Consiliul
Uniunii Europene

Bruxelles, 29 mai 2018
(OR. en)

9350/18

Dosar interinstituțional:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTĂ

Sursă:	Președinția
Destinatar:	Consiliul
Nr. doc. ant.:	8834/18
Nr. doc. Csie:	12183/17
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”) - Abordare generală

I. INTRODUCERE

1. La 13 septembrie 2017, în contextul strategiei sale privind piața unică digitală, Comisia a adoptat și a transmis Consiliului și Parlamentului European propunerea sus-menționată [1], având ca temei juridic articolul 114 din TFUE. Făcând parte din așa-numitul „pachet privind securitatea cibernetică", această propunere vizează atingerea unui nivel ridicat de securitate cibernetică, de reziliență cibernetică și de încredere în Uniune, cu scopul de a asigura buna funcționare a pieței interne.

2. Propunerea de regulament stabilește obiectivele, sarcinile și aspectele organizaționale ale ENISA – Agenția UE pentru Securitate Cibernetică – și creează un cadru pentru instituirea unor sisteme europene de certificare de securitate cibernetică în vederea asigurării unui nivel adecvat de securitate cibernetică al produselor și serviciilor TIC în Uniune. Propunerea Comisiei este însoțită de o evaluare a impactului care analizează un set specific format din opt opțiuni de politică, care se referă la revizuirea ENISA și la certificarea de securitate cibernetică în domeniul TIC.

3. Propunerea de regulament cuprinde două direcții majore:

   - un mandat permanent pentru agenție cu o sferă de întindere delimitată în funcție de necesitățile care derivă din noile priorități și instrumente de politică și un set reînnoit de sarcini și funcții pentru agenție, astfel încât să poată fi acordat un sprijin efectiv și eficace eforturilor depuse de statele membre, de instituțiile UE și de alte părți interesate în scopul asigurării unui spațiu cibernetic sigur;

   - un cadru european de certificare de securitate cibernetică pentru produsele și serviciile TIC și norme care să guverneze sistemele europene de certificare de securitate cibernetică, permițând ca certificatele eliberate în cadrul respectivelor sisteme să fie valabile și recunoscute în toate statele membre și abordând actuala fragmentare a pieței.

[1] Doc. 12183/17; 12183/1/17 REV 1; 12183/2/17 REV 2.

4. În octombrie 2017, Consiliul European [2] a solicitat ca propunerile Comisiei privind securitatea cibernetică să fie elaborate într-un mod holistic, să fie transmise în timp util și să fie examinate fără întârziere, pe baza unui plan de acțiune care urmează să fie stabilit de către Consiliu.

5. La 12 octombrie 2017, Consiliul Afaceri Generale a adoptat Planul de acțiune [3] pentru punerea în aplicare a concluziilor Consiliului [4] privind comunicarea comună [5] către Parlamentul European și Consiliu intitulată „Reziliență, prevenire și apărare: construirea unei securități cibernetice puternice pentru UE" Planul de acțiune a reflectat ambiția Consiliului de a ajunge la o abordare generală cu privire la propunere până în luna iunie 2018.

6. În Parlamentul European, dna Angelika NIEBLER (ITRE, PPE) a fost numită raportor. Votul Comisiei ITRE asupra raportului urmează să aibă loc la 19 iunie 2018.

7. Comitetul Economic și Social European a adoptat avizul său la 14 februarie 2018.

II. LUCRĂRILE DIN CADRUL CONSILIULUI

8. Comisia și-a prezentat propunerea și evaluarea impactului aferentă acesteia în cadrul Grupului de lucru orizontal pentru chestiuni cibernetice (denumit în continuare „grupul de lucru") la 26 septembrie 2017; a urmat o analiză a evaluării impactului în cadrul grupului de lucru la 20 octombrie 2017. Discuțiile ulterioare s-au axat pe capacitatea operațională a agenției și pe amploarea interacțiunii cu autoritățile naționale competente, precum și pe impactul cadrului de certificare asupra pieței și a competitivității întreprinderilor. În general, atât evaluarea impactului, cât și propunerea s-au bucurat de o reacție pozitivă din partea delegațiilor.

---

2 EUCO 14/17, punctul 11.
3 Doc. 15748/17.
4 Doc. 14435/17.
5 Doc. 12211/17.

9. În noiembrie 2017, în timpul președinției estoniene, grupul de lucru a început discuțiile privind propunerea propriu-zisă, acestea continuând în timpul președinției bulgare. Au avut loc 12 reuniuni în legătură cu propunerea, în urma cărora au rezultat opt versiuni consecutive revizuite ale propunerii, în scopul de a se ajunge la o abordare generală cu ocazia viitorului Consiliu TTT (Telecom) din 8 iunie 2018.

10. Rezultatul discuțiilor desfășurate în cadrul grupului de lucru la 14-15 mai 2018, precum și textul revizuit de compromis al Președinției figurează în anexa la prezenta notă. Considerentele au fost adaptate pentru a reflecta modificările aduse dispozițiilor de fond. Toate modificările aduse propunerii Comisiei sunt marcate cu **caractere aldine** sau cu [...]. Modificările față de ultimul document al grupului de lucru, 8834/18, sunt marcate cu **caractere aldine subliniate**, iar eliminările sunt indicate prin **[...]**.

III. CONCLUZIE

11. Textul de compromis al Președinției, astfel cum figurează în anexă, reflectă eforturile Președinției și ale statelor membre de a ajunge la un echilibru adecvat în text.

12. La 25 mai 2018, Comitetul Reprezentanților Permanenți a ajuns la un acord cu privire la textul de compromis al Președinției, sub rezerva modificărilor de la articolele 19 alineatul (5) și 48 alineatul (5), astfel cum figurează în anexă.

13. Prin urmare, Consiliul este invitat să adopte o abordare generală în cadrul reuniunii sale din 8 iunie 2018 și să mandateze Președinția să inițieze negocieri cu reprezentanții Parlamentului European și ai Comisiei Europene cu privire la acest dosar.

ANEXĂ

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind ENISA, „*Agenția [...] Uniunii Europene 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 ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European [6],

având în vedere avizul Comitetului Regiunilor [7],

hotărând în conformitate cu procedura legislativă ordinară,

[6] JO C , , p. .
[7] JO C , , p. .

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 (TIC) 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. Digitalizarea 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, milioane, dacă nu chiar miliarde de dispozitive digitale conectate vor intra în folosință în UE în următorul deceniu. Deși numărul dispozitivelor conectate la internet este în creștere, securitatea și reziliența nu sunt incluse suficient din faza de proiectare, ceea ce duce 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 despre caracteristicile de securitate cibernetică ale produselor și serviciilor TIC, ceea ce erodează încrederea în soluțiile digitale.

(3) Creșterea gradului de digitalizare și conectivitate duce la agravarea riscurilor pentru securitatea cibernetică, societatea, în general, devenind astfel mai vulnerabilă la amenințările cibernetice, iar pericolele cu care se confruntă persoanele fizice, mai ales 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 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 conectate 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, pentru sector și pentru 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, a provocărilor și a 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 nevoie de 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 [8] 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, Parlamentul European și Consiliul au adoptat Regulamentul (CE) nr. 1007/2008 [9], prelungind mandatul agenției până în martie 2012. Regulamentul (UE) nr. 580/2011 [10] a prelungit din nou mandatul agenției până la 13 septembrie 2013. În 2013, Parlamentul European și Consiliul au adoptat Regulamentul (UE) nr. 526/2013 [11] privind ENISA și de abrogare a Regulamentului (CE) nr. 460/2004, prin care mandatul agenției a fost prelungit până în iunie 2020.

---

[8] 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).

[9] 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).

[10] 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).

[11] 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).

(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, Uniunea a adoptat în 2016 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 NIS”). Directiva NIS 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 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 europene.

(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 **sprijine** [...] eforturile depuse la nivel național **și să contribuie proactiv** la eforturile depuse la nivelul UE, îndeplinindu-și totodată sarcinile în deplină cooperare cu instituțiile, [...] agențiile **și organele** 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, **precum și privind aspectele sale sectoriale pentru a consolida relevanța politicilor și legislației UE cu o dimensiune de securitate cibernetică și pentru a permite punerea lor în aplicare în mod coerent la nivel național** [...]. 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 NIS, care este esențială pentru sporirea rezilienței cibernetice. Având în vedere evoluția rapidă a naturii amenințărilor pentru securitatea cibernetică, 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, [...] agențiilor **și organelor** 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 [...] **amenințările** și incidentele [...] cibernetice 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. **Activitățile desfășurate de ENISA în privința capacităților operaționale ale statelor membre ar trebui să fie exclusiv complementare propriilor măsuri luate de statele membre pentru a-și îndeplini obligațiile ce decurg din Directiva NIS, netrebuind deci să li se substituie [...]**.

(15a) Agenția ar trebui de asemenea să acorde asistență la elaborarea și actualizarea strategiilor Uniunii și, la cerere, ale statelor membre în materie de securitate a rețelelor și a sistemelor informatice, în special în ceea ce privește securitatea cibernetică, să promoveze diseminarea lor și să le monitorizeze punerea în aplicare. 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 NIS 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, [...] **agenția ar trebui** să sprijine **schimbul de informații în cadrul sectoarelor și între acestea, mai ales în sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, furnizând bune practici și orientări despre instrumentele disponibile, proceduri și îndrumări despre modul de abordare a chestiunilor de reglementare legate de schimbul de informații, de exemplu prin facilitarea** [...] înființării unor centre sectoriale de schimb și de analiză de informații (ISACs) [...].

