148.

2. Agenția facilitează înființarea centrelor sectoriale de schimb și analiză de informații și le acordă un sprijin continuu, în special în sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, prin furnizarea de bune practici și de orientări privind instrumentele disponibile și procedura, precum și privind modul de abordare a aspectelor de reglementare legate de schimbul de informații.

Articolul 7

Sarcini legate de cooperarea operațională la nivelul Uniunii

1. Agenția sprijină cooperarea operațională dintre organismele publice competente și dintre părțile interesate.

2. Agenția cooperează la nivel operațional și stabilește sinergii cu instituțiile, organele, oficiile și agențiile Uniunii, inclusiv cu CERT-UE, cu serviciile care au atribuții de combatere a criminalității informatice și cu autoritățile de supraveghere care au atribuții de protecție a vieții private și a datelor cu caracter personal, în vederea abordării problemelor de interes comun, inclusiv prin:

   (a) schimbul de know-how și de bune practici;

   (b) furnizarea de consiliere și orientări privind chestiunile relevante legate de securitatea cibernetică;

   (c) stabilirea, după consultarea Comisiei, a modalităților practice pentru executarea unor sarcini specifice.

3. Agenția asigură secretariatul rețelei CSIRT în temeiul articolului 12 alineatul (2) din Directiva (UE) 2016/1148 și facilitează în mod activ schimbul de informații și cooperarea dintre membrii acesteia.

4. Agenția contribuie, de asemenea, la cooperarea operațională din cadrul rețelei CSIRT furnizând sprijin statelor membre, prin:

   (a) consiliere cu privire la modul de îmbunătățire a capabilităților acestora de prevenire și detectare a incidentelor și de răspuns la acestea;

   (b) furnizarea, la cererea lor, de asistență tehnică în cazul incidentelor care au un impact semnificativ sau substanțial;

   (c) analizarea vulnerabilităților, artefactelor și incidentelor.

În îndeplinirea acestor sarcini, agenția și CERT-UE desfășoară o cooperare structurată pentru a beneficia de sinergii, în special în ceea ce privește aspectele operaționale.

5. În urma unei cereri formulate de două sau mai multe state membre afectate și cu singurul scop de a furniza consiliere pentru prevenirea viitoarelor incidente, agenția acordă sprijin sau efectuează o anchetă tehnică *ex post* în urma notificărilor primite de întreprinderile afectate de incidente care au un impact semnificativ sau substanțial, în temeiul Directivei (UE) 2016/1148. De asemenea, agenția efectuează o astfel de anchetă numai în urma unei cereri justificate în mod corespunzător din partea Comisiei, cu acordul statelor membre în cauză, în situația în care astfel de incidente afectează mai mult de două state membre.

Domeniul de aplicare al anchetei și procedura care trebuie să fie urmată pentru efectuarea acesteia sunt stabilite de comun acord de către statele membre în cauză și de agenție și nu aduc atingere niciunei investigații penale în curs privind același incident. La încheierea anchetei, agenția întocmește un raport tehnic final, în special pe baza informațiilor și observațiilor transmise de către statele membre și întreprinderea (întreprinderile) în cauză și de comun acord cu statele membre respective. Un rezumat al raportului, care se concentrează pe recomandările formulate în vederea prevenirii unor viitoare incidente, va fi pus la dispoziția rețelei CSIRT.

6. Agenția organizează exerciții anuale de securitate cibernetică la nivelul UE și sprijină statele membre și instituțiile, agențiile și organele UE în ceea ce privește organizarea de exerciții, la cererea acestora. Exercițiile anuale la nivelul Uniunii includ elemente tehnice, operaționale și strategice și contribuie la pregătirea răspunsului la nivelul UE, bazat pe cooperare, la incidentele de securitate cibernetică transfrontaliere de mare amploare. De asemenea, agenția contribuie la exercițiile sectoriale de securitate cibernetică și sprijină, după caz, organizarea acestora, împreună cu centrele sectoriale de schimb și analiză de informații relevante și permite centrelor respective să participe și ele la exercițiile de securitate cibernetică desfășurate la nivelul Uniunii.

7. Agenția întocmește periodic un raport asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări, pe baza informațiilor din surse deschise, a propriei sale analize și pe baza unor rapoarte care îi sunt transmise de entități cum ar fi, printre altele: CSIRT ale statelor membre (pe bază de voluntariat) sau punctele unice de contact înființate în temeiul Directivei privind securitatea rețelelor și a informațiilor [în conformitate cu articolul 14 alineatul (5) din Directiva privind securitatea rețelelor și a informațiilor], Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol și CERT-UE.

8. Agenția contribuie la pregătirea unui răspuns bazat pe cooperare, atât la nivelul Uniunii, cât și la cel al statelor membre, la incidentele sau crizele transfrontaliere de mare amploare legate de securitatea cibernetică, în principal prin:

   (a) agregarea rapoartelor autorităților naționale, cu scopul de a contribui la o conștientizare comună a situației;

   (b) asigurarea unui flux eficient de informații și furnizarea de mecanisme decizionale de activare între rețeaua CSIRT și factorii de decizie la nivel politic și tehnic ai Uniunii;

   (c) sprijinirea gestionării din punct de vedere tehnic a unui incident sau a unei crize, inclusiv prin facilitarea schimbului de soluții tehnice dintre statele membre;

   (d) sprijinirea comunicării publice cu privire la incident sau la criză;

   (e) testarea planurilor de cooperare pentru răspunsul la aceste incidente sau crize.

Articolul 8

Sarcini legate de piață, de certificarea de securitate cibernetică și de standardizare

Agenția:

(a) sprijină și promovează elaborarea și punerea în aplicare a politicii Uniunii privind certificarea de securitate cibernetică a produselor și serviciilor TIC, astfel cum se prevede în titlul III din prezentul regulament, prin:

(1) pregătirea propunerilor de sisteme europene de certificare de securitate cibernetică pentru produsele și serviciile TIC, în conformitate cu articolul 44 din prezentul regulament;

(2) oferirea de asistență Comisiei în ceea ce privește asigurarea secretariatului Grupului european pentru certificarea de securitate cibernetică, în temeiul articolului 53 din prezentul regulament;

(3) compilarea și publicarea de orientări și dezvoltarea de bune practici în ceea ce privește cerințele în materie de securitate cibernetică pentru produsele și serviciile TIC, în cooperare cu autoritățile naționale de supraveghere în domeniul certificării și cu reprezentanți ai sectorului;

(b) facilitează stabilirea și adoptarea de standarde europene și internaționale pentru gestionarea riscurilor și pentru securitatea produselor și serviciilor TIC, precum și elaborarea, în colaborare cu statele membre, de avize și orientări în ceea ce privește domeniile tehnice legate de cerințele de securitate pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale, precum și în ceea ce privește standardele deja existente, inclusiv standardele naționale ale statelor membre, în temeiul articolului 19 alineatul (2) din Directiva (UE) 2016/1148;

(c) efectuează și diseminează analize periodice privind principalele tendințe de pe piața securității cibernetice, atât din punctul de vedere al cererii, cât și al ofertei, în vederea stimulării pieței securității cibernetice în cadrul Uniunii.

Articolul 9

Sarcini legate de cunoștințe, informații și sensibilizare

Agenția:

(a) efectuează analize ale tehnologiilor emergente și furnizează evaluări tematice privind impactul societal, juridic, economic și asupra reglementărilor pe care se preconizează că îl vor avea inovațiile tehnologice în materie de securitate cibernetică;

(b) efectuează analize strategice pe termen lung ale amenințărilor și incidentelor de securitate cibernetică, pentru a identifica tendințele emergente și a contribui la prevenirea problemelor legate de securitatea cibernetică;

(c) furnizează, în cooperare cu experți ai autorităților statelor membre, consiliere, orientări și bune practici pentru securitatea rețelelor și a sistemelor informatice, în special pentru securitatea infrastructurii de internet și a infrastructurilor care sprijină sectoarele enumerate în anexa II la Directiva (UE) 2016/1148;

(d) colectează, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea cibernetică, furnizate de instituțiile, agențiile și organele Uniunii;

(e) sensibilizează publicul cu privire la riscurile de securitate cibernetică și furnizează orientări cu privire la bune practici pentru utilizatorii individuali, destinate cetățenilor și organizațiilor;

(f) colectează și analizează informațiile disponibile public cu privire la incidentele semnificative și compilează rapoarte, cu scopul de a oferi orientări pentru întreprinderile și cetățenii din întreaga Uniune;

(g) organizează, în cooperare cu statele membre și cu instituțiile, organele, oficiile și agențiile Uniunii, campanii periodice de informare pentru sporirea securității cibernetice și a vizibilității acesteia în Uniune.

Articolul 10
Sarcini legate de cercetare și inovare

În ceea ce privește cercetarea și inovarea, agenția:

(a) consiliază Uniunea și statele membre cu privire la necesitățile și prioritățile în materie de cercetare în domeniul securității cibernetice pentru a face posibile răspunsuri eficace la riscurile și amenințările actuale și emergente, inclusiv în privința tehnologiilor informației și comunicațiilor noi și emergente, și pentru o folosire eficace a tehnologiilor de prevenire a riscurilor;

(b) participă, în cazul în care Comisia i-a delegat competențele relevante, la etapa de punere în aplicare a programelor de finanțare a cercetării și inovării sau în calitate de beneficiar al acestora.

Articolul 11
Sarcini legate de cooperarea internațională

Agenția contribuie la eforturile Uniunii de cooperare cu țări terțe și cu organizații internaționale pentru a promova cooperarea internațională privind aspecte legate de securitatea cibernetică prin:

(a) participarea, după caz, ca observator la organizarea de exerciții internaționale și realizarea de analize și de rapoarte destinate consiliului de administrație privind rezultatele acestor exerciții;

(b) facilitarea, la solicitarea Comisiei, a schimbului de bune practici dintre organizațiile internaționale relevante;

(c) furnizarea de expertiză Comisiei, la cererea acesteia.

CAPITOLUL II
ORGANIZAREA AGENȚIEI

Articolul 12
Structura

Structura administrativă și de conducere a agenției este compusă din următoarele:

(a) un consiliu de administrație, care exercită funcțiile prevăzute la articolul 14;

(b) un comitet executiv, care exercită funcțiile prevăzute la articolul 18;

(c) un director executiv, căruia îi revin responsabilitățile prevăzute la articolul 19, precum și

(d) un grup permanent al părților interesate care exercită funcțiile prevăzute la articolul 20;

SECȚIUNEA 1
CONSILIUL DE ADMINISTRAȚIE

Articolul 13
Componența consiliului de administrație

1. Consiliul de administrație este compus din câte un reprezentant al fiecărui stat membru și din doi reprezentanți numiți de Comisie. Toți reprezentanții au drept de vot.

2. Fiecare membru al consiliului de administrație are un supleant care îl reprezintă în absența sa.

3. Membrii consiliului de administrație și supleanții acestora sunt numiți în funcție de cunoștințele lor în domeniul securității cibernetice, ținând cont de competențele lor manageriale, administrative și bugetare relevante. Comisia și statele membre depun eforturi pentru a limita rotația reprezentanților lor în cadrul consiliului de administrație, cu scopul de a asigura continuitatea activității acestuia. Comisia și statele membre urmăresc obținerea unei reprezentări echilibrate a bărbaților și femeilor în consiliul de administrație.

4. Durata mandatului membrilor consiliului de administrație și al membrilor supleanți este de patru ani. Acest mandat se poate reînnoi.

Articolul 14
Funcțiile consiliului de administrație

1. Consiliul de administrație:

   (a) stabilește direcția generală de funcționare a agenției și se asigură, de asemenea, că agenția funcționează în conformitate cu normele și principiile stabilite în prezentul regulament. Acesta asigură, de asemenea, coerența activității agenției cu activitățile desfășurate de statele membre și cu cele de la nivelul Uniunii;

   (b) adoptă proiectul de document unic de programare al agenției menționat la articolul 21, înainte de transmiterea acestuia la Comisie, spre avizare;

   (c) adoptă, ținând seama de avizul Comisiei, documentul unic de programare al agenției cu o majoritate de două treimi din membrii săi și în conformitate cu articolul 17;

   (d) adoptă, cu o majoritate de două treimi din membrii săi, bugetul anual al agenției și exercită alte funcții privind bugetul agenției în conformitate cu capitolul III;

   (e) evaluează și adoptă raportul anual consolidat privind activitățile agenției și transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi, până la data de 1 iulie a anului următor, atât raportul, cât și evaluarea lui. Raportul anual include conturile agenției și descrie modul

în care aceasta și-a atins indicatorii de performanță. Raportul anual este făcut public;

(f) adoptă normele financiare aplicabile agenției în conformitate cu articolul 29;

(g) adoptă o strategie de combatere a fraudei care să fie proporțională cu riscurile de fraudă, ținând seama de analiza cost-beneficiu a măsurilor care ar urma să fie puse în aplicare;

(h) adoptă norme de prevenire și gestionare a conflictelor de interese în cazul membrilor săi;

(i) asigură luarea măsurilor adecvate pentru a da curs concluziilor și recomandărilor care rezultă din investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și din diferitele rapoarte și evaluări de audit intern sau extern;

(j) adoptă regulamentul său de procedură;

(k) în conformitate cu alineatul (2), exercită, în ceea ce privește personalul agenției, competențele conferite prin Statutul funcționarilor autorității împuternicite să facă numiri și, prin Regimul aplicabil celorlalți agenți ai Uniunii Europene, autorității abilitate să încheie contracte de muncă („competențele de autoritate împuternicită să facă numiri”);

(l) adoptă norme de aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți în conformitate cu procedura prevăzută la articolul 110 din Statutul funcționarilor;

(m) numește directorul executiv și, după caz, îi prelungește mandatul sau îl demite din funcție, în conformitate cu articolul 33 din prezentul regulament;

(n) numește un contabil, care poate fi contabilul Comisiei și care este complet independent în îndeplinirea îndatoririlor sale;

(o) ia toate deciziile privind instituirea structurilor interne ale agenției și, dacă este necesar, privind modificarea acestora, luând în considerare nevoile activității agenției și având în vedere buna gestiune bugetară;

(p) autorizează încheierea acordurilor de lucru în conformitate cu articolele 7 și 39.

2. Consiliul de administrație adoptă, în conformitate cu articolul 110 din Statutul funcționarilor, o decizie în baza articolului 2 alineatul (1) din Statutul funcționarilor și a articolului 6 din Regimul aplicabil celorlalți agenți, prin care competențele relevante de autoritate împuternicită să facă numiri sunt delegate directorului executiv și în care sunt definite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv este autorizat să subdelege aceste competențe.

3. În cazul în care apar împrejurări excepționale care impun acest lucru, consiliul de administrație poate, printr-o decizie, să suspende temporar delegarea competențelor de autoritate împuternicită să facă numiri către directorul executiv și delegarea competențelor subdelegate de către acesta din urmă și să le exercite el însuși sau să le delege unuia dintre membrii săi ori unui alt membru al personalului decât directorul executiv.

Articolul 15

Președintele consiliului de administrație

Consiliul de administrație alege cu o majoritate de două treimi din membrii săi un președinte și un vicepreședinte dintre membrii săi, pentru o perioadă de patru ani, care poate fi reînnoită o dată. Cu toate acestea, dacă pe durata mandatului încetează calitatea acestora de membri ai consiliului de administrație, mandatul lor expiră automat la aceeași dată. Vicepreședintele îl înlocuiește din oficiu pe președinte în cazul în care acesta din urmă nu își poate exercita prerogativele.

Articolul 16

Reuniunile consiliului de administrație

1. Reuniunile consiliului de administrație sunt convocate de către președintele acestuia.
2. Consiliul de administrație se reunește în ședință ordinară cel puțin de două ori pe an. De asemenea, consiliul se reunește în ședință extraordinară la cererea președintelui său, a Comisiei sau la cererea a cel puțin o treime din membrii săi.
3. Directorul executiv ia parte la ședințele consiliului de administrație fără a avea drept de vot.
4. Membrii Grupului permanent al părților interesate pot lua parte la reuniunile consiliului de administrație, la invitația președintelui, fără a avea drept de vot.
5. Membrii consiliului de administrație și supleanții lor pot, sub rezerva regulamentului de procedură, să fie asistați în cursul reuniunilor de consilieri sau de experți.
6. Agenția asigură secretariatul consiliului de administrație.

Articolul 17

Regulile de vot ale consiliului de administrație

1. Consiliul de administrație își adoptă deciziile cu majoritatea membrilor săi.
2. Pentru documentul unic de programare, bugetul anual, numirea, prelungirea mandatului sau demiterea din funcție a directorului executiv este necesară o majoritate de două treimi din toți membrii consiliului de administrație.
3. Fiecare membru dispune de un vot. În absența unui membru, dreptul său de vot poate fi exercitat de supleantul său.
4. Președintele participă la vot.
5. Directorul executiv nu participă la vot.
6. Regulamentul de procedură al consiliului de administrație stabilește în mod detaliat modalitățile de vot, în special condițiile în care un membru poate acționa în numele altui membru.

SECȚIUNEA 2
COMITETUL EXECUTIV

Articolul 18
Comitetul executiv

1. Consiliul de administrație este asistat de un comitet executiv.

2. Comitetul executiv:

   (a) pregătește deciziile care urmează să fie adoptate de consiliul de administrație;

   (b) asigură, împreună cu consiliul de administrație, luarea măsurilor adecvate pentru a da curs concluziilor și recomandărilor provenite din investigațiile OLAF și diferitele rapoarte și evaluări de audit intern sau extern;

   (c) fără a aduce atingere responsabilităților directorului executiv, prevăzute la articolul 19, îl asistă și îl consiliază pe directorul executiv în ceea ce privește punerea în aplicare a deciziilor consiliului de administrație privind aspecte administrative și bugetare în temeiul articolului 19.

3. Comitetul executiv este format din cinci membri numiți dintre membrii consiliului de administrație, printre care președintele consiliului de administrație, care poate prezida și comitetul executiv, și unul dintre reprezentanții Comisiei. Directorul executiv ia parte la reuniunile comitetului executiv, dar nu are drept de vot.

4. Durata mandatului membrilor comitetului executiv este de patru ani. Acest mandat se poate reînnoi.

5. Comitetul executiv se întrunește cel puțin o dată la trei luni. Președintele comitetului executiv convoacă reuniuni suplimentare la cererea membrilor săi.

6. Consiliul de administrație stabilește regulamentul de procedură al comitetului executiv.

7. Atunci când este necesar din motive de urgență, comitetul executiv poate lua anumite decizii provizorii în numele consiliului de administrație, îndeosebi cu privire la aspecte legate de gestionarea administrativă, inclusiv la suspendarea delegării competențelor de autoritate împuternicită să facă numiri, precum și cu privire la aspecte bugetare.

SECȚIUNEA 3
DIRECTORUL EXECUTIV

Articolul 19
Responsabilitățile directorului executiv

1. Agenția este condusă de un director executiv care este independent în îndeplinirea atribuțiilor sale. Directorul executiv răspunde în fața consiliului de administrație.

2. Directorul executiv prezintă Parlamentului European un raport privind modul în care și-a îndeplinit atribuțiile, atunci când este invitat să facă acest lucru. Consiliul poate solicita directorului executiv să prezinte un raport cu privire la îndeplinirea atribuțiilor sale.

3. Directorul executiv răspunde de:

(a) administrarea curentă a agenției;

(b) punerea în aplicare a deciziilor adoptate de consiliul de administrație;

(c) elaborarea unui proiect de document unic de programare și prezentarea acestuia consiliului de administrație spre aprobare, înainte de a fi trimis Comisiei;

(d) punerea în aplicare a documentului unic de programare și raportarea către consiliul de administrație cu privire la aceasta;

(e) pregătirea raportului anual consolidat privind activitățile agenției și prezentarea acestuia consiliului de administrație, spre evaluare și adoptare;

(f) pregătirea unui plan de acțiune pentru a da curs concluziilor evaluărilor retrospective și trimiterea către Comisie, la fiecare doi ani, a unui raport privind progresele înregistrate;

(g) elaborarea unui plan de acțiune în urma concluziilor rapoartelor de audit intern sau extern, precum și a investigațiilor desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și prezentarea, de două ori pe an Comisiei și periodic consiliului de administrație, a unui raport privind progresele înregistrate;

(h) elaborarea proiectului de norme financiare aplicabile agenției;

(i) întocmirea proiectului situației estimărilor de venituri și cheltuieli ale agenției și execuția bugetului acesteia;

(j) protejarea intereselor financiare ale Uniunii prin aplicarea de măsuri preventive de combatere a fraudei, a corupției și a altor activități ilegale, prin realizarea de controale eficace și, dacă se constată nereguli, prin recuperarea sumelor plătite nejustificat și, dacă este cazul, prin sancțiuni administrative și financiare eficace, proporționale și disuasive;

(k) pregătirea unei strategii antifraudă pentru agenție și prezentarea acesteia consiliului de administrație, spre adoptare;

(l) stabilirea și menținerea contactului cu comunitatea de afaceri și cu organizațiile consumatorilor, în vederea asigurării unui dialog periodic cu părțile interesate relevante;

(m) îndeplinirea altor sarcini care îi sunt încredințate directorului executiv prin prezentul regulament.

4. După caz, în limitele mandatului și în conformitate cu obiectivele și sarcinile agenției, directorul executiv poate înființa grupuri de lucru ad-hoc compuse din experți, inclusiv din rândul autorităților competente ale statelor membre. Consiliul de administrație este informat în prealabil. Procedurile referitoare în special la componența grupurilor de lucru, la numirea experților acestora de către directorul executiv și la funcționarea lor sunt prevăzute în regulamentul intern de funcționare al agenției.

5. Directorul executiv decide dacă este necesar ca membri ai personalului să fie stabiliți într-unul sau mai multe state membre în scopul îndeplinirii sarcinilor agenției într-un mod eficient și eficace. Înainte de a decide să înființeze un birou local, directorul executiv obține acordul prealabil al Comisiei, al consiliului de administrație și al statului membru (statelor membre) în cauză. Decizia respectivă precizează domeniul de aplicare al activităților care urmează să fie efectuate în cadrul respectivului birou local, astfel încât să se evite costurile inutile și dublarea funcțiilor administrative ale agenției. Se încheie un acord cu statul membru (statele membre) în cauză, dacă este oportun sau necesar.

SECȚIUNEA 4
GRUPUL PERMANENT AL PĂRȚILOR INTERESATE

Articolul 20
Grupul permanent al părților interesate

1. La propunerea directorului executiv, consiliul de administrație instituie un grup permanent al părților interesate, alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi sectorul TIC, furnizorii de rețele sau de servicii de comunicații electronice accesibile publicului, grupurile de consumatori, experții universitari în domeniul securității cibernetice și reprezentanți ai autorităților competente notificate în temeiul [Directivei de instituire a Codului European al Comunicațiilor Electronice], precum și autoritățile de aplicare a legii și cele de supraveghere a protecției datelor.
2. Procedurile privind grupul permanent al părților interesate, în special cele referitoare la numărul de membri, componență și numirea membrilor săi de către consiliul de administrație, la propunerea directorului executiv și la funcționarea grupului, se precizează în normele interne de funcționare ale agenției și se fac publice.
3. Grupul permanent al părților interesate este prezidat de directorul executiv sau de orice persoană numită de acesta de la caz la caz.
4. Mandatul membrilor grupului permanent al părților interesate este de doi ani și jumătate. Membrii consiliului de administrație nu pot fi membri ai grupului permanent al părților interesate. Experții Comisiei și ai statelor membre au dreptul de a participa la reuniunile grupului permanent al părților interesate și la activitățile acestuia. Reprezentanții altor organisme considerate relevante de către directorul executiv, care nu au calitatea de membri ai grupului permanent al părților interesate, pot fi invitați să participe la reuniunile grupului permanent al părților interesate și la activitățile acestuia.
5. Grupul permanent al părților interesate acordă consiliere agenției în exercitarea activităților sale. Acesta acordă consiliere în special directorului executiv în ceea ce privește elaborarea unei propuneri de program de activitate al agenției și asigurarea comunicării cu părțile interesate relevante referitor la toate aspectele legate de programul de activitate.

SECȚIUNEA 5
FUNCȚIONARE

Articolul 21
Documentul unic de programare

1. Agenția își desfășoară activitatea în conformitate cu documentul său unic de programare care conține programarea sa anuală și multianuală și care include toate activitățile sale planificate.

2. În fiecare an, directorul executiv elaborează un proiect de document unic de programare care conține programarea anuală și multianuală cu planificarea corespunzătoare a resurselor umane și financiare în conformitate cu articolul 32 din Regulamentul delegat (UE) nr. 1271/2013 al Comisiei[36] și luând în considerare orientările stabilite de Comisie.

3. Până la data de 30 noiembrie a fiecărui an, consiliul de administrație adoptă documentul unic de programare menționat la alineatul (1) și îl transmite Parlamentului European, Consiliului și Comisiei cel târziu până la data de 31 ianuarie a anului următor, împreună cu orice altă versiune ulterioară actualizată a documentului respectiv.

4. Documentul unic de programare devine definitiv după adoptarea finală a bugetului general al Uniunii și, dacă este necesar, se ajustează în mod corespunzător.

5. Programul anual de activitate cuprinde obiectivele detaliate și rezultatele preconizate, inclusiv indicatorii de performanță. Acesta include, de asemenea, o descriere a acțiunilor care urmează să fie finanțate și informații care indică resursele financiare și umane alocate fiecărei acțiuni, în conformitate cu principiile întocmirii bugetului și ale gestionării pe activități. Programul anual de activitate concordă cu programul multianual de activitate menționat la alineatul (7). Acesta indică în mod clar sarcinile care au fost adăugate, modificate sau eliminate față de exercițiul financiar precedent.

6. Consiliul de administrație modifică programul anual de activitate adoptat atunci când agenției îi este încredințată o nouă sarcină. Orice modificare substanțială a programului anual de activitate se adoptă prin aceeași procedură ca cea utilizată în cazul programului inițial. Consiliul de administrație poate să-i delege directorului executiv competența de a aduce modificări nesubstanțiale programului anual de activitate.

7. Programul multianual de activitate stabilește programarea strategică globală, inclusiv obiectivele, rezultatele preconizate și indicatorii de performanță. De asemenea, acesta stabilește programarea resurselor, inclusiv bugetul multianual și personalul.

8. Programarea resurselor se actualizează anual. Programarea strategică se actualizează după caz, în special pentru a ține seama de rezultatul evaluării menționate la articolul 56.

---

[36] Regulamentul delegat (UE) nr. 1271/2013 al Comisiei din 30 septembrie 2013 privind regulamentul financiar cadru pentru organismele menționate la articolul 208 din Regulamentul (UE, Euratom) nr. 966/2012 al Parlamentului European și al Consiliului (JO L 328, 7.12.2013, p. 42)

Articolul 22
Declarația de interese

1. Membrii consiliului de administrație, directorul executiv și funcționarii detașați temporar de statele membre întocmesc, fiecare în parte, o declarație de angajamente și o declarație în care să menționeze absența sau prezența oricăror interese directe sau indirecte despre care s-ar putea considera că aduc atingere independenței lor. Declarațiile sunt exacte și complete, se fac anual, în scris și sunt actualizate ori de câte ori este nevoie.

2. Membrii consiliului de administrație, directorul executiv și experții externi care participă la grupurile de lucru ad-hoc declară, fiecare în parte, precis și complet, cel târziu la începutul fiecărei reuniuni, toate interesele care ar putea fi considerate ca aducând atingere independenței lor în ceea ce privește punctele înscrise pe ordinea de zi și se abțin de la participarea la dezbaterile referitoare la punctele respective și de la votul în legătură cu acestea.

3. Agenția stabilește, în regulamentul său intern de funcționare, modalitățile practice pentru normele referitoare la declarațiile de interese menționate la alineatele (1) și (2).

Articolul 23
Transparența

1. Agenția își desfășoară activitățile cu un nivel ridicat de transparență și în conformitate cu articolul 25.

2. Agenția se asigură că publicului și tuturor părților interesate li se furnizează informații adecvate, obiective, fiabile și ușor accesibile, în special în ceea ce privește rezultatele activității sale. De asemenea, agenția face publice declarațiile de interese întocmite în conformitate cu articolul 22.

3. Consiliul de administrație, pe baza unei propuneri din partea directorului executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile agenției.

4. Agenția stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2).

Articolul 24
Confidențialitatea

1. Fără să aducă atingere articolului 25, agenția nu divulgă terților informațiile pe care le prelucrează sau pe care le primește și pentru care s-a cerut, printr-o solicitare motivată, un tratament confidențial, integral sau parțial.