(18) Agenția ar trebui să agrege și să analizeze rapoartele naționale **puse la dispoziție în mod voluntar** de CSIRT și CERT-UE, **în scopul de a acorda asistență statelor membre** la stabilirea unor [...] **proceduri**, limbaje și terminologii comune pentru schimbul de informații. Agenția ar trebui de asemenea să atragă participarea sectorului privat, în cadrul Directivei NIS care a prevăzut bazele schimbului voluntar de informații tehnice la nivel operațional [...] **în cadrul** rețelei 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 îndeplinită în conformitate cu mandatul care îi revine în temeiul prezentului regulament, iar statele membre ar trebui să convină asupra unei abordări în contextul Recomandării Comisiei privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare**. **Ea ar putea** include 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 cooperării prin exerciții [...] **periodice** de securitate cibernetică.

(20) [...] **În sprijinirea** cooperării **operaționale** [...], agenția ar trebui să apeleze la expertiza **tehnică și operațională** de care dispune CERT-UE, prin intermediul unei cooperări structurate [...]. [...] 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 **și pentru a se evita duplicarea activităților**.

(21) În conformitate cu sarcinile sale [...] **de sprijinire a cooperării operaționale în cadrul rețelei CSIRT**, agenția ar trebui să aibă posibilitatea de a oferi sprijin statelor membre, **la cererea lor,** de exemplu prin furnizarea de consiliere **privind modul de îmbunătățire a capabilităților lor de a preveni incidentele, de a le detecta și de a reacționa la ele, prin [...] facilitarea** [...] **gestionării din punct de vedere** tehnic a incidentelor **care au un impact semnificativ sau substanțial** [...] sau **prin** asigurarea analizelor amenințărilor și incidentelor. **În cadrul facilitării gestionării din punct de vedere tehnic a incidentelor care au un impact semnificativ sau substanțial, ENISA ar trebui, mai ales, să sprijine partajarea în mod voluntar a soluțiilor tehnice de către statele membre sau să producă informații tehnice combinate, de exemplu soluții tehnice partajate în mod voluntar de statele membre.** 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 un ajutor suplimentar pentru ENISA în [...] **sprijinirea cooperării 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 **și în strânsă cooperare cu statele membre** 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 [...] sau de punctele unice de contact instituite prin Directiva NIS **(în ambele cazuri în mod voluntar)**, de Centrul european de combatere a criminalității informatice (EC3) din cadrul Europolului 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) **Sprijinul acordat de agenție**, la cererea [...] statelor membre [...] **afectate**, pentru **anchetele** tehnice ex-post privind incidentele cu consecințe importante [...] ar trebui să se axeze pe prevenirea viitoarelor incidente [...]. **Statele membre afectate ar trebui să furnizeze informațiile necesare pentru a-i permite agenției să sprijine efectiv anchetele tehnice.**

(24) […]

(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 ca în cooperare cu statele membre și, după caz, cu organismele de statistică și cu alte entități să colecteze informațiile relevante **care sunt puse la dispoziția publicului sau care sunt partajate în mod voluntar**, 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 [...] **incidentelor** de securitatea cibernetică, prin efectuarea unor analize ale amenințărilor și incidentelor.

(27) Pentru a spori reziliența Uniunii, agenția ar trebui să vizeze excelența în materie de securitate **cibernetică** a infrastructurilor **care susțin mai ales sectoarele enumerate în anexa II la Directiva NIS, precum și a celor utilizate de furnizorii de servicii digitale enumerați în anexa III la aceeași directivă** [...], 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, [...] agențiile **și organele** 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 Europolului, 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), **Agenția pentru Sistemul Global de Navigație prin Satelit European (Agenția GNSS)** 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 rolul său** de [...] secretariat al 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 NIS. 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 [...] **periodice** de securitate cibernetică la nivelul Uniunii și să ajute statele membre și instituțiile, agențiile și organele UE, la cererea acestora, 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, [...] agențiile **și organele** Uniunii și, după caz, statele membre, la solicitarea acestora, cu privire la necesitățile în domeniul [...] securității cibernetice. **Pentru a identifica necesitățile și prioritățile în materie de cercetare, agenția ar trebui să consulte grupurile de utilizatori relevante.**

(37) **Amenințările pentru** [...] securitatea cibernetică au o dimensiune mondială. Este nevoie de o cooperare internațională mai strânsă pentru îmbunătățirea standardelor de securitate **cibernetică**, inclusiv prin definirea unor norme de comportament comune, și a schimburilor de informații, încurajând o colaborare internațională mai rapidă ca reacție la problemele de securitate a rețelelor și a informațiilor, precum și o abordare comună 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, [...] agențiilor **și organelor** relevante ale Uniunii.

(38) Agenția ar trebui să fie în măsură să răspundă solicitărilor ad-hoc de consiliere și asistență care îi sunt adresate de 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 **cuprinzând și punerea în aplicare a programului anual de lucru al agenției**, 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 [12]. 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 [13]. 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.

---

[12] 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).

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

(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) [...]

(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 NIS.

(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 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 **proceselor,** 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 eliberat 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, [...] 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 **și a declarațiilor de conformitate UE** pentru produse și servicii TIC. Cadrul european ar trebui să aibă un dublu scop: pe de o parte, 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, 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. Sistemele ar trebui să fie nediscriminatorii și să se bazeze pe standarde internaționale și/sau [...] **europene**, 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 **procese**, produse și servicii TIC. Aceste sisteme ar trebui să fie puse în aplicare și supervizate de către autoritățile naționale [...] de certificare **de securitate cibernetică**, iar certificatele eliberate 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 **proceselor**, produselor și serviciilor TIC certificate în temeiul unui astfel de sistem, **[...] pentru a [...] proteja** disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate ori transmise sau prelucrate ori funcțiile sau serviciile oferite prin aceste produse, procese, servicii și sisteme sau accesibile prin intermediul lor **pe durata întregului lor ciclu de viață**, în sensul prezentului regulament. În prezentul regulament nu pot fi detaliate cerințele de securitate cibernetică referitoare la toate **procesele**, produsele și serviciile TIC. **Procesele**, 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 **procese**, produse și servicii TIC specifice ar trebui 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 **atunci când nu sunt disponibile standarde corespunzătoare**.

(55a) Specificațiile tehnice de utilizat într-un sistem european de certificare de securitate cibernetică ar trebui identificate prin respectarea principiilor prevăzute în anexa II la Regulamentul (UE) 1025/2012. Cu toate acestea, s-ar putea considera necesare unele abateri de la aceste principii în cazuri justificate corespunzător, când respectivele specificații tehnice sunt destinate utilizării într-un sistem european de certificare de securitate cibernetică care face trimitere la nivelul de asigurare ridicat. Motivele care stau la baza acestor abateri trebuie puse la dispoziția publicului.

(55b) Evaluarea certificată a conformității este procesul prin care se evaluează dacă au fost îndeplinite cerințele specifice referitoare la un proces, produs sau serviciu TIC. Acest proces este efectuat de o parte terță independentă, alta decât fabricantul produsului sau furnizorul serviciului. Procesul de eliberare a unui certificat este ulterior procesului de evaluare pozitivă a unui proces, produs sau serviciu TIC. Ar trebui să fie considerat drept o confirmare a faptului că respectiva evaluare s-a derulat în mod adecvat. În funcție de nivelul de asigurare, sistemul european de securitate cibernetică ar trebui să determine dacă certificatul este eliberat de un organism privat sau de unul public. Evaluarea și certificarea de conformitate nu pot garanta *per se* că produsele și serviciile TIC certificate îndeplinesc condițiile de securitate cibernetică. Este vorba, mai degrabă, de o procedură și de o metodologie tehnică menite să ateste 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.

(55c) Alegerea, de către utilizatorii certificatelor, a nivelului adecvat de certificare și a cerințelor de securitate aferente ar trebui să se bazeze pe o evaluare a riscurilor legate de utilizarea procesului, produsului sau serviciului TIC. Astfel, nivelul de asigurare ar trebui să fie proporțional cu nivelul riscului asociat cu utilizarea preconizată a unui proces, produs sau serviciu TIC.

(55d) Un sistem european de certificare de securitate cibernetică ar putea să prevadă efectuarea unei evaluări de conformitate pe răspunderea exclusivă a fabricantului sau a furnizorului de produse și servicii TIC (autoevaluare a conformității). În astfel de cazuri, este suficient ca fabricantul sau furnizorul să efectueze el însuși toate verificările pentru a asigura conformitate proceselor, produselor sau serviciilor TIC cu sistemul de certificare. Acest tip de evaluare de conformitate ar trebui considerat adecvat pentru produse și servicii TIC având o complexitate redusă (de pildă atunci când concepția și mecanismul de producție sunt simple) și care prezintă un risc scăzut pentru interesul public. În plus, numai produsele și serviciile TIC care corespund unui nivel de asigurare de bază ar putea face obiectul unei autoevaluări de conformitate.