2. Membrii consiliului de administrație, directorul executiv, membrii grupului permanent al părților interesate, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului agenției, inclusiv funcționarii detașați temporar de statele membre, respectă cerințele de confidențialitate prevăzute la articolul 339 din Tratatul privind funcționarea Uniunii Europene („TFUE”), chiar și după încetarea atribuțiilor lor.

3. Agenția stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor de confidențialitate menționate la alineatele (1) și (2).

4. Dacă este necesar pentru realizarea sarcinilor agenției, consiliul de administrație decide să acorde agenției permisiunea de a gestiona informații clasificate. În acest caz, consiliul de administrație, cu acordul serviciilor Comisiei, adoptă un regulament intern de funcționare care să aplice principiile de securitate cuprinse în deciziile (UE, Euratom) 2015/443[37] și 2015/444[38] ale Comisiei. Regulamentul intern respectiv include dispoziții privind schimbul, prelucrarea și stocarea informațiilor clasificate.

Articolul 25
Accesul la documente

1. Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de agenție.

2. Consiliul de administrație adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001 în termen de șase luni de la înființarea agenției.

3. Deciziile adoptate de agenție în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului în temeiul articolului 228 din TFUE sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene în temeiul articolului 263 din TFUE.

CAPITOLUL III
ÎNTOCMIREA ȘI STRUCTURA BUGETULUI

Articolul 26
Întocmirea bugetului

1. În fiecare an, directorul executiv elaborează un proiect de situație a estimărilor de venituri și cheltuieli ale agenției pentru următorul exercițiu financiar și îl înaintează consiliului de administrație, împreună cu un proiect de schemă de personal. Veniturile și cheltuielile trebuie să fie în echilibru.

2. În fiecare an, pe baza proiectului situației estimărilor de venituri și cheltuieli menționat la alineatul (1), consiliul de administrație adoptă situația estimărilor de venituri și cheltuieli ale agenției pentru următorul exercițiu financiar.

3. În fiecare an, până la data de 31 ianuarie, consiliul de administrație transmite situația estimărilor menționată la alineatul (2), care face parte din documentul unic de programare, Comisiei și țărilor terțe cu care Uniunea a încheiat acorduri în conformitate cu articolul 39.

4. Pe baza situației estimărilor respective, Comisia înscrie în proiectul de buget al Uniunii estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care urmează să fie suportată din bugetul general, pe care le

[37] Decizia (UE, Euratom) 2015/443 a Comisiei din 13 martie 2015 privind securitatea în cadrul Comisiei (JO L 72, 17.3.2015, p. 41).

[38] Decizia (UE, Euratom) 2015/444 a Comisiei din 13 martie 2015 privind normele de securitate pentru protecția informațiilor UE clasificate (JO L 72, 17.3.2015, p. 53).

prezintă Parlamentului European și Consiliului în conformitate cu articolele 313 și 314 din TFUE.

5. Parlamentul European și Consiliul autorizează creditele reprezentând contribuția alocată agenției.

6. Parlamentul European și Consiliul adoptă schema de personal a agenției.

7. Consiliul de administrație adoptă bugetul agenției odată cu documentul unic de programare al acesteia. Bugetul agenției devine definitiv după adoptarea definitivă a bugetului general al Uniunii. Dacă este cazul, consiliul de administrație ajustează bugetul agenției și documentul unic de programare al acesteia în conformitate cu bugetul general al Uniunii.

Articolul 27
Structura bugetului

1. Fără a se aduce atingere altor resurse, veniturile agenției sunt alcătuite:

   (a) dintr-o contribuție de la bugetul Uniunii;

   (b) din venituri alocate unor cheltuieli specifice în conformitate cu normele sale financiare menționate la articolul 29;

   (c) dintr-o finanțare din partea Uniunii sub forma unor acorduri de delegare sau de granturi ad-hoc, în conformitate cu normele sale financiare menționate la articolul 29 și cu dispozițiile instrumentelor relevante care sprijină politicile Uniunii;

   (d) din eventuale contribuții din partea țărilor terțe care participă la lucrările agenției, astfel cum se prevede la articolul 39;

   (e) din orice contribuție voluntară din partea statelor membre, în bani sau în natură. Statele membre care oferă contribuții voluntare nu pot solicita niciun drept sau serviciu specific ca rezultat al acelor contribuții.

2. Cheltuielile agenției cuprind cheltuieli cu personalul, cheltuieli administrative și de suport tehnic, cheltuieli cu infrastructura și operaționale, precum și cheltuieli rezultate din contracte încheiate cu părți terțe.

Articolul 28
Execuția bugetului

1. Directorul executiv răspunde de execuția bugetului agenției.

2. Auditorul intern al Comisiei exercită asupra agenției aceleași prerogative ca și asupra serviciilor Comisiei.

3. Până la data de 1 martie a fiecărui exercițiu financiar (data de 1 martie a exercițiului N+1), contabilul agenției trimite conturile provizorii contabilului Comisiei și Curții de Conturi.

4. După primirea observațiilor formulate de Curtea de Conturi privind conturile provizorii ale agenției, contabilul agenției întocmește conturile finale ale agenției pe răspunderea sa.

5. Directorul executiv le prezintă consiliului de administrație în vederea obținerii unui aviz.

6. Directorul executiv trimite Parlamentului European, Consiliului, Comisiei și Curții de Conturi, până la data de 31 martie a exercițiului N + 1, raportul privind gestiunea bugetară și financiară.

7. Contabilul transmite Parlamentului European, Consiliului, contabilului Comisiei și Curții de Conturi, până la data de 1 iulie a exercițiului N+1, conturile finale împreună cu avizul consiliului de administrație.

8. La aceeași dată la care transmite conturile finale, contabilul transmite, de asemenea, Curții de Conturi o scrisoare cuprinzând declarațiile conducerii cu privire la aceste conturi finale, o copie a acesteia fiind trimisă contabilului Comisiei.

9. Directorul executiv publică conturile finale până la data de 15 noiembrie a exercițiului următor.

10. Directorul executiv transmite Curții de Conturi un răspuns la observațiile acesteia până la data de 30 septembrie a exercițiului N + 1 și adresează, de asemenea, o copie a răspunsului respectiv consiliului de administrație și Comisiei.

11. Directorul executiv prezintă Parlamentului European, la solicitarea acestuia, toate informațiile necesare pentru buna desfășurare a procedurii de descărcare de gestiune pentru exercițiul financiar în cauză, în conformitate cu dispozițiile articolului 165 alineatul (3) din Regulamentul financiar.

12. La recomandarea Consiliului, Parlamentul European acordă, înaintea datei de 15 mai a exercițiului N + 2, descărcarea de gestiune directorului executiv în ceea ce privește execuția bugetului pentru exercițiul N.

Articolul 29
Normele financiare

Normele financiare aplicabile agenției se adoptă de către consiliul de administrație după consultarea Comisiei. Acestea nu se abat de la Regulamentul (UE) nr. 1271/2013, cu excepția cazului în care funcționarea agenției necesită în mod expres o astfel de abatere, iar Comisia și-a dat acordul prealabil.

Articolul 30
Combaterea fraudei

1. Pentru a facilita, în temeiul Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului[39], combaterea fraudei, corupției și a altor activități ilegale, agenția aderă, în termen de șase luni de la data la care devine operațională, la Acordul interinstituțional din 25 mai 1999 privind investigațiile interne desfășurate de Oficiul European de Luptă Antifraudă (OLAF) și adoptă dispozițiile corespunzătoare care se aplică tuturor angajaților agenției, folosind modelul prevăzut în anexa la respectivul acord.

[39] Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului din 11 septembrie 2013 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF) și de abrogare a Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului și a Regulamentului (Euratom) nr. 1074/1999 al Consiliului (JO L 248, 18.9.2013, p. 1).

2. Curtea de Conturi are competența de a-i audita, pe bază de documente și la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții care au primit fonduri ale Uniunii din partea agenției.

3. OLAF poate efectua investigații, inclusiv controale și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului și în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului[40] din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Uniunii împotriva fraudei și a altor abateri, în scopul de a stabili existența unei fraude, a unui act de corupție sau dacă a avut loc orice altă activitate ilegală care afectează interesele financiare ale Uniunii în legătură cu un grant sau un contract finanțat de agenție.

4. Fără a aduce atingere alineatelor (1), (2) și (3), acordurile de cooperare cu țările terțe și cu organizațiile internaționale, contractele, acordurile de grant încheiate de agenție și deciziile de acordare a unui grant luate de aceasta conțin dispoziții care autorizează în mod expres Curtea de Conturi și OLAF să efectueze astfel de audituri și investigații, în limitele competențelor care le revin.

CAPITOLUL IV
PERSONALUL AGENȚIEI

Articolul 31
Dispoziții generale

Personalului agenției i se aplică Statutul funcționarilor, Regimul aplicabil celorlalți agenți și normele adoptate de comun acord de instituțiile Uniunii pentru punerea în aplicare a Statutului funcționarilor.

Articolul 32
Privilegii și imunități

Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene anexat la Tratatul privind Uniunea Europeană și la TFUE se aplică agenției și personalului acesteia.

Articolul 33
Directorul executiv

1. Directorul executiv este angajat ca agent temporar al agenției în conformitate cu articolul 2 litera (a) din Regimul aplicabil celorlalți agenți.

2. Directorul executiv este numit de consiliul de administrație dintr-o listă de candidați propusă de Comisie, în urma unei proceduri de selecție deschise și transparente.

3. În scopul încheierii contractului directorului executiv, agenția este reprezentată de președintele consiliului de administrație.

[40] Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului din 11 noiembrie 1996 privind controalele și inspecțiile la fața locului efectuate de Comisie în scopul protejării intereselor financiare ale Comunităților Europene împotriva fraudei și a altor abateri (JO L 292, 15.11.1996, p. 2).

4. Înainte de a fi numit în funcție, candidatul selectat de consiliul de administrație este invitat să facă o declarație în fața comisiei competente a Parlamentului European și să răspundă întrebărilor deputaților.

5. Durata mandatului directorului executiv este de cinci ani. Până la sfârșitul perioadei respective, Comisia realizează o analiză care ia în considerare evaluarea rezultatelor obținute de directorul executiv și viitoarele sarcini și provocări cu care se va confrunta agenția.

6. Consiliul de administrație adoptă deciziile privind numirea, prelungirea mandatului sau demiterea din funcție a directorului executiv cu o majoritate de două treimi din membrii săi cu drept de vot.

7. La propunerea Comisiei, care ia în considerare evaluarea menționată la alineatul (5), consiliul de administrație poate reînnoi mandatul directorului executiv o singură dată, cu cel mult cinci ani.

8. Consiliul de administrație informează Parlamentul European în legătură cu intenția sa de a prelungi mandatul directorului executiv. În cursul perioadei de trei luni care precede prelungirea mandatului său, directorul executiv, dacă este invitat, face o declarație în fața comisiei relevante a Parlamentului European și răspunde întrebărilor deputaților.

9. Un director executiv al cărui mandat a fost prelungit nu poate să participe la o nouă procedură de selecție pentru același post.

10. Directorul executiv poate fi demis din funcție numai printr-o decizie a consiliului de administrație care acționează la propunerea Comisiei.

Articolul 34
Experții naționali detașați și alte categorii de personal

1. Agenția poate recurge la experți naționali detașați sau alte categorii de personal care nu sunt angajați ai agenției. Acestor categorii de personal nu li se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți.

2. Consiliul de administrație adoptă o decizie de stabilire a normelor aplicabile detașării experților naționali la agenție.

CAPITOLUL V
DISPOZIȚII GENERALE

Articolul 35
***Statutul juridic* al agenției**

1. Agenția este un organ al Uniunii și are personalitate juridică.

2. În fiecare stat membru, agenția deține cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul legislației naționale. Aceasta poate în special să dobândească sau să înstrăineze bunuri mobile și imobile și să se constituie parte în instanță.

3. Agenția este reprezentată de directorul său executiv.

Articolul 36

Răspunderea agenției

1. Răspunderea contractuală a Agenției este reglementată de legea aplicabilă contractului în cauză.

2. Curtea de Justiție a Uniunii Europene este competentă să se pronunțe în temeiul oricărei clauze compromisorii cuprinse într-un contract încheiat de agenție.

3. În materie de răspundere necontractuală, agenția, în conformitate cu principiile generale comune legislațiilor statelor membre, repară toate prejudiciile cauzate de serviciile sau de angajații proprii în cursul exercitării atribuțiilor lor.

4. Curtea de Justiție a Uniunii Europene este competentă în ceea ce privește toate litigiile privind repararea unor astfel de prejudicii.

5. Răspunderea personală a angajaților față de agenție este reglementată de condițiile relevante care se aplică personalului agenției.

Articolul 37

Regimul lingvistic

1. Agenției i se aplică dispozițiile Regulamentului nr.1 al Consiliului[41]. Statele membre și celelalte organisme desemnate de către acestea se pot adresa agenției și pot primi răspunsuri într-una din limbile oficiale ale instituțiilor Uniunii, la alegerea lor.

2. Serviciile de traducere necesare funcționării agenției sunt asigurate de către Centrul de Traduceri pentru Organismele Uniunii Europene.

Articolul 38

Protecția datelor cu caracter personal

1. Prelucrarea datelor cu caracter personal de către agenție face obiectul Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului[42].

2. Consiliul de administrație adoptă măsurile de punere în aplicare menționate la articolul 24 alineatul (8) din Regulamentul (CE) nr. 45/2001. Consiliul de administrație poate adopta dispozițiile suplimentare necesare pentru aplicarea de către agenție a Regulamentului (CE) nr. 45/2001.

Articolul 39

Cooperarea cu țări terțe și cu organizații internaționale

1. În măsura în care este necesar pentru atingerea obiectivelor stabilite în prezentul regulament, agenția poate coopera cu autoritățile competente din țările terțe sau cu organizațiile internaționale sau cu ambele. În acest scop, agenția poate, sub rezerva aprobării prealabile de către Comisie, să stabilească acorduri de lucru cu autoritățile din țări terțe și cu organizații internaționale. Aceste acorduri nu creează obligații legale pentru Uniune și nici pentru statele sale membre.

---

41 Regulamentul nr. 1 de stabilire a regimului lingvistic al Comunității Europene a Energiei Atomice (JO 17, 6.10.1958, p. 401).

42 Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

2. Agenția este deschisă participării țărilor terțe care au încheiat acorduri cu Uniunea în acest sens. În baza dispozițiilor relevante ale acestor acorduri, se elaborează înțelegeri care să specifice, în special, caracterul, amploarea și modalitatea participării acestor țări la activitatea agenției, inclusiv dispoziții referitoare la participarea la inițiativele puse în practică de agenție, la contribuțiile financiare și la personal. În ceea ce privește chestiunile legate de personal, aceste înțelegeri respectă, în orice caz, Statutul funcționarilor.

3. Consiliul de administrație adoptă o strategie pentru relațiile cu țări terțe sau cu organizații internaționale, în ceea ce privește aspectele pentru care agenția deține competențe. Comisia se asigură că agenția își desfășoară activitatea în limitele mandatului său și ale cadrului instituțional existent prin încheierea unui acord de lucru adecvat cu directorul agenției.

Articolul 40

Normele de *securitate* privind protejarea informațiilor clasificate și a informațiilor sensibile neclasificate

În consultare cu Comisia, agenția își adoptă propriile norme de securitate care pun în aplicare principiile de securitate din normele de securitate ale Comisiei pentru protecția informațiilor clasificate ale Uniunii Europene (IUEC) și a informațiilor sensibile neclasificate, astfel cum sunt prevăzute în deciziile (UE, Euratom) 2015/443 și 2015/444 ale Comisiei. Sunt vizate, între altele, dispozițiile privind schimbul, prelucrarea și stocarea unor astfel de informații.

Articolul 41

Acordul privind sediul și condițiile de funcționare

1. Dispozițiile necesare referitoare la găzduirea agenției în statul membru gazdă și facilitățile care trebuie puse la dispoziție de către statul respectiv, împreună cu normele specifice aplicabile în statul membru gazdă cu privire la directorul executiv, la membrii consiliului de administrație, la personalul agenției și la membrii familiilor acestora, sunt prevăzute într-un acord privind sediul între agenție și statul membru în care își are sediul agenția, încheiat după ce s-a obținut aprobarea consiliului de administrație și cel târziu la [doi ani de la intrarea în vigoare a prezentului regulament].

2. Statul membru care găzduiește agenția pune la dispoziție cele mai bune condiții posibile pentru a asigura buna funcționare a agenției, printre care accesibilitatea amplasamentului, existența unor facilități adecvate de educație pentru copiii personalului, un acces corespunzător la piața muncii, la securitate socială și la asistență medicală atât pentru copii, cât și pentru soții/soțiile personalului.

Articolul 42

Controlul administrativ

Activitățile agenției fac obiectul supravegherii de către Ombudsman, în conformitate cu articolul 228 din TFUE.

TITLUL III
CADRUL DE CERTIFICARE DE SECURITATE CIBERNETICĂ

Articolul 43

Sistemele europene de certificare de securitate

Un sistem european de certificare de securitate cibernetică atestă că produsele și serviciile TIC care au fost certificate în conformitate cu sistemul respectiv sunt conforme cu cerințele specificate în ceea ce privește capacitatea acestora de a rezista, la un anumit nivel de asigurare, la acțiuni care au scopul de a compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise ori prelucrate sau funcțiile ori serviciile oferite de aceste produse, servicii și sisteme sau accesibile prin intermediul lor.

Articolul 44

Pregătirea și adoptarea unui sistem european de certificare de securitate cibernetică

1. În urma unei solicitări din partea Comisiei, ENISA pregătește o propunere de sistem european de certificare de securitate cibernetică ce îndeplinește cerințele prevăzute la articolele 45, 46 și 47 din prezentul regulament. Statele membre sau Grupul pentru certificare europeană de securitate cibernetică (denumit în continuare „Grupul”) instituit în temeiul articolului 53 pot propune Comisiei pregătirea unei propuneri de sistem european de certificare de securitate cibernetică.
2. Atunci când pregătește propunerile de sisteme menționate la alineatul (1) din prezentul articol, ENISA consultă toate părțile interesate relevante și cooperează îndeaproape cu Grupul. Grupul furnizează pentru ENISA asistența și consilierea de specialitate solicitate de aceasta în ceea ce privește pregătirea propunerii de sistem, inclusiv prin furnizarea de avize atunci când este necesar.
3. ENISA transmite Comisiei propunerea de sistem european de certificare de securitate cibernetică, pregătită în conformitate cu alineatul (2) din prezentul articol.
4. Comisia, pe baza propunerii de sistem prezentate de ENISA, poate adopta acte de punere în aplicare, în conformitate cu articolul 55 alineatul (1), care să prevadă sisteme europene de certificare de securitate cibernetică pentru produsele și serviciile TIC, care îndeplinesc cerințele prevăzute la articolele 45, 46 și 47 din prezentul regulament.
5. ENISA întreține un site web dedicat care oferă informații și publicitate privind sistemele europene de certificare de securitate cibernetică.

Articolul 45

Obiectivele de securitate ale sistemelor europene de certificare de securitate cibernetică

Un sistem european de certificare de securitate cibernetică este conceput astfel încât să ia în considerare, după caz, următoarele obiective de securitate:

(a) să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva stocării, prelucrării, accesului sau divulgării accidentale sau neautorizate;

(b) să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva distrugerii accidentale sau neautorizate, a pierderii sau modificării accidentale;

(c) să asigure că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces;

(d) să înregistreze datele, funcțiile sau serviciile care au fost comunicate, momentul în care au fost comunicate acestea și autorul comunicării;

(e) să asigure că este posibil să se verifice care sunt datele, serviciile sau funcțiile care au fost accesate sau utilizate, în ce moment și de către cine;

(f) să restabilească disponibilitatea datelor, serviciilor și funcțiilor și accesul la acestea în timp util în caz de incident fizic sau tehnic;

(g) să asigure că produsele și serviciile TIC sunt furnizate cu un software actualizat care nu conține vulnerabilități cunoscute și că sunt prevăzute mecanisme pentru actualizări securizate ale software-ului.

Articolul 46

Nivelurile de asigurare ale sistemelor europene de certificare de securitate cibernetică

1. Un sistem european de certificare de securitate cibernetică poate stabili unul sau mai multe dintre următoarele niveluri de asigurare: de bază, substanțial și/sau ridicat, pentru produsele și serviciile TIC din cadrul sistemului respectiv.

2. Nivelurile de asigurare de bază, substanțial și ridicat îndeplinesc următoarele criterii:

(a) nivelul de asigurare de bază se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad limitat de încredere în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a reduce riscul de incidente de securitate cibernetică;

(b) nivelul de asigurare substanțial se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad substanțial de încredere în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a reduce substanțial riscul de incidente de securitate cibernetică;

(c) nivelul de asigurare ridicat se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad mai ridicat de încredere, față de certificatele având un nivel de asigurare substanțial, în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a preveni riscul de incidente de securitate cibernetică;

Articolul 47

Elementele sistemelor europene de certificare de securitate cibernetică

1. Un sistem european de certificare de securitate cibernetică include următoarele elemente:

   (a) obiectul și domeniul de aplicare al certificării, inclusiv tipul sau categoriile de produse și servicii TIC acoperite;

   (b) specificarea detaliată a cerințelor de securitate cibernetică în raport cu care sunt evaluate produsele și serviciile TIC în cauză, de exemplu prin trimitere la standarde sau specificații tehnice ale Uniunii sau internaționale;

   (c) după caz, unul sau mai multe niveluri de asigurare;

   (d) criteriile și metodele specifice de evaluare, inclusiv tipurile de evaluări, utilizate pentru a demonstra că obiectivele specifice menționate la articolul 45 sunt îndeplinite;

   (e) informațiile necesare pentru certificare ce trebuie furnizate organismelor de evaluare a conformității de către solicitant;

   (f) în cazul în care sistemul prevede mărci sau etichete, condițiile în care pot fi utilizate aceste mărci sau etichete;

   (g) în cazul în care supravegherea face parte din sistem, normele pentru monitorizarea conformității cu cerințele certificatelor, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate;

   (h) condițiile de acordare, menținere, continuare, extindere și restrângere a domeniului de aplicare al certificării;

   (i) normele privind consecințele neconformității cu cerințele de certificare a produselor și serviciilor TIC certificate;

   (j) normele privind modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale unor produse și servicii TIC;

   (k) normele privind păstrarea evidențelor de către organismele de evaluare a conformității;

   (l) identificarea sistemelor naționale de certificare de securitate cibernetică care acoperă aceleași tipuri sau categorii de produse și servicii TIC;

   (m) conținutul certificatelor emise.

2. Cerințele specificate ale sistemului nu intră în contradicție cu cerințele legale aplicabile, în special cu cerințele care decurg din legislația armonizată a Uniunii.

3. În cazul în care un act specific al Uniunii prevede acest lucru, certificarea în cadrul unui sistem european de certificare de securitate cibernetică poate fi utilizată pentru a demonstra prezumția de conformitate cu cerințele din acel act.

4. În absența unei legislații armonizate a Uniunii, dreptul unui stat membru poate prevedea, de asemenea, că se poate folosi un sistem european de certificare de securitate cibernetică pentru a stabili prezumția de conformitate cu cerințele legale.

Articolul 48

Certificarea de securitate cibernetică

1. Produsele și serviciile TIC care au fost certificate în cadrul unui sistem european de certificare de securitate cibernetică adoptat în temeiul articolului 44 sunt prezumate a fi conforme cu cerințele acestui sistem.

2. Certificarea este voluntară, cu excepția cazului în care se prevede altfel în legislația Uniunii.

3. Organismele de evaluare a conformității menționate la articolul 51 emit un certificat european de securitate cibernetică în temeiul prezentului articol pe baza criteriilor incluse în sistemul european de certificare de securitate cibernetică adoptat în temeiul articolului 44.

4. Prin derogare de la dispozițiile alineatului (3), în cazurile justificate în mod corespunzător, un anumit sistem european de securitate cibernetică poate prevedea că un certificat european de securitate cibernetică ce rezultă din acel sistem poate fi emis numai de un organism public. Acest organism public este una din următoarele entități:

   (a) o autoritate națională de supraveghere în materie de certificare menționată la articolul 50 alineatul (1);

   (b) un organism care este acreditat ca organism de evaluare a conformității în temeiul articolului 51 alineatul (1) sau

   (c) un organism înființat în temeiul unor acte cu putere lege, al unor instrumente legale sau al altor proceduri administrative oficiale ale statului membru în cauză și care îndeplinesc cerințele pentru organismele care certifică produse, procese și servicii noi în conformitate cu ISO/IEC 17065: 2012.

5. Persoana fizică sau juridică ale cărei produse sau servicii TIC sunt supuse mecanismului de certificare furnizează organismului de evaluare a conformității menționat la articolul 51 toate informațiile necesare pentru desfășurarea procedurii de certificare.

6. Certificatele se emit pentru o perioadă maximă de trei ani și pot fi reînnoite în aceleași condiții, numai dacă sunt îndeplinite în continuare cerințele relevante.

7. Un certificat european de securitate cibernetică emis în temeiul prezentului articol este recunoscut în toate statele membre.

Articolul 49

Sistemele și certificatele naționale de certificare de securitate cibernetică

1. Fără a se aduce atingere dispozițiilor de la alineatul (3), sistemele naționale de certificare de securitate cibernetică și procedurile aferente pentru produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate cibernetică încetează să mai producă efecte de la data stabilită în actul de punere în aplicare adoptat în temeiul articolului 44 alineatul (4). Sistemele naționale existente de certificare de securitate cibernetică și procedurile aferente pentru produsele și serviciile TIC care nu fac obiectul unui sistem european de certificare de securitate cibernetică continuă să existe.

2. Statele membre nu introduc noi sisteme naționale de certificare de securitate cibernetică pentru produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate cibernetică în vigoare.

3. Certificatele existente emise în temeiul sistemelor naționale de certificare de securitate cibernetică rămân valabile până la data expirării lor.

Articolul 50

Autoritățile naționale de supraveghere în materie de certificare

1. Fiecare stat membru desemnează o autoritate națională de supraveghere în materie de certificare.

2. Fiecare stat membru informează Comisia cu privire la identitatea autorității desemnate.

3. Fiecare autoritate națională de supraveghere în materie de certificare este independentă în ceea ce privește organizarea, deciziile de finanțare, structura juridică și luarea de decizii, de entitățile pe care le supraveghează.

4. Statele membre se asigură că autoritățile naționale de supraveghere în materie de certificare dispun de resursele adecvate pentru a-și exercita competențele și pentru a-și îndeplini cu eficacitate și în mod eficient sarcinile atribuite.

5. Pentru punerea efectivă în aplicare a prezentului regulament, este oportun ca aceste autorități să participe, într-un mod activ, eficace, eficient și sigur, la activitățile Grupului european pentru certificarea de securitate cibernetică instituit în temeiul articolului 53.

6. Autoritățile naționale de supraveghere în materie de certificare:

   (a) monitorizează și asigură aplicarea dispozițiilor de la prezentul titlu la nivel național și supraveghează conformitatea certificatelor emise de organismele de evaluare a conformității stabilite pe teritoriile lor cu cerințele stabilite în prezentul titlu și în sistemul european de certificare de securitate cibernetică corespunzător;

   (b) monitorizează și supraveghează activitățile organismelor de evaluare a conformității în scopul prezentului regulament, inclusiv în ceea ce privește notificarea organismelor de evaluare a conformității și sarcinile conexe prevăzute la articolul 52 din prezentul regulament;

   (c) tratează plângerile depuse de persoane fizice sau juridice în legătură cu certificatele emise de organismele de evaluare a conformității stabilite pe teritoriul lor, investighează, în măsura în care este oportun, subiectul plângerii și informează reclamantul cu privire la stadiul și rezultatul investigației, într-un termen rezonabil;

   (d) cooperează cu alte autorități naționale de supraveghere în materie de certificare sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor și serviciilor TIC cu cerințele prezentului regulament sau ale sistemului european de certificare de securitate cibernetică specific;

   (e) monitorizează evoluțiile relevante din domeniul certificării de securitate cibernetică.