(55e) Un sistem european de certificare de securitate cibernetică ar putea permite atât certificarea, cât și autoevaluarea de conformitate a produselor și serviciilor TIC. În acest caz, sistemul ar trebui să prevadă modalități clare și ușor de înțeles, astfel încât consumatorii și alți utilizatori să diferențieze produsele și serviciile care sunt evaluate pe răspunderea fabricantului sau a furnizorului de produsele și serviciile care sunt certificate de o parte terță.

(55f) Fabricantul sau furnizorul de produse și servicii TIC care efectuează o autoevaluare de conformitate ar trebui să întocmească și să semneze declarația de conformitate UE în cadrul procedurii de evaluare a conformității. Declarația de conformitate UE este documentul care specifică că produsul sau serviciul TIC în cauză este conform cu cerințele sistemului. Prin întocmirea și semnarea declarației de conformitate UE, fabricantul sau furnizorul își asumă răspunderea pentru conformitatea produsului sau serviciului TIC cu cerințele legale ale sistemului. O copie a declarației de conformitate UE ar trebui transmisă autorității naționale de certificare de securitate cibernetică și ENISA.

(55g) Fabricantul sau furnizorul de produse și servicii TIC ar trebui să păstreze la dispoziția autorității naționale competente de certificare de securitate cibernetică, pe durata stabilită în sistemul european de certificare de securitate cibernetică corespunzător, declarația de conformitate UE și documentația tehnică conținând toate informațiile relevante legate de conformitatea produselor sau serviciilor TIC cu un sistem. Documentația tehnică ar trebui să specifice cerințele aplicabile și să acopere, în măsura relevantă pentru evaluare, proiectarea, fabricarea și exploatarea produsului sau serviciului TIC. Documentația tehnică ar trebui să fie alcătuită astfel încât să permită evaluarea conformității unui produs sau serviciu TIC cu cerințele relevante.

(55h) Statele membre și organizațiile interesate ar trebui să aibă dreptul să recomande Grupului european pentru certificarea de securitate cibernetică pregătirea unei propuneri de sistem. Organizațiile interesate sunt organizațiile care reprezintă industria sau consumatorii, inclusiv reprezentanți ai organizațiilor de IMM-uri care au un interes întemeiat în dezvoltarea unui anumit sistem european de certificare de securitate cibernetică. Aceste propuneri ar trebui examinate din perspectiva criteriilor elaborate de Grupul european pentru certificarea de securitate cibernetică prin orientări bazate pe principiile de transparență, deschidere, imparțialitate, consens, eficacitate, relevanță și coerență.

(56) Comisia [...] **și grupul** ar trebui să fie împuternicite să adreseze ENISA solicitarea de a pregăti **fără întârzieri nejustificate** propuneri de sisteme pentru **procese**, produse sau servicii TIC specifice. Pe baza propunerii de sistem prezentate de ENISA, Comisia ar trebui să fie apoi împuternicită 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 **procese**, 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 de evaluare și metodele de evaluare, precum și nivelul de asigurare vizat: de bază, substanțial și/sau ridicat **și nivelurile de evaluare, după caz**.

(56a) Asigurarea pe care o oferă un sistem european de certificare este motivul încrederii că un proces, produs sau serviciu TIC îndeplinește cerințele de securitate ale unui sistem european de securitate cibernetică specific. Pentru a asigura coerența cadrului referitor la procesele, produsele și serviciile TIC certificate, un sistem european de certificare de securitate cibernetică ar putea să specifice niveluri de asigurare pentru certificatele europene de securitate cibernetică și pentru declarațiile de conformitate UE eliberate în cadrul respectivului sistem. Fiecare certificat sau declarație de conformitate UE s-ar putea referi la unul din nivelurile de asigurare: de bază, substanțial sau ridicat, însă declarația de conformitate UE nu s-ar putea referi decât la nivelul de asigurare de bază. Nivelurile de asigurare indică un grad corespunzător al eforturilor de evaluare [...] și se caracterizează prin trimitere la specificațiile tehnice și cu standardele și procedurile conexe, incluzând controale tehnice, al căror scop este atenuarea sau prevenirea incidentelor de securitate cibernetică. Fiecare nivel de asigurare ar trebui să fie coerent în cadrul diferitelor domenii sectoriale în care se aplică certificarea.

(56b) Un sistem european de certificare de securitate cibernetică poate specifica mai multe niveluri de evaluare în funcție de rigurozitatea și profunzimea metodologiei de evaluare utilizate, care ar trebui să corespundă unuia din nivelurile de asigurare și să fie asociate unei combinații adecvate de componente ale asigurării. Pentru toate nivelurile de asigurare, produsul sau serviciul TIC ar trebui să conțină o serie de funcții securizate, astfel cum sunt definite de sistem, care pot include: o configurație securizată a produsului livrat, un cod semnat, o actualizare securizată, atenuarea consecințelor defectelor de exploatare (*exploit mitigation)* și protecția completă a memoriilor în stivă/heap. Aceste funcții ar fi trebuit să fie dezvoltate și întreținute prin utilizarea unor abordări axate pe dezvoltare și prin instrumente conexe pentru a asigura că sunt încorporate în mod fiabil mecanisme eficace (atât software, cât și hardware). Pentru nivelul de asigurare de bază, evaluarea ar trebui să se bazeze cel puțin pe următoarele componente ale asigurării: evaluarea ar trebui să includă cel puțin o analiză a documentației tehnice a produsului sau serviciului TIC de către organismul de evaluare a conformității. În cazul în care certificarea include procese TIC, procesul utilizat pentru proiectarea, dezvoltarea și întreținerea unui produs sau serviciu TIC ar trebui de asemenea să facă obiectul analizei tehnice. În cazul în care un sistem european de certificare de securitate cibernetică prevede o autoevaluare de conformitate, ar trebui să fie suficient dacă fabricantul sau furnizorul a efectuat o autoevaluare privind conformitatea proceselor, produselor sau serviciilor TIC cu sistemul de certificare. Pentru nivelul de asigurare substanțial, evaluarea ar trebui să se bazeze, în plus față de elementele necesare pentru nivelul de asigurare de bază, cel puțin pe verificarea conformității funcțiilor de securitate ale produsului sau serviciului TIC cu documentația sa tehnică. Pentru nivelul de asigurare ridicat, evaluarea ar trebui să se bazeze, în plus față de elementele necesare pentru nivelul de asigurare substanțial, cel puțin pe un test de eficacitate care să evalueze rezistența funcțiilor de securitate ale produsului sau serviciului TIC împotriva celor care lansează atacuri cibernetice elaborate având competențe și resurse semnificative.

(56c) Atunci când pregătește o propunere de sistem, ENISA ar trebui să consulte toate părțile interesate relevante, cum ar fi organizațiile europene de standardizare, autoritățile naționale relevante, organizațiile întemeiate pe baza acordurilor de recunoaștere reciprocă, precum ARR al SOG-IS, IMM-urile, organizațiile consumatorilor, precum și părțile interesate din domeniul mediului și social.

(56d) ENISA ar trebui să întrețină un site web care să ofere informații despre sistemele europene de certificare de securitate cibernetică și să le facă publicitate, conținând, printre altele, cererile de pregătire a unei propuneri de sistem european de certificare de securitate cibernetică, precum și observațiile primite în cadrul procesului de consultare derulat de ENISA în etapa de pregătire. Un astfel de site ar trebui să ofere informații și despre certificatele și declarațiile de conformitate UE eliberate în temeiul prezentului regulament.

(57) Recurgerea la certificarea europeană de securitate cibernetică **și la declarația de conformitate UE** ar trebui să rămână voluntară, cu excepția cazului în care există dispoziții contrare în legislația Uniunii sau în cea națională **adoptată în conformitate cu dreptul Uniunii**. **În lipsa unei legislații armonizate, statele membre pot adopta reglementări tehnice la nivel național, în conformitate cu Directiva (UE) 2015/1535, care să prevadă certificarea obligatorie în cadrul unui sistem european de certificare de securitate cibernetică. Statele membre ar putea recurge astfel la certificarea europeană de securitate cibernetică în contextul achizițiilor publice și al Directivei 2014/214/UE**.[...]

(57a) 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. Cu toate acestea, statele membre nu ar trebui împiedicate să adopte sau să mențină sisteme naționale de certificare în scopuri de securitate națională.

(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 restricționeze, să suspende sau** 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) **[...]** Statele membre **[...] ar trebui** să desemneze una **sau mai multe** autorități [...] de certificare de securitate cibernetică care să supravegheze conformitatea **cu obligațiile ce decurg din prezentul regulament**. **Dacă un stat membru consideră că acest lucru este adecvat, sarcinile pot fi atribuite de asemenea unor autorități deja existente. Statele membre ar trebui să aibă în același timp posibilitatea de a decide, de comun acord cu alt stat membru, să desemneze una sau mai multe autorități de supraveghere pe teritoriul acestui alt stat membru. Autoritățile ar trebui în special să monitorizeze obligațiile fabricantului sau ale furnizorului de produse și servicii TIC stabiliți pe teritoriile lor respective în ceea ce privește declarația de conformitate UE și să asigure respectarea acestor obligații, să ofere asistență organismelor naționale de acreditare la monitorizarea și supravegherea activităților derulate de organismele de evaluare a conformității, oferindu-le expertiză și informații relevante, să autorizeze organismele de evaluare a conformității să își îndeplinească sarcinile atunci când respectă cerințele suplimentare prevăzute într-un sistem și să monitorizeze evoluțiile relevante în domeniul certificării de securitate cibernetică [...]**. Autoritățile naționale [...] de certificare de **securitate cibernetică** ar trebui să se ocupe de plângerile depuse de persoane fizice sau juridice în legătură cu certificatele **pe care le-au eliberat sau care au fost eliberate de organismele de evaluare a conformității corespunzând nivelului de asigurare ridicat** [...], 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, ele ar trebui să coopereze cu alte autorități naționale [...] de certificare **de securitate cibernetică** 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”), compus din **reprezentanți ai** autorităților naționale de [...] certificare de **securitate cibernetică sau ai altor autorități naționale competente**. Principalele sarcini ale grupului ar trebui să constea în furnizarea de 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 acordarea de asistență agenției și în cooperarea îndeaproape cu aceasta la pregătirea propunerilor de sisteme europene de certificare de securitate cibernetică, în recomandarea Comisiei să solicite agenției să pregătească o propunere de sistem european de certificare de securitate cibernetică și în adoptarea de avize adresate **agenției cu privire la propunerile de sisteme și adresate** Comisiei cu privire la întreținerea și revizuirea sistemelor europene de certificare de securitate cibernetică existente.

(60a) Grupul ar trebui să faciliteze schimbul de bune practici și de expertiză între autoritățile naționale de certificare a securității cibernetice responsabile cu autorizarea organismelor de evaluare a conformității și cu eliberarea certificatelor. Grupul ar trebui să sprijine dezvoltarea unui mecanism de evaluare inter pares în contextul pregătirii unei propuneri de sistem și al punerii sale în aplicare pentru organismele care eliberează certificatele europene de securitate cibernetică pentru nivelul de asigurare ridicat. Astfel de evaluări inter pares ar trebui îndeosebi să evalueze dacă organismele în cauză dispun de expertiza adecvată și dacă își îndeplinesc sarcinile în mod armonizat. Rezultatele evaluărilor inter pares ar trebui puse la dispoziția publicului. Aceste organisme pot adopta măsurile corespunzătoare pentru a-și adapta practicile și expertiza.

(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.

(61a) Pentru a facilita și mai mult comerțul și având în vedere că lanțurile de aprovizionare TIC sunt mondiale, Uniunea poate încheia, în conformitate cu articolul 218 din TFUE, acorduri de recunoaștere reciprocă referitoare la certificatele eliberate de sistemele instituite în temeiul cadrului european de certificare de securitate cibernetică. Ținând seama de avizele primite din partea ENISA și a Grupului european pentru certificarea de securitate cibernetică, Comisia poate recomanda inițierea negocierilor relevante. Fiecare sistem ar trebui să prevadă condiții specifice pentru recunoașterea reciprocă cu țări terțe.

(62) […]

(63) [...]

(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 [...] certificare de **securitate cibernetică** 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

(1) 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 [...] **Uniunii Europene** 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 **proceselor,** 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.

(2) **Prezentul regulament nu aduce atingere competențelor statelor membre în domeniul securității cibernetice și, în orice caz, nu aduce atingere activităților aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.**

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 **genera daune sau perturbări** la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor acestora și a persoanelor afectate, sau care poate avea un **alt fel de** impact negativ asupra acestora;

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 sau **evaluării conformității proceselor,** produselor și serviciilor tehnologiei informației și comunicațiilor (TIC) ce se încadrează în domeniul de aplicare al sistemului în cauză;

9a. „sistem național de certificare de securitate cibernetică” înseamnă un set cuprinzător de norme, de cerințe tehnice, de standarde și de proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității proceselor, produselor și serviciilor TIC ce se încadrează în domeniul de aplicare al sistemului în cauză;

10. „certificat european de securitate cibernetică” înseamnă un document [...] prin care se atestă că un anumit **proces**, produs sau serviciu TIC [...] **a fost evaluat în scopul verificării conformității cu** cerințele **de securitate** specifice prevăzute în cadrul unui sistem european de certificare de securitate cibernetică;

11. „produs [...] TIC” înseamnă orice element sau grup de elemente al rețelelor și al sistemelor informatice;

11a. „serviciu TIC” înseamnă orice serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informațiilor prin intermediul rețelelor și al sistemelor informatice;

11b. „proces TIC” înseamnă orice set de activități desfășurate pentru a proiecta, a dezvolta, a furniza și a întreține un produs sau un serviciu TIC;

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**;**

16a. „specificație tehnică” înseamnă un document care stabilește cerințele tehnice pe care trebuie să le îndeplinească procesul, produsul sau serviciul TIC;

16b. „nivel de asigurare” înseamnă un motiv de încredere că un proces, un produs sau un serviciu TIC întrunește cerințele de securitate ale unui sistem european de securitate cibernetică specific și indică nivelul la care a fost evaluat; nivelul de asigurare nu măsoară securitatea unui proces, produs sau serviciu TIC în sine.

TITLUL II

ENISA - „*Agenția [...] Uniunii Europene pentru Securitate Cibernetică*”

CAPITOLUL I

MANDAT ȘI OBIECTIVE *[...]*

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 întreaga** Uniune, **mai ales oferind sprijin statelor membre și instituțiilor, agențiilor și organelor Uniunii pentru a-și îmbunătăți securitatea cibernetică**. **Agenția servește drept punct de referință în ceea ce privește consilierea și expertiza în materie de securitate cibernetică pentru instituțiile, agențiile și organele Uniunii.**

(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.

(2a) În îndeplinirea sarcinilor sale, agenția acționează în mod independent și ține seama în cea mai mare măsură de expertiza națională a autorităților relevante ale statelor membre, evitând totodată duplicarea activităților.

(3) […]

Articolul 4

Obiective

(1) Agenția este un centru de expertiză în materie de securitate cibernetică, datorită independenței sale, a calității științifice și tehnice a consilierii și asistenței acordate și informațiilor furnizate, a transparenței procedurilor și metodelor sale de funcționare, precum și a 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 **Uniunii** legate de securitatea cibernetică**, inclusiv a politicilor sectoriale privind securitatea cibernetică**.

(3) Agenția sprijină consolidarea capacităților și procesul de pregătire în întreaga Uniune, furnizând asistență **instituțiilor, agențiilor și organelor** Uniunii, **precum și** statelor membre și părților interesate din sectorul public și privat pentru a spori protecția rețelelor și a sistemelor informatice ale acestora, pentru a dezvolta **și a îmbunătăți reziliența cibernetică și capacitățile de răspuns și pentru a dezvolta** aptitudini și competențe în domeniul securității cibernetice [...].

(4) Agenția promovează cooperarea și coordonarea la nivelul Uniunii între statele membre, instituțiile, agențiile și organele Uniunii și părțile interesate relevante **din sectorul public și privat** [...] cu privire la chestiuni legate de securitatea cibernetică.

(5) Agenția **contribuie la sporirea** [...] capabilităților de securitate cibernetică la nivelul Uniunii pentru a [...] **acorda asistență** statelor membre în ceea ce privește prevenirea amenințărilor cibernetice și reacția la acestea, în special în cazul incidentelor transfrontaliere.

(6) Agenția promovează recurgerea la certificare **în scopul de a se evita fragmentarea sistemelor de certificare în UE**. **În special, agenția contribuie** [...] 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.

CAPITOLUL IA
SARCINI

Articolul 5
[...] Elaborarea și punerea în aplicare a politicii și a dreptului Uniunii

Agenția contribuie la elaborarea și punerea în aplicare a politicii și a 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 [...] **incidentele** de securitate 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

[...] ***Consolidarea capacităților***

(1) Agenția acordă asistență:

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

(b) Instituțiilor, [...] agențiilor și **organelor** Uniunii, în ceea ce privește eforturile acestora de a îmbunătăți prevenirea, detectarea și analiza [...] **amenințărilor** și incidentelor în materie de securitate cibernetică și capacitatea de răspuns la acestea, **mai ales** 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 și **monitorizează** [...] diseminarea acestor strategii în întreaga Uniune pentru a favoriza 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 [...] **periodice** 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, **în ceea ce privește** [...] 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 **sprijină schimbul de informații în cadrul sectoarelor și între acestea** [...], 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

*[...] **Cooperarea operațională la nivelul Uniunii***

(1) Agenția sprijină cooperarea operațională între **statele membre, instituțiile, agențiile și** organele [...] Uniunii, precum și între părțile interesate.

(2) Agenția cooperează la nivel operațional și stabilește sinergii cu instituțiile, [...] agențiile **și organele** 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**, în această capacitate,** facilitează [...] schimbul de informații și cooperarea între membrii acesteia.

(4) Agenția **sprijină** [...] cooperarea operațională din cadrul rețelei CSIRT furnizând sprijin statelor membre**, la cererea lor,** prin:

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

(b) [...] **facilitarea gestionării** din punct de vedere tehnic [...] a incidentelor care au un impact semnificativ sau substanțial, **mai ales prin sprijinirea partajării voluntare a soluțiilor tehnice între statele membre**;

(c) analizarea vulnerabilităților, [...] și a incidentelor**;**

(ca) oferirea de sprijin pentru anchetele tehnice ex-post privind incidentele care au un impact semnificativ sau substanțial, în temeiul Directivei (UE) 2016/1148.

În îndeplinirea acestor sarcini, agenția și CERT-UE desfășoară o cooperare structurată pentru a beneficia de sinergii **și pentru a evita duplicarea activităților** [...].