7. Fiecare autoritate națională de supraveghere în materie de certificare dispune cel puțin de următoarele competențe:

(a) competența de a cere organismelor de evaluare a conformității și deținătorilor de certificate europene de securitate cibernetică să furnizeze orice informație care îi este necesară pentru îndeplinirea sarcinilor sale;

(b) competența de a efectua investigații, sub formă de audituri, asupra organismelor de evaluare a conformității și a titularilor de certificate europene de securitate cibernetică, pentru a verifica conformitatea cu dispozițiile de la titlul III;

(c) competența de a lua măsuri adecvate, în conformitate cu legislația națională, pentru a se asigura că organismele de evaluare a conformității sau titularii de certificate respectă prezentul regulament sau un sistem european de certificare de securitate cibernetică;

(d) competența de a obține acces la orice sediu al organismelor de evaluare a conformității și al titularilor de certificate europene de securitate cibernetică cu scopul de a desfășura investigații în conformitate cu dreptul Uniunii sau cu dreptul procedural al statului membru;

(e) competența de a retrage, în conformitate cu legislația națională, certificatele care nu sunt conforme cu prezentul regulament sau cu un sistem european de certificare de securitate cibernetică;

(f) competența de a impune sancțiuni, astfel cum se prevede la articolul 54, în conformitate cu legislația națională, și de a cere încetarea imediată a încălcărilor obligațiilor prevăzute de prezentul regulament.

8. Autoritățile naționale de supraveghere în materie de certificare cooperează între ele și cu Comisia și fac în special schimb de informații, de experiență și de bune practici în ceea ce privește certificarea de securitate cibernetică și aspectele tehnice privind securitatea cibernetică a produselor și a serviciilor TIC.

Articolul 51

Organismele de evaluare a conformității

1. Organismele de evaluare a conformității sunt acreditate de către organismul național de acreditare desemnat în temeiul Regulamentului (CE) nr. 765/2008 numai dacă îndeplinesc cerințele stabilite în anexa la prezentul regulament.

2. Acreditarea se acordă pentru o perioadă de maximum cinci ani și poate fi reînnoită în aceleași condiții numai dacă organismul de evaluare a conformității îndeplinește cerințele prevăzute la prezentul articol. Organismele de acreditare revocă acreditarea unui organism de evaluare a conformității în temeiul alineatului (1) din prezentul articol în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care măsurile luate de un organism de evaluare a conformității încalcă dispozițiile prezentului regulament.

Articolul 52
Notificarea

1. Pentru fiecare sistem european de certificare de securitate cibernetică adoptat în temeiul articolului 44, autoritățile naționale de supraveghere în materie de certificare notifică Comisiei organismele de evaluare a conformității acreditate să emită certificate la nivelurile de asigurare specificate menționate la articolul 46, precum și, fără nicio întârziere nejustificată, orice modificare ulterioară referitoare la acestea.

2. La un an de la intrarea în vigoare a unui sistem european de certificare de securitate cibernetică, Comisia publică în Jurnalul Oficial lista organismelor de evaluare a conformității notificate.

3. În cazul în care Comisia primește o notificare după expirarea perioadei menționate la alineatul (2), aceasta publică în *Jurnalul Oficial al Uniunii Europene* modificările listei menționate la alineatul (2) în termen de două luni de la data primirii notificării respective.

4. O autoritate națională de supraveghere în materie de certificare poate înainta Comisiei o cerere de retragere a unui organism de evaluare a conformității notificat de respectiva autoritate națională de supraveghere în materie de certificare din lista menționată la alineatul (2) din prezentul articol. Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările corespunzătoare aduse listei, în termen de o lună de la data primirii cererii adresate de autoritatea națională de supraveghere în materie de certificare.

5. Comisia poate, prin intermediul actelor de punere în aplicare, să stabilească circumstanțele, formatele și procedurile pentru notificările menționate la alineatul (1) din prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

Articolul 53
Grupul european pentru certificarea de securitate cibernetică

1. Se instituie Grupul european pentru certificarea de securitate cibernetică („Grupul”).

2. Grupul este compus din autoritățile naționale de supraveghere în materie de certificare. Autoritățile sunt reprezentate de conducătorii sau de alți reprezentanți la nivel înalt ai autorităților naționale de supraveghere în materie de certificare.

3. Grupul are următoarele sarcini:

   (a) să acorde consiliere și asistență Comisiei în activitatea sa de asigurare a punerii în practică și aplicării coerente a dispozițiilor prezentului titlu, în special în ceea ce privește chestiunile legate de politica în materie de certificare de securitate cibernetică, de coordonarea abordărilor privind politicile și de pregătirea unor sisteme europene de certificare de securitate cibernetică;

   (b) să acorde asistență și consiliere pentru ENISA și să coopereze cu aceasta în legătură cu pregătirea unei propuneri de sistem în conformitate cu articolul 44 din prezentul regulament;

   (c) să propună Comisiei să solicite ca agenția să pregătească o propunere de sistem european de certificare de securitate cibernetică în conformitate cu articolul 44 din prezentul regulament;

(d) să adopte avize adresate Comisiei cu privire la întreținerea și revizuirea sistemelor europene de certificare de securitate cibernetică existente;

(e) să examineze evoluțiile relevante din domeniul securității cibernetice și să facă schimb de bune practici privind sistemele de certificare de securitate cibernetică;

(f) să faciliteze cooperarea dintre autoritățile naționale de supraveghere în materie de certificare desfășurată în temeiul prezentului titlu prin schimbul de informații, în special prin stabilirea unor metode care să permită schimbul eficient de informații referitoare la toate chestiunile privind certificarea de securitate cibernetică.

4. Comisia prezidează Grupul și asigură secretariatul acestuia, cu asistență din partea ENISA, astfel cum se prevede la articolul 8 litera (a).

Articolul 54
Sancțiunile

Statele membre stabilesc normele privind sancțiunile care se aplică în cazul încălcării dispozițiilor din prezentul titlu și a sistemelor europene de certificare de securitate cibernetică și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancțiunile prevăzute sunt eficace, proporționale și cu efect de descurajare. Statele membre informează Comisia [până la .../fără întârziere] cu privire la normele și măsurile respective și notifică acesteia orice modificare ulterioară care le afectează.

TITLUL IV
DISPOZIȚII FINALE

Articolul 55
Procedura comitetului

1. Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.
2. În cazul în care se face trimitere la prezentul alineat, se aplică articolul 4 din Regulamentul (UE) nr. 182/2011.

Articolul 56
Evaluarea și revizuirea

1. În termen de cel mult cinci ani de la data menționată la articolul 58 și la fiecare cinci ani după aceea, Comisia evaluează impactul, eficacitatea și eficiența activității agenției și a practicilor sale de lucru, posibila necesitate de a modifica mandatul agenției și implicațiile financiare ale unei astfel de modificări. Evaluarea ține seama de orice punct de vedere comunicat agenției ca răspuns la activitățile sale. În cazul în care Comisia consideră că nu se mai justifică continuarea activității agenției în raport cu obiectivele, mandatul și sarcinile atribuite, aceasta poate propune modificarea dispozițiilor referitoare la agenție din prezentul regulament.
2. Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor din titlul III în ceea ce privește obiectivele de asigurare a unui nivel adecvat de securitate cibernetică a produselor și serviciilor TIC în Uniune și de îmbunătățire a funcționării pieței interne.
3. Comisia trimite raportul de evaluare, împreună cu concluziile sale, Parlamentului European, Consiliului și consiliului de administrație. Concluziile raportului de evaluare sunt făcute publice.

Articolul 57
Abrogarea și succesiunea

1. Regulamentul (CE) nr. 526/2013 se abrogă cu efect de la [….].
2. Trimiterile la Regulamentul (CE) nr. 526/2013 și la ENISA se interpretează ca trimiteri la prezentul regulament și la agenție.
3. Agenția succede agenției instituite prin Regulamentul (CE) nr. 526/2013 în ceea ce privește toate aspectele legate de proprietate, acorduri, obligații juridice, contracte de muncă, angajamente financiare și răspunderi. Toate deciziile existente ale consiliului de administrație și ale comitetului executiv rămân valabile, cu condiția ca acestea să nu intre în conflict cu dispozițiile prezentului regulament.
4. Agenția se înființează de la [….] pentru o perioadă nedeterminată.

5. Directorul executiv numit în temeiul articolului 24 alineatul (4) din Regulamentul (CE) nr. 526/2013 este directorul executiv al agenției pentru perioada rămasă din mandatul său.

6. Membrii consiliului de administrație și supleanții lor numiți în temeiul articolului 6 din Regulamentul (CE) nr. 526/2013 sunt membrii consiliului de administrație al agenției și supleanții lor pentru perioada rămasă din mandatul lor.

Articolul 58

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

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

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președintele	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Denumirea propunerii/inițiativei

Propunere de Regulament al Parlamentului European și al Consiliului privind ENISA, „Agenția UE pentru Securitate Cibernetică”, și de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate în domeniul tehnologiei informației și comunicațiilor („Legea/Regulamentul privind securitatea cibernetică”)

1.2. Domeniul (domeniile) de politică vizat(e)

Domeniul de politică: 09 - Rețele de comunicare, conținut și tehnologie

Activitatea: 09.02 - Piața unică digitală

1.3. Tipul propunerii/inițiativei

☒ Propunerea/inițiativa se referă la **o acțiune nouă (Titlul III – Certificare)**

☐ Propunerea/inițiativa se referă la **o acțiune nouă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[43]

☒Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente** (**Titlul II – mandatul ENISA)**

☐ Propunerea/inițiativa se referă la **o acțiune reorientată către o acțiune nouă**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) strategic(e) multianual(e) al(e) Comisiei vizat(e) de propunere/inițiativă

1. Sporirea rezilienței statelor membre, a întreprinderilor și a UE în ansamblu

2. Asigurarea bunei funcționări a pieței interne a UE pentru produsele și serviciile TIC

3. Sporirea competitivității globale a întreprinderilor din UE care își desfășoară activitatea în domeniul TIC.

4. Apropierea actelor cu putere de lege și a actelor administrative ale statelor membre care prevăd obligația de asigura securitatea cibernetică

1.4.2. Obiectiv(e) specific(e)

Având în vedere obiectivele generale, în contextul mai larg al Strategiei privind securitatea cibernetică revizuite, instrumentul își propune, prin delimitarea domeniului de aplicare și a mandatului ENISA și prin instituirea unui cadru european de certificare pentru produsele și serviciile TIC, să realizeze următoarele obiective specifice:

1. sporirea **capabilităților și a nivelului de pregătire** ale statelor membre și ale întreprinderilor;
2. îmbunătățirea **cooperării și a coordonării** dintre statele membre și instituțiile, agențiile și organele UE;
3. sporirea **capabilităților la nivelul UE care să completeze acțiunea statelor membre**, în special în cazul unei crize cibernetice transfrontaliere;
4. sporirea **gradului de sensibilizare** a cetățenilor și a întreprinderilor cu privire la

[43] Astfel cum sunt menționate la articolul 54 alineatul (2) litera (a) sau litera (b) din Regulamentul financiar.

aspectele legate de securitatea cibernetică;

5. consolidarea încrederii în piața unică digitală și în inovarea digitală prin sporirea, la nivel global, a **transparenței asigurării securității cibernetice**[44] a produselor și serviciilor TIC.

ENISA va contribui la realizarea obiectivelor menționate anterior prin:

sprijin sporit pentru elaborarea politicilor – furnizarea de orientări și consiliere Comisiei și statelor membre în vederea actualizării și dezvoltării unui cadru normativ global în domeniul securității cibernetice, precum și a inițiativelor politice și legislative specifice sectorului, în care sunt implicate aspecte de securitate cibernetică, contribuția la activitatea grupului de cooperare [articolul 11 din Directiva (UE) 2016/1148] prin furnizarea de expertiză și de asistență, acordarea de sprijin pentru elaborarea și punerea în aplicare de politici în domeniul identității electronice și al serviciilor de încredere, promovarea schimbului de bune practici între autoritățile competente;

sprijin sporit pentru consolidarea capacităților - furnizarea de sprijin statelor membre, instituțiilor, organelor, oficiilor și agențiilor Uniunii în vederea dezvoltării și ameliorării prevenirii, detectării și analizei, precum și a capacității de a reacționa la probleme și incidente de securitate cibernetică, oferirea de asistență statelor membre, la solicitarea acestora, în ceea ce privește dezvoltarea CSIRT naționale și elaborarea de strategii naționale în domeniul securității cibernetice, oferirea de asistență instituțiilor Uniunii în elaborarea și revizuirea strategiilor de securitate cibernetică ale Uniunii, furnizarea de formare în materie de securitate cibernetică, oferirea de asistență statelor membre prin intermediul grupului de cooperare în ceea ce privește schimbul de bune practici, facilitarea înființării unor centre sectoriale de schimb și de analiză de informații (ISACs);

sprijinirea cooperării operaționale și a gestionării crizelor – sprijinirea cooperării dintre organismele publice competente și dintre părțile interesate prin instituirea unei cooperări sistematice cu instituțiile, organele, oficiile și agențiile Uniunii care se ocupă cu securitatea cibernetică, criminalitatea informatică și protecția vieții private și a datelor cu caracter personal, asigurarea secretariatului rețelei CSIRT [articolul 12 alineatul (2) din Directiva (UE) 2016/1148] și contribuirea la cooperarea operațională în cadrul rețelei prin furnizarea de sprijin statelor membre, în cooperare cu CERT-UE, la solicitarea acestora, organizarea de exerciții periodice de securitate cibernetică, contribuirea la dezvoltarea unui răspuns bazat pe cooperare la incidentele și crizele de securitate cibernetică transfrontaliere de mare amploare, efectuarea, în cooperare cu rețeaua CSIRT, de anchete tehnice *ex post* privind incidentele semnificative și formularea de recomandări privind măsurile ulterioare;

sarcini legate de piață (standardizare, certificare) - îndeplinirea unei serii de funcții prin care se sprijină cu precădere piața internă: „observator al pieței” securității cibernetice, prin analizarea tendințelor relevante de pe piața securității cibernetice, pentru a corela mai bine cererea și oferta, sprijinirea și promovarea elaborării și punerii în aplicare a politicii Uniunii în materie de certificare de securitate cibernetică a produselor și serviciilor TIC prin pregătirea propunerilor de sisteme europene de certificare de securitate cibernetică pentru produsele și serviciile TIC, asigurarea secretariatului Grupului pentru certificarea de securitate cibernetică al Uniunii, furnizarea de orientări și de bune practici privind cerințele în materie de securitate a produselor și serviciilor TIC în cooperare cu autoritățile naționale de supraveghere în materie de certificare și cu sectorul; **sprijin pentru o mai bună**

[44] Transparența asigurării securității cibernetice înseamnă furnizarea de informații suficiente utilizatorilor cu privire la proprietățile de securitate cibernetică care le permit acestora să determine în mod obiectiv nivelul de securitate al unui anumit produs, serviciu sau proces TIC.

cunoaștere, informare și sensibilizare – furnizarea de asistență și consiliere Comisiei și statelor membre în vederea atingerii unui nivel ridicat de cunoștințe, pe întreg teritoriul Uniunii, cu privire la aspectele legate de securitatea rețelelor și a informațiilor și aplicarea acesteia părților interesate din sector. Acest lucru presupune, de asemenea, punerea în comun, organizarea și punerea la dispoziția publicului, prin intermediul unui portal dedicat, de informații privind securitatea rețelelor și a sistemelor informatice [sau securitatea cibernetică]. Un alt element important sunt activitățile de sensibilizare și campaniile de informare destinate publicului larg cu privire la riscurile de securitate cibernetică;

sprijin sporit pentru cercetare și inovare - oferirea de consiliere cu privire la nevoile de cercetare și stabilirea priorităților în domeniul securității cibernetice;

sprijinirea cooperării internaționale – sprijinirea eforturilor Uniunii de a coopera cu țările terțe și cu organizațiile internaționale în vederea promovării cooperării internaționale privind securitatea cibernetică.