(5) […]

[…]

(6) Agenția organizează exerciții **periodice** [...] 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. **Aceste exerciții la nivelul Uniunii pot include elemente tehnice, operaționale și strategice** [...]. **Din doi în doi ani se organizează un exercițiu la scară largă care va cuprinde toate elementele respective.** De asemenea, agenția contribuie la exercițiile sectoriale de securitate cibernetică și sprijină, după caz, organizarea acestora, împreună cu [...] **organizațiile** relevante **care pot** participa de asemenea la exercițiile de securitate cibernetică desfășurate la nivelul Uniunii.

(7) **În strânsă cooperare cu statele membre,** 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 [...] sau punctele unice de contact instituite prin Directiva NIS (**în ambele cazuri în mod voluntar** [...]); 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 **puse la dispoziție în mod voluntar**, 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) [...] **la cererea statelor membre, facilitarea** gestionării din punct de vedere tehnic a unui incident sau a unei crize, **mai ales** [...] **prin sprijinirea** partajării **voluntare** a soluțiilor tehnice între statele membre;

(d) sprijinirea **instituțiilor, agențiilor și organelor UE precum și, la cerere, a statelor membre, în ceea ce privește** comunicarea publică în legătură cu un incident sau cu o criză;

(e) **sprijinirea statelor membre, la cererea lor, pentru a** testa [...] planurile de cooperare pentru răspunsul la aceste incidente sau crize.

Articolul 8

[...] Piața, certificarea de securitate cibernetică și standardizarea

Agenția:

(a) sprijină și promovează elaborarea și punerea în aplicare a politicii Uniunii privind certificarea de securitate cibernetică a **proceselor**, 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 informatică pentru **procesele**, produsele și serviciile TIC în **cooperare cu întreprinderile din sector și 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 [...] certificare de **securitate cibernetică** și cu reprezentanți ai sectorului;

(3a) recomandarea unor specificații tehnice adecvate pentru recurgerea la dezvoltarea unor sisteme europene de certificare de securitate cibernetică, astfel cum se menționează la articolul 47 alineatul (1) litera (b), în cazurile în care standardele nu sunt disponibile;

(3b) contribuirea la o consolidare suficientă a capacităților în legătură cu procesele de evaluare și certificare prin compilarea și publicarea unor orientări, precum și oferind sprijin statelor membre, la cererea lor;

(b) facilitarea elaborării și adoptării de standarde europene și internaționale pentru gestionarea riscurilor și pentru securitatea **proceselor**, produselor, rețelelor și serviciilor [...]**;**

(ba) 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

[...] ***Cunoștințe*** *și* [...] **informații** [...]

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 **incidentelor** [...] de securitate 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 [...] infrastructurilor care sprijină sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, **precum și a celor utilizate de furnizorii de servicii digitale enumerați în anexa III la respectiva directivă;**

(d) colectează, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea cibernetică, furnizate de instituțiile, agențiile și organele Uniunii **și, în mod voluntar, de statele membre și de părțile interesate private și publice**;

(e) [...]

(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) [...].

Articolul 9a

Sensibilizare și educare

Agenția:

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

(b) **organizează, în cooperare cu statele membre și cu instituțiile, agențiile și organele Uniunii, precum și cu sectoarele industriale, campanii periodice de informare pentru sporirea securității cibernetice și a vizibilității acesteia în Uniune;**

(c) **oferă asistență statelor membre în eforturile acestora de a sensibiliza publicul în legătură cu securitatea cibernetică și de a promova educarea în privința securității cibernetice;**

(d) **sprijină coordonarea mai strânsă și schimbul de bune practici în rândul statelor membre în legătură cu sensibilizarea și educarea în materie de securitate cibernetică, facilitând înființarea și menținerea unei rețele de puncte de contact naționale în domeniul educației.**

Articolul 10

[...] ***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

[...] ***Cooperare 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, [...] **în cadrele internaționale de cooperare relevante**, a schimbului de bune practici [...].

(c) furnizarea de expertiză Comisiei, la cererea acesteia**;**

(ca) în colaborare cu Grupul european pentru certificarea de securitate cibernetică instituit în temeiul articolului 53, consilierea și sprijinirea Comisiei în chestiuni referitoare la acorduri de recunoaștere reciprocă a certificatelor de securitate cibernetică cu țări terțe.

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;[...]

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

(da) o rețea a ofițerilor naționali de legătură, care exercită funcțiile prevăzute la articolul 20a.

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;

(ca) supraveghează punerea în aplicare a programării multianuale și anuale cuprinse în documentul unic de programare;

(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) […]

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, **inclusiv punerea în aplicare a programului anual de lucru**, 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;

(la) desfășurarea de schimburi periodice cu instituțiile, agențiile și organele Uniunii în ceea ce privește activitățile lor în materie de securitate cibernetică, pentru a asigura coerența în dezvoltarea și punerea în aplicare a politicilor UE;

(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) **După caz, în scopul îndeplinirii sarcinilor agenției într-un mod eficient și eficace și pe baza unei analize cost-beneficiu adecvate,** directorul executiv **poate** decide [...] **înființarea unuia sau mai multor birouri locale într-unul sau mai multe state membre**. Înainte de a decide să înființeze un birou local, directorul executiv **caută să afle opinia statului membru/statelor membre în cauză, inclusiv a statului membru în care este situat sediul agenției, și** să obțină acordul prealabil al Comisiei **și** al consiliului de administrație[...]. **În cazurile de dezacord în cursul procesului de consultare între directorul executiv și statele membre în cauză, chestiunea este supusă consiliului spre dezbatere.** Decizia respectivă precizează domeniul de aplicare al activităților care urmează să fie efectuate în cadrul biroului local, astfel încât să se evite costurile inutile și dublarea funcțiilor administrative ale agenției. [...] **Numărul personalului din toate birourile locale este menținut la un minim și nu depășește <u>în total</u> 40 % din <u>[...]</u> personalul <u>care se găsește în statul membru în care este situat sediul agenției</u>. Numărul personalului din fiecare birou local nu depășește 10 % din [...] numărul [...] personalului <u>care se găsește în statul membru în care este situat sediul agenției</u>.**

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, **operatorii de servicii esențiale**, 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.

(5a) Grupul permanent al părților interesate informează periodic consiliul de administrație despre activitățile sale.

SECȚIUNEA 4A
REȚEAUA OFIȚERILOR NAȚIONALI DE LEGĂTURĂ

Articolul 20a

Rețeaua ofițerilor naționali de legătură

(1) Consiliul de administrație, acționând la propunerea directorului executiv, instituie o rețea a ofițerilor naționali de legătură, formată din reprezentanți ai statelor membre.

(2) Rețeaua ofițerilor naționali de legătură este formată din reprezentanții tuturor statelor membre. Fiecare stat membru numește un reprezentant. Reuniunile rețelei pot fi ținute în diverse configurații ale experților dintr-un anumit domeniu.

(3) Rețeaua ofițerilor naționali de legătură facilitează cu precădere schimbul de informații între ENISA și statele membre. În special, aceasta sprijină ENISA în diseminarea activităților, constatărilor și recomandărilor sale la nivelul UE, către părțile interesate relevante.

(4) **Ofițerii naționali de legătură acționează ca puncte de convergență și de contact la nivel național pentru a facilita cooperarea între ENISA și experții naționali în contextul punerii în aplicare a programului de lucru al ENISA.**

(5) **Deși ofițerii naționali de legătură ar trebui să coopereze strâns cu reprezentanții țărilor lor respective în cadrul consiliului de administrație, rețeaua însăși nu dublează activitatea consiliului de administrație, și nici a altor foruri ale UE.**

(6) **Funcțiile și procedurile pentru rețeaua ofițerilor naționali de legătură sunt specificate în normele interne de funcționare ale agenției și se fac publice.**

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 [14] 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.

---

14 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).

(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.

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

Transparență

(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

Confidențialitate

(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 [15] și 2015/444 [16] ale Comisiei. Regulamentul intern respectiv include dispoziții privind schimbul, prelucrarea și stocarea informațiilor clasificate.

---

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

[16] 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).

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.

TITLUL 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 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 bugetară

(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

Reglementări 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 (CE, Euratom) 883/2013 al Parlamentului European și al Consiliului [17], combaterea fraudei, a 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.

(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.

[17] 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).

(3) OLAF poate efectua investigații, inclusiv controale și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul nr. 883/2013 al Parlamentului European și al Consiliului și în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului [18] 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.

---

18 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).

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.

(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 **patru** [...] 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 **patru** [...] 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 revocat din funcție doar în urma unei decizii a consiliului de administrație [...].

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 [19]. 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 [20].

(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.

---

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

[20] 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).

Articolul 39

Cooperarea cu țările terțe și cu organizațiile 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.

(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

Norme de securitate privind protecția 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 oferă [...] condiții 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 copiii, 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

Cadrul *european de certificare de securitate cibernetică* [...]