CERTIFICARE

Cadrul de certificare va contribui la îndeplinirea obiectivelor prin sporirea transparenței la nivel global a asigurării securității cibernetice[45] a produselor și serviciilor TIC și, prin urmare, la consolidarea încrederii în piața unică digitală și în inovarea digitală. Acest lucru ar trebui să contribuie, de asemenea, la evitarea fragmentării sistemelor de certificare în UE și a cerințelor de securitate aferente, precum și a criteriilor de evaluare din toate statele membre și toate sectoarele.

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.

O ENISA consolidată (capabilități de sprijin, prevenire, cooperare și sensibilizare la nivelul UE menite, prin urmare, să sporească reziliența cibernetică generală a UE) și sprijinirea totodată a cadrului UE de certificare a produselor și serviciilor TIC ar trebui să aibă următoarele impacturi (listă neexhaustivă):

Impactul global

- impact global pozitiv asupra pieței interne datorită reducerii fragmentării pieței și consolidării încrederii în tehnologiile digitale, printr-o mai bună cooperare, abordări mai armonizate ale politicilor UE în materie de securitate cibernetică și capabilități sporite la nivelul UE. Aceasta ar trebui să aibă drept rezultat un impact economic pozitiv, contribuind la reducerea costurilor incidentelor de securitate cibernetică/criminalității informatice, pentru care impactul economic estimat în Uniune se ridică la 0,41 % din PIB-ul UE (și anume, în jur de 55 de miliarde EUR).

Rezultate specifice:

Îmbunătățirea capabilităților și a nivelului de pregătire în ceea ce privește securitatea cibernetică ale statelor membre și ale întreprinderilor

- îmbunătățirea capabilităților și a nivelului de pregătire în ceea ce privește securitatea cibernetică ale statelor membre (datorită analizei strategice pe termen lung a amenințărilor

[45] Transparența asigurării securității cibernetice înseamnă furnizarea de informații suficiente utilizatorilor cu privire la proprietățile de securitate cibernetică care le permit acestora să determine în mod obiectiv nivelul de securitate al unui anumit produs, serviciu sau proces TIC.

și incidentelor cibernetice, orientărilor și rapoartelor, intermedierii de expertiză și de bune practici, formării și punerii la dispoziție de materiale de formare, exercițiilor CyberEurope consolidate);

- îmbunătățirea capabilităților actorilor din sectorul privat, datorită sprijinului pentru înființarea de centre de schimb și analiză de informații în diverse sectoare;

- îmbunătățirea nivelului de pregătire în ceea ce privește securitatea cibernetică al UE și al statelor membre, datorită disponibilității unor planuri, convenite în caz de incident de securitate cibernetică transfrontalier de mare amploare, supuse unor simulări adecvate și testate în cadrul exercițiilor CyberEurope;

Îmbunătățirea cooperării și a coordonării dintre statele membre și instituțiile, agențiile și organele UE

- îmbunătățirea cooperării atât în cadrul sectorului public și al celui privat, cât și între acestea;

- o mai bună coerență a abordării în ceea ce privește punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor la nivel transfrontalier și transsectorial;

- îmbunătățirea cooperării în domeniul certificării, datorită unui cadru instituțional care să permită dezvoltarea de sisteme europene de certificare de securitate cibernetică și dezvoltarea unei politici comune în acest domeniu;

Capabilități sporite la nivelul UE care să completeze acțiunea statelor membre

- îmbunătățirea „capacității operaționale a UE" care să completeze acțiunea statelor membre și să le sprijine, la cerere și în ceea ce privește servicii limitate și identificate în prealabil. Se preconizează că acestea vor avea un impact pozitiv asupra succesului acțiunilor de prevenire și detectare a incidentelor, precum și asupra răspunsului la acestea, atât la nivelul statelor membre, cât și la nivelul Uniunii;

Sporirea gradului de sensibilizare a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică

- sensibilizare sporită, în general, a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică;

- îmbunătățirea abilității de a lua decizii de achiziționare în cunoștință de cauză privind produsele și serviciile TIC, datorită certificării de securitate cibernetică;

Consolidarea încrederii în piața unică digitală și în inovarea digitală prin sporirea transparenței la nivel global a nivelului de asigurare a securității cibernetice a produselor și serviciilor TIC

- sporirea transparenței în ceea ce privește asigurarea securității cibernetice[46] a produselor și serviciilor TIC datorită simplificării procedurilor de certificare de securitate prin intermediul unui cadru la nivelul UE;

- îmbunătățirea nivelului de asigurare a proprietăților de securitate ale produselor și serviciilor TIC;

- utilizarea sporită a certificării de securitate, stimulată de procedurile simplificate, de costurile reduse și de perspectiva unor oportunități de afaceri la nivelul întregii UE care nu se confruntă cu obstacole determinate de fragmentarea pieței;

[46] Transparența asigurării securității cibernetice înseamnă furnizarea de informații suficiente utilizatorilor cu privire la proprietățile de securitate cibernetică care le permit acestora să determine în mod obiectiv nivelul de securitate al unui anumit produs, serviciu sau proces TIC.

- îmbunătățirea competitivității pe piața securității cibernetice în UE ca urmare a reducerii costurilor și a sarcinii administrative pentru IMM-uri și a eliminării barierelor potențiale la intrarea pe piață cauzate de numeroasele sisteme naționale de certificare;

Altele

- nu se preconizează un impact de mediu semnificativ pentru niciunul dintre obiective;

- în ceea ce privește bugetul UE, există posibilitatea sporirii eficienței prin intensificarea cooperării și a coordonării activităților între instituțiile, agențiile și organele UE.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

(a)

Obiectiv: sporirea capabilităților și a nivelului de pregătire ale statelor membre și ale întreprinderilor:

- numărul cursurilor de formare organizate de ENISA;
- acoperirea geografică (numărul de țări și de zone) a asistenței directe furnizate de ENISA;
- nivelul de pregătire atins de statele membre în ceea ce privește maturitatea CSIRT și supravegherea măsurilor de reglementare referitoare la securitatea cibernetică;
- numărul de bune practici la nivelul UE pentru infrastructurile critice, furnizate de ENISA;
- numărul de bune practici la nivelul UE pentru IMM-uri, furnizate de ENISA;
- publicarea anuală de către ENISA a unor analize strategice ale amenințărilor și incidentelor cibernetice pentru a se identifica tendințele emergente;
- contribuția periodică a ENISA la activitatea grupurilor de lucru în domeniul securității cibernetice ale organizațiilor de standardizare europene.

Obiectiv: îmbunătățirea cooperării și a coordonării dintre statele membre și instituțiile, agențiile și organele UE:

- numărul statelor membre care au utilizat în procesul de elaborare a propriilor politici recomandările și avizele formulate de ENISA;
- numărul instituțiilor, agențiilor și organelor UE care au utilizat în procesul de elaborare a propriilor politici recomandările și avizele formulate de ENISA;
- punerea în aplicare cu regularitate a programului de lucru al rețelei CSIRT și buna funcționare a infrastructurii IT și a canalelor de comunicare ale acesteia;
- numărul rapoartelor tehnice puse la dispoziția grupului de cooperare și utilizate de acesta;
- coerența abordării în ceea ce privește punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor la nivel transfrontalier și transsectorial;
- numărul evaluărilor efectuate de ENISA în ceea ce privește respectarea reglementărilor;

- numărul centrelor de schimb și analiză de informații înființate în diferite sectoare, în special pentru infrastructurile critice;
- crearea și funcționarea regulată a platformelor de informații prin care se diseminează informații din domeniul securității cibernetice care provin de la instituțiile, agențiile și organele UE;
- contribuția regulată la pregătirea unor programe de lucru ale UE în domeniul cercetării și inovării;
- instituirea unui acord de cooperare între ENISA, EC3 și CERT-UE;
- numărul sistemelor de certificare incluse și dezvoltate în temeiul cadrului;

Obiectiv: sporirea capabilităților la nivelul UE care să completeze acțiunea statelor membre, în special în cazul unei crize cibernetice transfrontaliere

- publicarea de către ENISA a unei analize strategice anuale a amenințărilor și incidentelor cibernetice pentru a se identifica tendințele emergente;
- publicarea de informații agregate cu privire la incidentele raportate de ENISA în temeiul Directivei privind securitatea rețelelor și a informațiilor ;
- numărul exercițiilor paneuropene coordonate de agenție și numărul statelor membre și al organizațiilor implicate;
- numărul solicitărilor de sprijin pentru reacție în situații de urgență la care agenția a răspuns adresate ENISA de către statele membre;
- numărul analizelor efectuate de ENISA în cooperare cu CERT-UE privind vulnerabilitățile, artefactele și incidentele;
- disponibilitatea, pe întreg teritoriul UE, a rapoartelor situaționale bazate pe informațiile puse la dispoziția ENISA de către statele membre și alte entități în caz de incident cibernetic transfrontalier de mare amploare.

Obiectiv: sporirea gradului de sensibilizare a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică:

- desfășurarea cu periodicitate de campanii de sensibilizare la nivelul UE și la nivel național și actualizarea cu regularitate a tematicilor, în funcție de noile necesități în materie de învățare;
- sporirea gradului de sensibilizare în rândul cetățenilor UE cu privire la aspectele cibernetice;
- organizarea cu regularitate de quiz-uri de sensibilizare în materie de securitate cibernetică și creșterea în timp a procentajului răspunsurilor corecte;
- publicarea periodică a unor bune practici de securitate și de igienă cibernetică, destinate angajaților și organizațiilor.

Obiectiv: consolidarea încrederii în piața unică digitală și în inovarea digitală prin sporirea transparenței globale a asigurării securității cibernetice[47] a produselor și serviciilor TIC:

- numărul sistemelor care respectă cadrul UE;

[47] Transparența asigurării securității cibernetice înseamnă furnizarea de informații suficiente utilizatorilor cu privire la proprietățile de securitate cibernetică care le permit acestora să determine în mod obiectiv nivelul de securitate al unui anumit produs, serviciu sau proces TIC.

- costuri reduse pentru obținerea unui certificat de securitate TIC;
- numărul de organisme de evaluare a conformității specializate în certificarea TIC, din toate statele membre;
- înființarea Grupului european pentru certificarea de securitate cibernetică și organizarea de reuniuni periodice;
- orientări pentru certificarea în conformitate cu cadrul UE în vigoare;
- publicarea cu periodicitate a unor analize ale principalelor tendințe de pe piața securității cibernetice din UE;
- numărul de produse și servicii TIC certificate în conformitate cu normele cadrului european de certificare a securității în domeniul TIC;
- creșterea numărului de utilizatori finali care cunosc caracteristicile de securitate ale produselor și serviciilor TIC;

(b)

1.4.5. Cerință (cerințe) de îndeplinit pe termen scurt sau lung

Având în vedere cerințele de reglementare și situația amenințărilor în materie de securitate cibernetică, care se schimbă rapid, mandatul ENISA trebuie revizuit pentru a se stabili un nou set de sarcini și de funcții, în vederea sprijinirii cu eficacitate și în mod eficient a eforturilor statelor membre, instituțiilor UE și ale altor părți interesate de a asigura un spațiu cibernetic sigur în Uniunea Europeană. Domeniul de aplicare propus al mandatului este delimitat, fiind consolidate domeniile în care agenția și-a demonstrat în mod clar valoarea adăugată și fiind adăugate domeniile noi în care este nevoie de sprijin având în vedere noile priorități și instrumente de politică, în special Directiva privind securitatea rețelelor și a informațiilor, revizuirea Strategiei de securitate cibernetică a UE, Planul de acțiune al UE privind securitatea cibernetică pentru cooperare în caz de criză cibernetică și certificarea de securitate în domeniul TIC. Noul mandat propus urmărește să atribuie agenției un rol mai puternic și mai proeminent, în special și prin sprijinirea statelor membre într-un mod mai activ pentru a contracara amenințările specifice (capacitate operațională) și prin dobândirea statutului de centru de expertiză care acordă sprijin statelor membre și Comisiei cu privire la certificarea de securitate cibernetică.

În același timp, propunerea stabilește un cadru european de certificare de securitate cibernetică pentru produsele și serviciile TIC și precizează funcțiile și sarcinile esențiale ale ENISA în domeniul certificării de securitate cibernetică. Cadrul stabilește dispoziții și proceduri comune care permit crearea unor sisteme de certificare de securitate cibernetică la nivelul UE pentru produse/servicii TIC specifice sau pentru riscurile de securitate cibernetică. Crearea unor sisteme europene de certificare de securitate cibernetică în conformitate cu cadrul va permite ca certificatele emise în cadrul acestor sisteme să fie valabile și recunoscute în toate statele membre și să constituie o soluție pentru actuala fragmentare a pieței.

1.4.6. Valoarea adăugată a intervenției UE

Securitatea cibernetică este cu adevărat o problemă globală, care este, prin natura sa, transfrontalieră și care devine din ce în ce mai mult transsectorială având în vedere interdependențele dintre rețelele și sistemele informatice. Numărul, complexitatea și amploarea incidentelor de securitate cibernetică, precum și impactul acestora asupra economiei și societății cresc de-a lungul timpului și se preconizează creșterea în

continuare a acestora în paralel cu evoluțiile tehnologice, de exemplu, proliferarea internetului obiectelor. Aceasta implică faptul că în viitor vor fi necesare eforturi comune sporite din partea statelor membre, a instituțiilor UE și a părților interesate din sectorul privat pentru a face față amenințărilor în materie de securitate cibernetică.

De la înființarea sa, în 2004, ENISA a urmărit să favorizeze cooperarea dintre statele membre și părțile interesate din domeniul securității rețelelor și a informațiilor, inclusiv sprijinirea cooperării dintre sectorul public și cel privat. Acest sprijin pentru cooperare a inclus activitatea desfășurată la nivel tehnic pentru a se furniza o situație a amenințărilor la nivelul întregii UE, instituirea grupurilor de experți și organizarea de exerciții paneuropene de gestionare a incidentelor și crizelor cibernetice pentru sectoarele public și privat (în special „Cyber Europe"). Prin Directiva privind securitatea rețelelor și a informațiilor au fost încredințate Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor sarcini suplimentare, inclusiv rolul de secretariat al rețelei CSIRT pentru cooperarea operațională dintre statele membre.

Valoarea adăugată a unei acțiuni la nivelul UE, în special cu scopul de a spori cooperarea dintre statele membre, dar și dintre comunitățile din domeniul securității rețelelor și a informațiilor, a fost recunoscută în Concluziile Consiliului[48] din 2016 și reiese, de asemenea, în mod clar din evaluarea ENISA din 2017, care arată că valoarea adăugată a agenției constă, în principal, în capacitatea sa de a spori cooperarea dintre aceste părți interesate. Nu există niciun alt actor la nivelul UE care să sprijine cooperarea dintre același tip de părți interesate cu privire la securitatea rețelelor și a informațiilor.

Valoarea adăugată a ENISA în ceea ce privește reunirea comunităților și a părților interesate din domeniul securității cibernetice este valabilă și în domeniul certificării. Creșterea criminalității informatice și a amenințărilor la adresa securității a dus la apariția unor inițiative naționale de stabilire a unor cerințe de înalt nivel în materie de securitate cibernetică și de certificare pentru componentele TIC utilizate în infrastructura tradițională. Deși sunt importante, aceste inițiative prezintă riscul de fragmentare a pieței unice și de creare de obstacole pentru interoperabilitate. S-ar putea să fie necesar ca un furnizor de TIC să treacă prin mai multe procese de certificare pentru a putea vinde în mai multe state membre. Este foarte puțin probabil ca ineficacitatea/ineficiența sistemelor actuale de certificare să fie soluționată în absența unei intervenții a UE. Dacă nu se iau măsuri, este foarte probabil ca fragmentarea pieței să se accentueze pe termen scurt și mediu (în următorii 5-10 ani) odată cu apariția unor noi sisteme de certificare. Lipsa de coordonare și de interoperabilitate între aceste sisteme constituie un element care diminuează potențialul pieței unice digitale. Acest lucru dovedește valoarea adăugată a instituirii unui cadru european de certificare de securitate cibernetică pentru produsele și serviciile TIC prin crearea condițiilor adecvate pentru o abordare eficace a problemei legate de coexistența mai multor proceduri de certificare în diferitele state membre, costurile de certificare fiind reduse, iar certificarea la nivelul UE devenind astfel mai atractivă, în general, din perspectivă comercială și concurențială.

1.4.7. Învățăminte desprinse din experiențe anterioare similare

În conformitate cu temeiul juridic al ENISA, Comisia a efectuat o evaluare a agenției, care a inclus un studiu independent și, de asemenea, o consultare publică. Concluzia evaluării a fost că obiectivele ENISA rămân de actualitate. În contextul evoluțiilor tehnologiilor și

[48] Concluziile Consiliului privind „Consolidarea sistemului de reziliență cibernetică al Europei și încurajarea unui sector al securității cibernetice competitiv și inovator - 15 noiembrie 2016.

amenințărilor și al unei nevoi acute de sporire a securității rețelelor și informațiilor în UE, este necesară o expertiză tehnică cu privire la evoluția aspectelor de securitate a rețelelor și a informațiilor. Este necesar să se consolideze, în statele membre, capacități de înțelegere a amenințărilor și de răspuns la acestea, iar părțile interesate trebuie să coopereze în diverse domenii tematice și cu diverse instituții.

Agenția a contribuit cu succes la sporirea securității rețelelor și a informațiilor în Europa prin consolidarea capacităților în 28 state membre și prin intensificarea cooperării dintre statele membre și părțile interesate din domeniul securității rețelelor și a informațiilor, prin furnizarea de expertiză, prin dezvoltarea de comunități și prin sprijinirea politicilor.

ENISA a reușit să obțină un impact, cel puțin într-o anumită măsură, în vastul domeniu al securității rețelelor și informațiilor, dar nu a reușit să dezvolte pe deplin un nume de marcă puternic și să obțină vizibilitate suficientă pentru a fi recunoscută drept „centrul de expertiză” în Europa. Aceasta se explică prin mandatul extins al ENISA pentru care nu s-au alocat resurse proporțional de mari. În plus, ENISA rămâne singura agenție a UE cu un mandat cu durată fixă, fapt care limitează capacitatea acesteia de a dezvolta o viziune pe termen lung și de a sprijini părțile interesate în mod durabil. Acest lucru este, de asemenea, în contradicție cu dispozițiile Directivei privind securitatea rețelelor și a informațiilor, care prevede pentru ENISA sarcini fără dată de finalizare.

În ceea ce privește certificarea de securitate cibernetică pentru produsele și serviciile TIC, la ora actuală nu există un cadru european. Cu toate acestea, creșterea criminalității informatice și a amenințărilor la adresa securității a dus la apariția unor inițiative naționale, fapt care creează riscul de fragmentare a pieței unice.

1.4.8. Compatibilitatea și posibila sinergie cu alte instrumente corespunzătoare

Inițiativa este coerentă într-o mare măsură cu politicile existente, în special în domeniul pieței interne. Într-adevăr, aceasta este concepută în conformitate cu strategia globală în ceea ce privește securitatea cibernetică, astfel cum este definită de revizuirea Strategiei privind piața unică digitală, pentru a completa un set cuprinzător de măsuri, cum ar fi revizuirea Strategiei de securitate cibernetică a UE, planul de acțiune pentru cooperarea în caz de criză cibernetică și inițiativele de combatere a criminalității informatice. Aceasta ar asigura alinierea la legislația existentă în materie de securitate cibernetică și se va baza pe dispozițiile acesteia, în special Directiva privind securitatea rețelelor și a informațiilor, în vederea unei reziliențe cibernetice sporite a UE, prin consolidarea capabilităților, cooperării, gestionării riscurilor și a sensibilizării cu privire la aspectele cibernetice.

Măsurile de certificare sugerate ar trebui să abordeze fragmentarea potențială cauzată de sistemele naționale de certificare existente și emergente, contribuind astfel la dezvoltarea pieței unice digitale. De asemenea, inițiativa sprijină și completează punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor, furnizând întreprinderilor care fac obiectul directivei un instrument pentru a demonstra respectarea cerințelor privind securitatea rețelelor și a informațiilor în întreaga Uniune.

Cadrul european de certificare de securitate cibernetică a TIC propus nu aduce atingere Regulamentului general privind protecția datelor[49] și, în special, dispozițiilor relevante în materie de certificare[50], astfel cum se aplică acestea securității prelucrării datelor cu caracter personal. În cele din urmă, dar nu mai puțin important, sistemele propuse în viitorul cadru european ar trebui să se bazeze cât mai mult posibil pe standardele internaționale, astfel încât să se evite crearea de obstacole în calea comerțului și să se asigure coerența cu inițiativele internaționale.

[49] Regulamentul (UE) 2016/679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

[50] Cum ar fi articolele 42 (Certificare) și 43 (Organisme de certificare), precum și articolele 57, 58 și 70 privind sarcinile, respectiv competențele relevante ale autorităților de supraveghere independente, precum și sarcinile Comitetului european pentru protecția datelor.

1.5. Durata și impactul financiar

☐ Propunere/inițiativă pe **durată determinată**

– ☐ Propunere/inițiativă în vigoare de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA

☒ Propunere/inițiativă pe **durată nedeterminată**

– Punere în aplicare cu o perioadă de creștere în intensitate din 2019 până în 2020,

– urmată de o perioadă de funcționare în regim de croazieră.

1.6. Modul (modurile) de gestionare preconizat(e)[51]

☒ **Gestiune directă** asigurată de către Comisie (Titlul III - Certificare)

– ☐ de către agențiile executive;

☐ **Gestiune partajată** cu statele membre

☒ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

☐BEI și Fondului European de Investiții;

☒ organismelor menționate la articolele 208 și 209 (Titlul II - ENISA);

☐ organismelor de drept public;

☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să prezinte garanții financiare adecvate;

☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și care prezintă garanții financiare adecvate;

☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, identificate în actul de bază relevant.

Observații

Regulamentul include: - titlul II din regulamentul propus revizuiește mandatul Agenției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) conferindu-i un rol important în certificare în timp ce - titlul III stabilește un cadru pentru crearea sistemelor europene de certificare de securitate cibernetică a produselor și serviciilor TIC, în care ENISA joacă un rol esențial.

[51] Explicațiile privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și de raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Monitorizarea va începe imediat după adoptarea instrumentului juridic și se va concentra pe punerea sa în aplicare. Comisia va organiza reuniuni cu ENISA, cu reprezentanții statelor membre (de exemplu, grupul de experți) și cu părțile interesate relevante, în special pentru a facilita punerea în aplicare a normelor privind certificarea, cum ar fi instituirea consiliului.

Prima evaluare ar trebui să aibă loc la 5 ani de la data intrării în vigoare a instrumentului juridic, dacă sunt disponibile suficiente date. În instrumentul juridic este inclusă o clauză de evaluare explicită și de revizuire [articolul XXX], în temeiul căreia Comisia va efectua o evaluare independentă. Comisia va trimite ulterior Parlamentului European și Consiliului un raport privind evaluarea sa, însoțit, după caz, de o propunere de revizuire, pentru a măsura impactul și valoarea adăugată a regulamentului. Evaluările ulterioare ar trebui să aibă loc o dată la cinci ani. Se va aplica metodologia de evaluare prevăzută de măsurile Comisiei privind o mai bună legiferare. Aceste evaluări vor fi efectuate pe baza unor discuții cu experți și a unor studii specifice, precum și a unor ample consultări cu părțile interesate.

Directorul executiv al ENISA ar trebui să prezinte o dată la doi ani consiliului de administrație o evaluare *ex post* a activităților ENISA. De asemenea, agenția ar trebui să elaboreze un plan de măsuri ulterioare în ceea ce privește concluziile evaluărilor retrospective și să prezinte Comisiei, o dată la doi ani, un raport privind progresele înregistrate. Consiliului de administrație ar trebui să îi revină responsabilitatea monitorizării modului în care s-au luat măsuri adecvate în urma acestor concluzii.

Presupusele cazuri de administrare defectuoasă a activităților agenției fac obiectul investigațiilor efectuate de Ombudsmanul European în conformitate cu prevederile articolului 228 din tratat.

Sursele de date pentru monitorizarea planificată ar putea fi în cea mai mare parte ENISA, Grupul european pentru certificare în domeniul cibernetic, grupul de cooperare, rețeaua CSIRT și autoritățile statelor membre. Pe lângă datele provenite din rapoartele (inclusiv rapoartele de activitate anuale) ENISA, ale Grupului european pentru certificare în domeniul cibernetic, ale grupului de cooperare și ale rețelei CSIRT, vor fi utilizate, atunci când va fi necesar, instrumente specifice de colectare a datelor (de exemplu, anchete adresate autorităților naționale, sondaje Eurobarometru și rapoartele efectuate în urma campaniei Luna securității cibernetice și a exercițiilor paneuropene).

2.2. Sistemul de gestiune și de control

2.2.1. Riscul (riscurile) identificat(e)

Riscurile identificate sunt limitate: există deja o agenție a Uniunii, iar mandatul acesteia va fi delimitat, fiind consolidate domeniile în care agenția și-a demonstrat în mod clar valoarea adăugată și fiind adăugate acele domenii noi în care este nevoie de sprijin având în vedere noile priorități și instrumente de politică, în special Directiva privind securitatea rețelelor și a informațiilor, revizuirea Strategiei de securitate cibernetică a UE, Planul de acțiune al UE

privind securitatea cibernetică pentru cooperare în caz de criză cibernetică și certificarea de securitate TIC.

Prin urmare, propunerea detaliază funcțiile agenției și duce la sporirea eficienței. Sporirea competențelor și sarcinilor operaționale nu reprezintă un risc real, întrucât acestea ar completa acțiunea statelor membre și le-ar acorda sprijin, la cerere și în ceea ce privește unele servicii limitate și identificate în prealabil.

În plus, modelul de agenție propus, în conformitate cu abordarea comună, asigură că există un control suficient pentru a garanta că activitatea ENISA urmărește îndeplinirea obiectivelor sale. Riscurile operaționale și financiare ale modificărilor propuse par a fi limitate.

În același timp, este necesar să se asigure resurse financiare adecvate pentru ca ENISA să își îndeplinească sarcinile încredințate prin noul mandat, inclusiv în materie de certificare.

2.2.2. Metoda (metodele) de control preconizată (preconizate)

Conturile agenției vor fi supuse aprobării Curții de Conturi, vor face obiectul procedurii descărcării de gestiune și sunt avute în vedere audituri.

De asemenea, operațiunile agenției fac obiectul supravegherii de către Ombudsman în conformitate cu dispozițiile articolului 228 din tratat.

A se vedea, de asemenea, punctele 2.1. și 2.2.1. de mai sus.