(1) **Cadrul european de certificare de securitate cibernetică este instituit pentru a îmbunătăți condițiile de funcționare a pieței interne prin sporirea nivelului de securitate cibernetică din Uniune. Acesta stabilește o guvernanță care permite o abordare armonizată la nivelul UE a sistemelor europene de certificare de securitate cibernetică, în vederea creării unei piețe unice digitale pentru procese, produse și servicii TIC.**

(2) **Cadrul european de certificare de securitate cibernetică definește un mecanism pentru instituirea** [...] unor sisteme europene de certificare de securitate cibernetică [...] **și pentru** a atesta că **procesele**, produsele și serviciile TIC care au fost [...] **evaluate** în conformitate cu sistem**ele** respective sunt conforme cu cerințele de **securitate** specificate [...], **cu scopul de a proteja** disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise ori prelucrate sau funcțiile ori serviciile oferite de aceste produse, procese [...] **și** servicii sau accesibile prin intermediul lor **pe parcursul întregului lor ciclu de viață**.

Articolul 44

Pregătirea și adoptarea unui sistem european de certificare de securitate cibernetică

(1) În urma unei solicitări din partea Comisiei **sau a Grupului european pentru certificarea de securitate cibernetică („grupul") instituit în temeiul articolului 53**, 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.[...]

(1a) Pregătirea unei propuneri de sistem european de certificare de securitate cibernetică poate fi recomandată grupului de către state membre sau de către organizații ale părților interesate. Grupul evaluează propunerile respective pe baza unor criterii stabilite de grup prin intermediul unor orientări în conformitate cu articolul 53 alineatul (3) litera (ca) și poate solicita ENISA să pregătească o propunere 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 **prin intermediul unor procese de consultare transparente** și cooperează îndeaproape cu grupul. Grupul furnizează pentru ENISA asistență și consiliere [...] în ceea ce privește pregătirea propunerii de sistem **și adoptă un aviz privind propunerea de sistem înainte ca aceasta să fie prezentată Comisiei**[...]. **ENISA se asigură că propunerile de sistem sunt coerente cu standardul armonizat aplicabil utilizat pentru acreditarea organismului de evaluare a conformității.**

(3) ENISA **ține seama în cea mai mare măsură posibilă de avizul grupului înainte de a transmite** Comisiei [...] propunerea de sistem [...] 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 (2), care să prevadă sisteme europene de certificare de securitate cibernetică pentru **procesele**, produsele și serviciile TIC, care îndeplinesc cerințele prevăzute la articolele 45, 46 și 47 din prezentul regulament.

(5) […]

Articolul 44a

Întreținerea sistemelor europene de certificare de securitate cibernetică

(1) Agenția întreține un site web dedicat care oferă informații și face publicitate cu privire la sistemele europene de certificare de securitate cibernetică, certificatele și declarațiile de conformitate UE eliberate în conformitate cu articolul 47a.

(2) Agenția, în strânsă cooperare cu grupul, revizuiește cel puțin o dată la cinci ani sistemele europene de certificare de securitate cibernetică, ținând seama de observațiile primite de la părțile interesate. Dacă se consideră necesar, Comisia sau grupul pot solicita agenției să demareze procesul de elaborare a unei propuneri revizuite de sistem în conformitate cu articolul 44 alineatele (2) și (3).

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 [...] **atingă**, după caz, **cel puțin** 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 **pe întregul ciclu de viață al procesului, produsului sau serviciului**;

(b)

să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva distrugerii accidentale sau neautorizate, [...] pierderii sau modificării, ori lipsei de disponibilitate **pe întregul ciclu de viață al procesului, produsului sau serviciului**;

(c) [...] 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 [...] **accesate, utilizate sau procesate în alt mod**, în ce moment și de către cine;

(e) [...] este posibil să se verifice care sunt datele, serviciile sau funcțiile care au fost accesate, [...] utilizate **sau procesate în alt mod**, 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) [...] **procesele**, produsele și serviciile TIC sunt furnizate cu software **și hardware** actualizate care [...] nu conțin vulnerabilități cunoscute **public** și sunt prevăzute mecanisme pentru actualizări securizate ale [...] acestora**;**

(ga) procesele, produsele și serviciile TIC sunt dezvoltate, fabricate și furnizate în conformitate cu cerințele de securitate menționate în sistemul respectiv.

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 **procesele**, produsele și serviciile TIC [...]. **Astfel, nivelul de asigurare este proporțional cu nivelul riscului asociat cu utilizarea preconizată a unui proces, produs sau serviciu TIC.**

(2) Nivelurile de asigurare de bază, substanțial și/sau ridicat [...] **se referă la un certificat sau o declarație de conformitate UE eliberată în contextul unui sistem european de certificare de securitate care oferă pentru fiecare nivel de asigurare cerințe de securitate respective, inclusiv funcții de securitate și nivelul corespunzător de efort pentru evaluarea unui proces, produs sau serviciu TIC. Certificatul sau declarația de conformitate UE se caracterizează prin trimiteri la specificații tehnice, standarde și proceduri conexe acestora, inclusiv controale tehnice, al căror scop este de a diminua riscul de incidente de securitate cibernetică sau de a le preveni, după cum urmează:**

(a) **un certificat european de securitate cibernetică sau o declarație de conformitate UE care face trimitere la** nivelul de asigurare **„**de bază**" oferă asigurare cu privire la faptul că procesele, produsele și serviciile TIC îndeplinesc cerințele de securitate respective, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care permite minimizarea riscurilor de bază cunoscute în ceea ce privește incidentele cibernetice. Activitățile de evaluare includ cel puțin o examinare a documentației tehnice sau, în cazurile în care nu este aplicabilă, acestea includ activități substituitoare cu efect echivalent** [...]:

(b) **un certificat european de securitate cibernetică care face trimitere la** nivelul de asigurare **„**substanțial**” oferă asigurare cu privire la faptul că procesele, produsele și serviciile TIC îndeplinesc cerințele de securitate respective, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care permite minimizarea riscurilor, incidentelor și atacurilor cibernetice cunoscute, efectuate de actori cu competențe și resurse limitate. Activitățile de evaluare includ cel puțin: examinarea lipsei de aplicabilitate a vulnerabilităților cunoscute public și testarea faptului că procesele, produsele sau serviciile TIC implementează corect funcțiile de securitate necesare; în cazurile în care nu sunt aplicabile, acestea includ activități substituitoare cu efect echivalent.**[...];

(c) **un certificat european de securitate cibernetică care face trimitere la** nivelul de asigurare **„**ridicat**” oferă asigurare cu privire la faptul că procesele, produsele și serviciile TIC îndeplinesc cerințele de securitate respective, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care permite minimizarea riscurilor de atacuri cibernetice de ultimă generație, efectuate de actori cu competențe și resurse substanțiale. Activitățile de evaluare includ cel puțin: examinarea lipsei de aplicabilitate a vulnerabilităților cunoscute public, testarea faptului că procesele, produsele sau serviciile TIC implementează corect funcțiile de securitate necesare, la nivel de ultimă generație, și evaluarea rezistenței acestora la atacatori competenți prin teste de rezistență la intruziuni; în cazurile în care nu sunt aplicabile, acestea includ activități substituitoare cu efect echivalent.**[...].

(2a) Un sistem european de certificare de securitate cibernetică poate specifica mai multe niveluri de evaluare în funcție de rigoarea și profunzimea metodologiei de evaluare. Fiecare dintre nivelurile de evaluare corespunde unuia dintre nivelurile de asigurare și este definit printr-o combinație corespunzătoare de componente ale asigurării.

Articolul 47

Elementele sistemelor europene de certificare de securitate cibernetică

(1) Un sistem european de certificare de securitate cibernetică include **cel puțin** următoarele elemente:

(a) obiectul și domeniul de aplicare al **sistemului de** certificare, inclusiv tipul sau categoriile de **procese**, produse și servicii TIC acoperite, **precum și elaborarea modului în care sistemul de certificare corespunde nevoilor grupurilor-țintă preconizate**;

(b) [...] trimitere la [...] standardele internaționale, **europene sau naționale urmate în cadrul evaluării. În cazul în care standardele nu sunt disponibile, se face trimitere la** [...] specificațiile tehnice **care îndeplinesc cerințele din anexa II la Regulamentul 1025/2012 sau, dacă acestea nu sunt disponibile, la specificații tehnice sau la alte cerințe de securitate cibernetică definite în sistem**;

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

(ca) după caz, cerințe specifice sau suplimentare aplicabile organismelor de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică;

(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) **după caz,** informațiile necesare pentru certificare ce trebuie furnizate **sau puse în alt mod la dispoziția** 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) [...] normele pentru monitorizarea conformității cu cerințele certificatelor **sau ale declarațiilor de conformitate UE**, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate;

(h) **după caz**, condițiile de acordare **și de reînnoire a unui certificat**, **precum și de** menținere, continuare, extindere **sau** restrângere a domeniului de aplicare al certificării;

(i) normele privind consecințele neconformității cu cerințele [...] **sistemului** a produselor și serviciilor TIC certificate **sau autoevaluate**;

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

(k) **după caz,** normele privind păstrarea evidențelor de către organismele de evaluare a conformității;

(l) identificarea sistemelor naționale **sau internaționale** de certificare de securitate cibernetică care acoperă aceleași tipuri sau categorii de **procese,** produse și servicii TIC, **cerințele de securitate și criteriile și metodele de evaluare;**

(m) conținutul certificatului eliberat **sau al declarației de conformitate UE eliberate;**

(ma) perioada de stocare a declarației de conformitate UE și documentația tehnică conținând toate informațiile relevante prevăzute de producătorul sau de furnizorul produselor și serviciilor TIC;

(mb[...]) perioada de valabilitate maximă a certificatelor;

(mc[...]) politica de divulgare pentru certificatele acordate, modificate sau retrase;

(md[...]) condițiile pentru recunoașterea reciprocă a sistemelor de certificare cu țări terțe;

(me[...]) după caz, normele privind un mecanism de evaluare inter pares pentru organismele care eliberează certificate europene de securitate cibernetică pentru nivelul de asigurare ridicat [...] în temeiul articolului 48 alineatul (4a).

(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 **sau declarația de conformitate UE** 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 47a

Autoevaluarea conformității

(1) Un sistem european de certificare de securitate cibernetică poate permite efectuarea unei evaluări de conformitate pe răspunderea exclusivă a fabricantului sau a furnizorului de produse și servicii TIC. O astfel de evaluare a conformității se aplică numai produselor și serviciilor TIC prezentând un risc redus, corespunzând nivelului de asigurare de bază.

(2) Fabricantul sau furnizorul de produse și servicii TIC poate elibera o declarație de conformitate UE care menționează că s-a demonstrat îndeplinirea cerințelor stabilite în sistem. Prin redactarea unei astfel de declarații, producătorul sau furnizorul de produse și servicii TIC își asumă responsabilitatea pentru conformitatea produsului sau serviciului TIC cu cerințele stabilite în sistem.

(3) Fabricantul sau furnizorul de produse și servicii TIC păstrează la dispoziția autorității naționale de certificare de securitate cibernetică menționată la articolul 50 alineatul (1), pe durata stabilită în sistemul european de certificare de securitate cibernetică corespunzător, declarația de conformitate UE și documentația tehnică conținând toate informațiile relevante legate de conformitatea produselor sau serviciilor TIC cu un sistem. Se transmite o copie a declarației de conformitate UE către autoritatea națională de certificare de securitate cibernetică și către ENISA.

(4) Eliberarea unei declarații de conformitate UE este voluntară, cu excepția cazului în care se prevede altfel în legislația Uniunii sau în cea a statelor membre.

(5) Declarația de conformitate UE eliberată în temeiul prezentului articol este recunoscută în toate statele membre.

Articolul 48

Certificarea de securitate cibernetică

(1) **Procesele,** 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 **sau în cea a statelor membre**.

(3) Organismele de evaluare a conformității menționate la articolul 51 emit un certificat european de securitate cibernetică în temeiul prezentului articol**, care face trimitere la nivelul de bază sau substanțial,** 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 **certificare 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 [...] este una din următoarele entități:

(a) o autoritate națională de [...] certificare **de securitate cibernetică** menționată la articolul 50 alineatul (1);

(b) un organism **public** care este acreditat ca organism de evaluare a conformității în temeiul articolului 51 alineatul (1) [...]

(c) [...].

(4a) În cazurile în care un sistem european de certificare de securitate cibernetică în temeiul articolului 44 impune un nivel de asigurare ridicat, certificatul poate fi eliberat numai de o autoritate națională de certificare de securitate cibernetică menționată la articolul 50 alineatul (1) sau, în condițiile următoare, de un organism de evaluare a conformității menționat la articolul 51;

(a) cu aprobarea prealabilă din partea unei autorități de certificare de securitate cibernetică pentru fiecare certificat individual eliberat de un organism de evaluare a conformității; sau

(b) cu delegarea generală prealabilă a acestei sarcini către organismul de evaluare a conformității de către autoritatea națională de certificare de securitate cibernetică.

(5) Persoana fizică sau juridică ale cărei **procese,** produse sau servicii TIC sunt supuse mecanismului de certificare [...] **pune la dispoziția** organismului de evaluare a conformității menționat la articolul 51 **sau la dispoziția autorității naționale de certificare de securitate cibernetică menționată la articolul 50**, **în cazul în care această autoritate este organismul care eliberează certificatul,** [...] toate informațiile necesare pentru desfășurarea procedurii de certificare.

(5a) Deținătorul unui certificat informează organismul care a eliberat certificatul despre orice vulnerabilități sau nereguli detectate ulterior, legate de securitatea procesului, produsului sau serviciului TIC certificat, care pot avea un impact asupra cerințelor legate de certificare. Organismul transmite aceste informații fără întârzieri nejustificate autorității naționale de certificare de securitate cibernetică.

(6) Certificatele se eliberează pentru [...] **durata stabilită de sistemul de certificare în cauză** și pot fi reînnoite [...] numai dacă sunt îndeplinite în continuare cerințele relevante.

(7) Un certificat european de securitate cibernetică eliberat 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 **procesele,** 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 de certificare de securitate cibernetică și procedurile aferente pentru **procesele,** 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 **procesele,** produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate cibernetică în vigoare.

(3) Certificatele existente eliberate în temeiul sistemelor naționale de certificare de securitate cibernetică **și acoperite de un sistem european de certificare de securitate cibernetică** rămân valabile până la data expirării lor.

Articolul 50

Autoritățile naționale de certificare **de securitate cibernetică***[...]*

(1) Fiecare stat membru [...] **desemnează pe teritoriul său una sau mai multe autorități** naționale [...] de certificare **de securitate cibernetică sau, de comun acord cu un alt stat membru, desemnează una sau mai multe autorități stabilite în celălalt stat membru pentru a fi responsabile de atribuțiile de supraveghere în statul membru care face desemnarea.**

(2) Fiecare stat membru informează Comisia cu privire la identitatea autorităților **desemnate [...] și la sarcinile alocate acestora**.

(3) **Fără a aduce atingere articolului 48 alineatul (4) litera (a) și articolului 48 alineatul (4a),** [...] fiecare autoritate națională de [...] certificare **de securitate cibernetică** este independentă în ceea ce privește organizarea, deciziile de finanțare, structura juridică și luarea de decizii, de entitățile pe care le supraveghează.

(3a) Statele membre se asigură că se aderă la o separare strictă a rolurilor și responsabilităților între activitățile autorității naționale de certificare de securitate cibernetică legate de eliberarea de certificate în conformitate cu articolul 48 alineatul (4) litera (a) și cu articolul 48 alineatul (4a) și activitățile de supraveghere de la prezentul articol și că ambele activități funcționează independent una de cealaltă.

(4) Statele membre se asigură că autoritățile naționale de [...] certificare **de securitate cibernetică** 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 [...] certificare **de securitate cibernetică**:

(a) […]

(aa) monitorizează și asigură respectarea obligațiilor prevăzute la articolul 47a alineatele (2) și (3) și în sistemul european de certificare de securitate cibernetică corespunzător, care revin fabricantului sau furnizorului de produse și servicii TIC stabilit pe teritoriile lor respective;

(b) [...] **fără a aduce atingere articolului 51 alineatul (1b), sprijină organismele naționale de acreditare în monitorizarea și supravegherea** activităților organismelor de evaluare a conformității în scopul prezentului regulament [...];

(ba) monitorizează și supraveghează activitățile organismelor menționate la articolul 48 alineatul (4);

(bb) autorizează organismele de evaluare a conformității menționate la articolul 51 alineatul (1b) și restricționează, suspendă sau retrag autorizația existentă în cazurile de neconformitate cu cerințele prezentului regulament;

(c) tratează plângerile depuse de persoane fizice sau juridice în legătură cu certificatele eliberate de [...] **autoritatea națională de certificare de securitate cibernetică sau, în conformitate cu articolul 48 alineatul (4a), de organismele de evaluare a conformității**, 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 [...] certificare **de securitate cibernetică** sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a **proceselor,** 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 [...] certificare **de securitate cibernetică** dispune cel puțin de următoarele competențe:

(a) competența de a cere organismelor de evaluare a conformității**,** [...] deținătorilor de certificate europene de securitate cibernetică **și entităților care eliberează declarația de conformitate UE** 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**,** [...] a titularilor de certificate europene de securitate cibernetică **și a entităților care eliberează declarația de conformitate UE** 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**,** [...] titularii de certificate **și entitățile care eliberează [...] declarația de conformitate UE** 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 **eliberate de autoritatea națională de certificare de securitate cibernetică sau, în conformitate cu articolul 48 alineatul (4a) de organismele de evaluare a conformității** 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 [...] certificare **de securitate cibernetică** 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 **proceselor,** produselor și a serviciilor TIC.

Articolul 51

Organisme 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.

(1a) În cazurile în care un certificat european de securitate cibernetică este eliberat de o autoritate națională de certificare de securitate cibernetică în temeiul articolului 48 alineatul (4) litera (a) și al articolului 48 alineatul (4a), organismul de certificare al autorității naționale de certificare de securitate cibernetică este acreditat ca organism de evaluare a conformității în temeiul alineatului (1) de la prezentul articol.

(1b) După caz, organismele de evaluare a conformității sunt autorizate de autoritatea națională de certificare de securitate cibernetică să își îndeplinească sarcinile atunci când respectă cerințe specifice sau suplimentare prevăzute în sistemul european de certificare în temeiul articolului (47) alineatul (1) litera (ca).

(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 **iau toate măsurile corespunzătoare într-un termen rezonabil pentru a restricționa, a suspenda sau** a revoca 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

Notificare

(1) Pentru fiecare sistem european de certificare de securitate cibernetică adoptat în temeiul articolului 44, autoritățile naționale de [...] certificare **de securitate cibernetică** notifică Comisiei [...] organismele de evaluare a conformității acreditate **și, după caz, autorizate în temeiul articolului 51 alineatul (1b)** să elibereze 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 [...] certificare **de securitate cibernetică** poate înainta Comisiei o cerere de retragere a unui organism de evaluare a conformității notificat de statul membru respectiv 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 certificare de **securitate cibernetică**.