2.3. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

Ar urma să se aplice măsurile de prevenire și de protecție ale ENISA, și anume:

- personalul agenției verifică plățile pentru orice fel de servicii sau de studii solicitate, înainte de efectuarea plății, luând în considerare toate obligațiile contractuale, principiile economice și bunele practici financiare sau de gestionare; - toate acordurile și contractele încheiate între agenție și beneficiarii plăților vor cuprinde dispoziții antifraudă (control, cerințe privind raportarea etc.);

- pentru a combate fraudele, corupția și alte activități ilegale, dispozițiile Regulamentului (UE) nr. 883/2013 al Parlamentului European și al Consiliului din 25 mai 1999 privind investigațiile efectuate de Oficiul European Antifraudă (OLAF) se aplică fără restricții;

- agenția subscrie, în șase luni de la data intrării în vigoare a prezentului regulament, la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene și Comisia Comunităților Europene privind investigațiile interne ale Oficiului European Antifraudă (OLAF) și emite, fără întârziere, dispozițiile corespunzătoare care se aplică tuturor angajaților agenției.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul cheltuielilor	Contribuție			
		Dif./Nedif. [52]	Țări AELS[53]	Țări candidate[54]	Țări terțe	În sensul articolului 21 alineatul (2) litera (b) din Regulamentul financiar
1a Competitivitate pentru creștere economică și ocuparea forței de muncă	09.0203 ENISA și certificarea de securitate în domeniul tehnologiei informației și comunicațiilor	Dif.	DA	NU	NU	NU
5 Cheltuieli administrative]	09.0101 Cheltuieli cu personalul în activitate din domeniul Rețele de comunicare, conținut și tehnologie 09.0102 Cheltuieli cu personalul extern în activitate din domeniul Rețele de comunicare, conținut și tehnologie	Nedif.	NU	NU	NU	NU

[52] Dif. = credite diferențiate / Nedif. = credite nediferențiate.
[53] AELS: Asociația Europeană a Liberului Schimb.
[54] Țările candidate și, după caz, țările potențial candidate din Balcanii de Vest.

	09.010211 Alte cheltuieli de gestiune					

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	1a	Competitivitate pentru creștere economică și ocuparea forței de muncă

ENISA			**referință** **2017 (31/12/2016)**		**2019** ***(de la 1.7.2019)***	**2020**	**2021**	**2022**	**TOTAL**
Titlul 1: Cheltuieli cu personalul *(de asemenea, inclusiv cheltuielile legate de recrutarea personalului, formare, infrastructura sociomedicală și serviciile externe)*	Angajamente	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	Plăți	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Titlul 2: Cheltuieli de infrastructură și de funcționare	Angajamente	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	Plăți	(2 a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Titlul 3: Cheltuieli operaționale	Angajamente	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	Plăți	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTAL credite pentru ENISA	Angajamente	= 1 + 1a + 3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Plăți	=2+2 a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Rubrica din cadrul financiar multianual	**5**	„Cheltuieli administrative”

milioane EUR (cu trei zecimale)

		2019 *(de la 1.7.2019)*	**2020**	**2021**	**2022**	**TOTAL**
DG: CNECT						
• Resurse umane		0,216	0,846	0,846	0,846	**2,754**
• Alte cheltuieli administrative		0,102	0,235	0,238	0,242	**0,817**
TOTAL DG CNECT	Credite	0,318	1,081	1,084	1,088	**3,571**

Costurile cu personalul au fost calculate în funcție de data planificată pentru recrutare (se prevede că angajările de personal vor începe de la data de 1.7.2019).

Perspectivele privind resursele pentru perioada de după 2020 sunt orientative și nu aduc atingere propunerilor Comisiei pentru cadrul financiar multianual de după 2020

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)	0,318	1,081	1,084	1,088	**3,571**

milioane EUR (cu trei zecimale)

		2019	**2020**	**2021**	**2022**	**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1-5 din cadrul financiar multianual	Angajamente	16,868	21,727	23,332	24,11	**86,038**
	Plăți	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Impactul estimat asupra creditelor agenției

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☒ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTAL**
Sporirea capabilităților și a nivelului de pregătire ale statelor membre și ale întreprinderilor	1,408	1,900	1,931	1,969	7,208
Îmbunătățirea cooperării și a coordonării dintre statele membre și instituțiile, agențiile și organele UE	0,939	1,266	1,288	1,313	4,806
Capabilități sporite la nivelul UE care să completeze acțiunea statelor membre, în special în cazul unei crize cibernetice transfrontaliere.	0,704	0,950	0,965	0,985	3,604
Sporirea gradului de sensibilizare a cetățenilor și a întreprinderilor cu privire la aspectele legate de securitatea cibernetică.	0,704	0,950	0,965	0,985	3,604
Consolidarea încrederii în piața unică digitală și în inovarea digitală prin sporirea transparenței la nivel global a asigurării securității cibernetice a produselor și serviciilor TIC.	0,939	1,266	1,288	1,313	4,806
COSTURI TOTALE	4,694	6,332	6,437	6,565	24,028

[55] Acest tabel prezintă numai cheltuielile operaționale conform titlului 3.

3.2.3. Impactul estimat asupra resurselor umane ale agenției

3.2.3.1. Sinteză

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☒ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Q3/4 2019	**2020**	**2021**	**2022**
Agenți temporari (gradul AD)	4,242	5,695	6,381	6,709
Agenți temporari (gradul AST)	1,601	1,998	2,217	2,217
Agenți contractuali	2,041	2,041	2,041	2,041
Experți naționali detașați	0,306	0,447	0,656	0,796
TOTAL	**8,190**	**10,181**	**11,295**	**11,763**

Costurile cu personalul au fost calculate în funcție de data planificată pentru recrutare (s-a presupus că angajarea integrală a personalului actual al ENISA va avea loc începând cu 1.1.2019). S-a prevăzut că angajarea treptată de noi angajați va începe la 1.7.2019, iar angajarea integrală se va finaliza în 2022. Perspectivele privind resursele pentru perioada de după 2020 sunt orientative și nu aduc atingere propunerilor Comisiei pentru cadrul financiar multianual de după 2020

Impact estimat asupra personalului (ENI suplimentare) – schema de personal

Grupa de funcții și gradul	2017 **ENISA la ora actuală**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
Total AD	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Total AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Total AST/SC					
TOTAL GENERAL	48	12	10	7	3

Sarcinile personalului suplimentar AD/AST pentru realizarea obiectivelor instrumentului, astfel cum se descrie în secțiunea 1.4.2:

Sarcini	AD	AST	END	Total
Politici și consolidarea capacităților	8	1		9
Cooperare operațională	8	1	7	16
Certificare (sarcini legate de piață)	9	3	2	14
Cunoștințe, informare și sensibilizare	1	1		2
TOTAL	26	6	9	41

Descrierea sarcinilor care trebuie efectuate:

Sarcini	**Resursele suplimentare necesare**
Dezvoltarea și punerea în aplicare a politicilor UE & Consolidarea capacităților	Sarcinile ar include acordarea de asistență grupului de cooperare, sprijinirea punerii în aplicare coerente la nivel transfrontalier a Directivei privind securitatea rețelelor și a informațiilor, întocmirea de rapoarte periodice privind situația punerii în aplicare a cadrului juridic al UE; consilierea și coordonarea inițiativelor sectoriale din domeniul securității cibernetice, inclusiv din domeniul energiei, transporturilor (de exemplu, aerian/rutier/maritim/al vehiculelor conectate),

	sănătății, finanțelor, oferirea de sprijin pentru înființarea de centre de schimb și analiză de informații în diverse sectoare.
Cooperarea operațională și gestionarea crizelor	**Sarcinile ar include:** Activități de secretariat pentru rețeaua CSIRT prin asigurarea, printre altele, a bunei funcționări a infrastructurii IT și a canalelor de comunicare ale rețelei CSIRT. Asigurarea unei cooperări structurate cu CERT-UE, cu EC3 și cu alte organisme competente ale UE. Organizarea **exercițiilor Cyber Europe**[56] - sarcini legate de desfășurarea mai frecventă a exercițiului, o dată pe an în loc de o dată la doi ani, și asigurarea că acesta analizează incidentul de la început până la sfârșit. **Asistență tehnică -** sarcinile ar include o cooperare structurată cu CERT-UE în vederea furnizării de asistență tehnică în cazul unor incidente semnificative și a sprijinirii analizei incidentelor. Aceasta ar include oferirea de asistență statelor membre pentru gestionarea incidentelor și analiza vulnerabilităților, artefactelor și incidentelor. Facilitează cooperarea dintre statele membre în ceea ce privește răspunsul în situații de urgență, prin analizarea și agregarea rapoartelor situaționale naționale pe baza informațiilor puse la dispoziția agenției de către statele membre și alte entități. **Un plan de acțiune privind răspunsul coordonat la incidentele de securitate cibernetică transfrontaliere de mare amploare -** agenția va contribui la dezvoltarea unui răspuns bazat pe cooperare, atât la nivelul Uniunii, cât și la nivelul statelor membre, la incidentele sau crizele transfrontaliere de mare amploare legate de securitatea cibernetică prin intermediul unor sarcini diverse - de la contribuția la cunoașterea situației la nivelul Uniunii, la testarea planurilor de cooperare pentru incidente. **Anchete tehnice *ex post* privind incidentele** - efectuarea sau participarea la anchetele tehnice *ex*

[56] Cyber Europe este cel mai mare și mai cuprinzător exercițiu de securitate cibernetică al UE de până în prezent, la care participă peste 700 de specialiști în domeniul securității cibernetice din toate cele 28 de state membre. Se desfășoară o dată la doi ani. Evaluarea ENISA și Strategia de securitate cibernetică a UE din 2013 indică faptul că numeroase părți interesate susțin transformarea Cyber Europe într-un eveniment anual, având în vedere evoluția rapidă a amenințărilor cibernetice. Însă acest lucru nu este posibil în prezent din cauza resurselor limitate ale agenției.

	post privind incidentele în cooperare cu rețeaua CSIRT, în scopul formulării de recomandări și al consolidării capabilităților, sub forma unor rapoarte publice, în vederea unei mai bune preveniri a incidentelor viitoare.
Sarcini legate de piață (standardizare, certificare)	Sarcinile ar include sprijinirea activă a activităților desfășurate în contextul cadrului de certificare, inclusiv furnizarea de expertiză tehnică pentru pregătirea propunerilor de sisteme europene de certificare de securitate cibernetică. Sarcinile vor include, de asemenea, sprijin pentru elaborarea și punerea în aplicare a politicii Uniunii privind standardizarea, certificarea și observatorul pieței - acest lucru va necesita facilitarea adoptării de standarde de gestionare a riscurilor produselor, rețelelor și serviciilor electronice și consilierea operatorilor de servicii esențiale și furnizorilor de servicii digitale cu privire la cerințele tehnice de securitate. Sarcinile vor include, de asemenea, furnizarea de analize privind principalele tendințe de pe piața securității cibernetice.
Cunoștințe și informații, acțiuni de sensibilizare:	În vederea asigurării unui acces mai ușor la informații mai bine structurate privind riscurile legate de securitatea cibernetică și măsurile corective posibile, propunerea conferă agenției o sarcină nouă - aceea de a dezvolta și a întreține „platforma de informare” a Uniunii. Sarcinile ar include colectarea, organizarea și punerea la dispoziția publicului, prin intermediul unui portal dedicat, de informații privind securitatea rețelelor și a sistemelor informatice, în special securitatea cibernetică, furnizate de instituțiile, agențiile și organele UE. Sarcinile ar include, de asemenea, sprijinirea activităților ENISA în domeniul creșterii gradului de sensibilizare pentru a permite agenției să își intensifice eforturile.

3.2.3.2. Necesarul de resurse umane estimat pentru DG-ul sub tutela căruia se află agenția

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ☒ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimarea se exprimă în numere întregi (sau cel mult cu o zecimală)

		Personal suplimentar			
	Nivelul de referință din 2017	Q3/4 2019	2020	2021	2020
• **Posturi din schema de personal (funcționari și agenți temporari)**					
09 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)	1	2	3		
• **Personal extern (în echivalent normă întreagă: ENI)**[57]					
09 01 02 01 (AC, END, INT din „pachetul global”)	1	2			
TOTAL		**4**	**3**		

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	Reprezintă Comisia în cadrul consiliului de administrație al agenției. Elaborează avizul Comisiei privind documentul unic de programare al ENISA și monitorizează punerea în aplicare a acestuia. Supraveghează întocmirea bugetului agenției și monitorizează execuția sa. Acordă asistență agenției în ceea ce privește dezvoltarea activităților sale în concordanță cu politicile Uniunii, inclusiv prin participarea la reuniuni relevante. Supraveghează punerea în aplicare a cadrului pentru sistemele europene de certificare de securitate cibernetică a produselor și serviciilor TIC. Menține contacte cu statele membre și alte părți interesate în legătură cu activitatea de certificare. Cooperează cu ENISA în ceea ce privește propunerile de sisteme. Pregătește propuneri de sisteme europene de securitate cibernetică.
Personal extern	Ca mai sus

[57] AC = agent contractual; AL = agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JED = expert tânăr în delegații.

3.2.4. Compatibilitatea cu actualul cadru financiar multianual

– ☐ Propunerea/inițiativa este compatibilă cu actualul cadru financiar multianual.

– ☒ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

Propunerea necesită reprogramarea articolului 09 02 03 din cauza revizuirii mandatului ENISA, care conferă agenției sarcini noi referitoare, printre altele, la punerea în aplicare a Directivei privind securitatea rețelelor și a informațiilor și la cadrul european de certificare de securitate cibernetică. Sumele corespunzătoare:

Anul	Avute în vedere	Solicitate
2019	10,739	16,550
2020	10,954	20,646
2021	N/A	22,248*
2022	N/A	23,023*

* Aceasta este o cifră estimativă. Finanțarea UE după 2020 va fi examinată în cadrul unei dezbateri la nivelul Comisiei privind toate propunerile pentru perioada de după 2020. Aceasta înseamnă că, odată ce Comisia a făcut propunerea pentru următorul cadru financiar multianual, aceasta va prezenta o situație financiară legislativă modificată, ținând seama de concluziile evaluării impactului[58].

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[59].

3.2.5. Contribuția terților

– ☐ Propunerea/inițiativa nu prevede cofinanțare din partea terților.

– ☒ Propunerea/inițiativa prevede cofinanțare, estimată în cele ce urmează:

	Anul **2019**	Anul **2020**	Anul **2021**	Anul **2022**
AELS	p.m.[60]	p.m.	p.m.	p.m.

58 Link către pagina cu evaluarea impactului

59 A se vedea articolele 11 și 17 din Regulamentul (UE, Euratom) nr. 1311/2013 al Consiliului de stabilire a cadrului financiar multianual pentru perioada 2014-2020.

60 Suma exactă pentru următorii ani va fi cunoscută atunci când se va stabili factorul de proporționalitate al AELS pentru anul în cauză.

3.3. Impactul estimat asupra veniturilor

– ☒ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

  – ☐ asupra resurselor proprii

  – ☐ asupra veniturilor diverse