(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 **reprezentanți ai** autorităților naționale de [...] certificare **de securitate cibernetică sau din reprezentanți ai altor autorități naționale competente**. [...] **Niciun membru al grupului nu poate reprezenta mai mult decât un singur alt stat membru**.

(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;

(ba) să adopte un aviz cu privire la propunerea de sistem în temeiul articolului (4) din prezentul regulament;

(c) să [...] **solicite** agenției să pregătească o propunere de sistem european de certificare de securitate cibernetică în conformitate cu articolul 44 din prezentul regulament;

(ca) să elaboreze și să adopte orientări privind criterii de evaluare a propunerilor pentru pregătirea unei propuneri de sistem transmise [...] grupului în temeiul articolului 44 alineatul (1a);

(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 certificare **de securitate cibernetică** desfășurată în temeiul prezentului titlu prin **consolidarea capacităților și 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**;**

(fa) să ofere sprijin pentru punerea în aplicare a mecanismului de evaluare inter pares în conformitate cu normele stabilite în cadrul unui sistem european de certificare de securitate cibernetică în temeiul articolului 47 alineatul (1) litera (md) din prezentul regulament.

(4) Comisia prezidează grupul **în calitatea de moderator** și asigură secretariatul acestuia, cu asistență din partea ENISA, astfel cum se prevede la articolul 8 litera (a).

Articolul 53a

***Dreptul de a depune o plângere la autoritatea [...] națională de certificare* de securitate cibernetică**

(1) Persoanele fizice sau juridice au dreptul de a depune o plângere la autoritatea națională de certificare de securitate cibernetică în legătură cu un certificat eliberat de aceeași autoritate sau, în conformitate cu articolul 48 alineatul (4a), de organisme de evaluare a conformității.

(2) Autoritatea națională de certificare de securitate cibernetică la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul articolului 53b.

Articolul 53b

Dreptul la o cale de atac judiciară eficace

(1) Persoanele fizice sau juridice au dreptul de a exercita o cale de atac judiciară eficace împotriva unei decizii cu caracter a obligatoriu luate, în ceea ce le privește, de o autoritate națională de certificare de securitate cibernetică.

(2) Persoanele fizice sau juridice au dreptul de a exercita o cale de atac judiciară eficace în cazul în care autoritatea națională de certificare de securitate cibernetică nu tratează o plângere.

(3) Acțiunile împotriva unei autorități naționale de certificare de securitate cibernetică se formulează în fața curților statului membru în care este stabilită autoritatea.

Articolul 54

Sancțiuni

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 5 alineatul **(4) litera (b)** 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

Intrarea în vigoare

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

(1a) Prezentul regulament se aplică de la [...] cu excepția articolelor 50, 51, 52, 53a, 53b și 54, care se aplică de la [24 de luni de la data publicării sale 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*

ANEXĂ

CERINȚELE CARE TREBUIE SĂ FIE ÎNDEPLINITE DE ORGANISMELE DE EVALUARE A CONFORMITĂȚII

Organismele de evaluare a conformității care doresc să fie acreditate trebuie să îndeplinească următoarele cerințe:

(1) Un organism de evaluare a conformității trebuie să fie înființat în temeiul legislației naționale și să aibă personalitate juridică.

(2) Un organism de evaluare a conformității trebuie să fie un organism terț independent de organizația sau de produsele ori de serviciile TIC pe care le evaluează.

(3) Un organism care aparține unei asociații de întreprinderi sau unei federații profesionale care reprezintă întreprinderile implicate în proiectarea, fabricarea, furnizarea, asamblarea, utilizarea sau întreținerea produselor sau serviciilor TIC pe care le evaluează poate fi considerat un organism de evaluare a conformității, cu condiția să demonstreze că este independent și că nu există conflicte de interese.

(4) Un organism de evaluare a conformității, personalul de conducere de nivel superior al acestuia și personalul responsabil cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi nici proiectantul, fabricantul, furnizorul, instalatorul, cumpărătorul, proprietarul, utilizatorul sau operatorul de întreținere al produsului sau serviciului TIC care este evaluat și nici reprezentantul autorizat al vreuneia dintre aceste părți. Acest lucru nu împiedică utilizarea produselor evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea acestor produse în scopuri personale.

(5) Un organism de evaluare a conformității, personalul său de conducere și personalul său responsabil cu îndeplinirea sarcinilor de evaluare a conformității nu pot fi direct implicați în proiectarea, fabricarea sau construcția, comercializarea, instalarea, utilizarea sau întreținerea acelor produse sau servicii TIC și nu pot reprezenta părțile angajate în acele activități. Aceștia nu trebuie să se implice în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității pentru care sunt notificați. Aceste dispoziții trebuie să se aplice în special serviciilor de consultanță.

(6) Organismele de evaluare a conformității trebuie să se asigure că activitățile filialelor sau ale subcontractanților lor nu afectează confidențialitatea, obiectivitatea sau imparțialitatea activităților lor de evaluare a conformității.

(7) Organismele de evaluare a conformității și personalul acestora trebuie să îndeplinească activitățile de evaluare a conformității cu cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și nu trebuie să facă obiectul niciunei presiuni și niciunei persuasiuni, inclusiv de natură financiară, care le-ar putea influența deciziile sau rezultatele activităților lor de evaluare a conformității, în special în ceea ce privește persoanele sau grupurile de persoane având interese legate de rezultatele acelor activități.

(8) Un organism de evaluare a conformității competent trebuie să fie capabil să efectueze toate sarcinile de evaluare a conformității care îi sunt atribuite în temeiul prezentului regulament, indiferent dacă sarcinile respective sunt realizate în mod direct de organismul de evaluare a conformității sau în numele său și pe răspunderea sa.

(9) În orice moment și pentru fiecare procedură de evaluare a conformității și fiecare tip, categorie sau subcategorie de produse sau servicii TIC, organismul de evaluare a conformității trebuie să dispună de:

(a) personalul necesar având cunoștințele tehnice necesare și experiența suficientă și corespunzătoare pentru a efectua sarcinile de evaluare a conformității;

(b) descrierile necesare ale procedurilor pe baza cărora se realizează evaluarea conformității, asigurându-se transparența acelor proceduri și posibilitatea de a le reproduce. Acesta trebuie să prevadă politicile și procedurile adecvate care fac distincție între atribuțiile îndeplinite ca organism notificat și alte activități;

(c) procedurile necesare pentru a-și desfășura activitatea ținând seama în mod corespunzător de dimensiunea unei întreprinderi, de sectorul în care își desfășoară activitatea și de structura acesteia, de gradul de complexitate a tehnologiei produsului sau serviciului TIC în cauză, precum și de caracterul de serie sau de masă al procesului de producție.

(10) Un organism de evaluare a conformității trebuie să dispună de mijloacele necesare pentru a îndeplini în mod corespunzător sarcinile tehnice și administrative legate de activitățile de evaluare a conformității și să aibă acces la toate echipamentele sau facilitățile necesare.

(11) Personalul responsabil cu îndeplinirea activităților de evaluare a conformității trebuie să posede următoarele calități

(a) o bună pregătire tehnică și profesională care acoperă toate activitățile de evaluare a conformității;

(b) cunoștințe satisfăcătoare ale cerințelor evaluărilor pe care le realizează și autoritatea corespunzătoare pentru realizarea acestor evaluări;

(c) cunoștințe și o înțelegere corespunzătoare a cerințelor și standardelor de testare aplicabile;

(d) abilitatea necesară pentru a elabora certificate, evidențe și rapoarte care să demonstreze că evaluările au fost realizate.

(12) Trebuie să fie garantată imparțialitatea organismelor de evaluare a conformității, a personalului de conducere de nivel superior și a personalului de evaluare al acestora.

(13) Remunerația personalului de conducere de nivel superior și a personalului de evaluare ale unui organism de evaluare a conformității nu trebuie să depindă de numărul de evaluări realizate sau de rezultatele evaluărilor respective.

(14) Organismele de evaluare a conformității trebuie să încheie o asigurare de răspundere civilă în cazul în care răspunderea nu este asumată de stat în conformitate cu dreptul intern sau statul membru nu este direct responsabil pentru evaluarea conformității.

(15) Personalul organismelor de evaluare a conformității trebuie să păstreze secretul profesional referitor la toate informațiile obținute în îndeplinirea sarcinilor sale în temeiul prezentului regulament sau al oricărei dispoziții din legislația națională de punere în aplicare a acestuia, excepție făcând relația cu autoritățile competente ale statului membru în care își îndeplinește activitățile.

(16) Organismele de evaluare a conformității îndeplinesc cerințele standardului **relevant care este armonizat în temeiul Regulamentului (CE) 765/2008 pentru acreditarea organismelor de evaluare a conformității care efectuează certificarea proceselor, produselor sau serviciilor** [...].

(17) Organismele de evaluare a conformității se asigură că laboratoarele de testare utilizate în scopul evaluării conformității respectă cerințele standardului **relevant care este armonizat în temeiul Regulamentului (CE) 765/2008 pentru acreditarea laboratoarelor care efectuează testări** [...].