Proiect

UE

LEGE

privind certificarea securității cibernetice

Parlamentul adoptă prezenta lege organică.

Prezenta lege pune în aplicare parțial Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), publicat în Jurnalul Oficial al Uniunii Europene L 151 din 7 iunie 2019, CELEX: 32019R0881, așa cum a fost modificat ultima dată prin Regulamentul (UE) 2025/37 al Parlamentului European și al Consiliului din 19 decembrie 2024 de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 2025/37 din 15 ianuarie 2025, CELEX: 32025R0037.

Capitolul I
DISPOZIȚII GENERALE

Articolul 1. Obiect

(1) Prezenta lege stabilește cadrul juridic și instituțional privind certificarea securității cibernetice a produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, inclusiv privind:

a) elaborarea, aprobarea, administrarea și revizuirea sistemelor naționale de certificare a securității cibernetice;

b) desemnarea, atribuțiile și competențele autorității naționale de certificare a securității cibernetice;

c) acreditarea, autorizarea, recunoașterea și supravegherea organismelor de evaluare a conformității;

d) emiterea, menținerea, suspendarea, retragerea și reînnoirea certificatelor de securitate cibernetică, precum și autoevaluarea conformității și declarația de conformitate;

e) recunoașterea certificatelor europene de securitate cibernetică, a declarațiilor de conformitate UE și a rezultatelor evaluării conformității;

f) transparența, supravegherea, răspunderea și căile de atac în domeniul certificării securității cibernetice.

(2) Scopul prezentei legi constă în asigurarea unui nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate puse la dispoziție pe piața Republicii Moldova.

Articolul 2. Domeniul de aplicare

(1) Prezenta lege se aplică certificării securității cibernetice și autoevaluării conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, efectuate în cadrul sistemelor naționale de certificare a securității cibernetice, precum și recunoașterii certificatelor și a declarațiilor de conformitate emise în cadrul sistemelor europene de certificare a securității cibernetice.

(2) Prezenta lege se aplică producătorilor și furnizorilor de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate, indiferent de locul înregistrării acestora, în măsura în care produsele, serviciile sau procesele respective sunt puse la dispoziție pe piața Republicii Moldova ori sunt certificate, la cerere, în cadrul unui sistem național, precum și organismelor de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare.

(3) Prezenta lege nu aduce atingere competențelor autorităților publice în ceea ce privește activitățile aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.

Articolul 3. Noțiuni

În sensul prezentei legi, următoarele noțiuni semnifică:

acreditare - astfel cum este definit la art. 2 din Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității;

administrarea incidentului - procedurile utilizate pentru detectarea, analiza și limitarea unui incident cibernetic și răspunsul la acesta;

amenințare cibernetică - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

autoevaluare a conformității - acțiune desfășurată de un producător sau de un furnizor de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate care evaluează dacă respectivele produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate îndeplinesc cerințele unui sistem de certificare a securității cibernetice specific;

certificat de securitate cibernetică – document emis de un organism relevant prin care se atestă că un anumit produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat a fost evaluat în scopul verificării conformității cu cerințele de securitate specifice prevăzute în cadrul unui sistem de certificare a securității cibernetice;

evaluare a conformității - astfel cum este definit la art. 2 din Legea nr. 235/2011;

furnizor de servicii digitale - persoană juridică care furnizează un serviciu digital;

incident cibernetic - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

nivel de asigurare - temeiul încrederii că un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat întrunește cerințele de securitate ale unui sistem de certificare a securității cibernetice specific și indică nivelul la care a fost evaluat un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, dar care nu măsoară ca atare securitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat în cauză;

organism național de acreditare - astfel cum este definit la art. 2 din Legea nr. 235/2011;

organism de evaluare a conformității - astfel cum este definit la art. 2 din Legea nr. 235/2011;

proces al tehnologiei informației și comunicațiilor (proces TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

produs al tehnologiei informației și comunicațiilor (produs TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

securitate cibernetică - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

serviciu al tehnologiei informației și comunicațiilor (serviciu TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

serviciu de securitate gestionat - serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor cibernetice, testele de rezistență la intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate, în legătură cu asistența tehnică;

sistem european de certificare a securității cibernetice - set cuprinzător de norme, cerințe tehnice, standarde și proceduri, instituite la nivelul Uniunii, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate;

sistem național de certificare a securității cibernetice - set cuprinzător de norme, cerințe tehnice, standarde și proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care intră în domeniul de aplicare al sistemului în cauză;

specificație tehnică - document care stabilește cerințele tehnice pe care trebuie să le îndeplinească un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, ori procedurile de evaluare a conformității referitoare la acestea;

standard - astfel cum este definit la art. 2 din Legea nr. 20/2016 cu privire la standardizarea națională.

Capitolul II
CADRUL INSTITUȚIONAL

Articolul 4. Autoritatea națională de certificare a securității cibernetice

(1) Agenția pentru Securitate Cibernetică (în continuare – Agenția) este desemnată în calitate de autoritate națională de certificare a securității cibernetice.

(2) În exercitarea atribuțiilor prevăzute de prezenta lege, Agenția este independentă, în ceea ce privește organizarea, luarea deciziilor și structura juridică, de entitățile pe care le supraveghează.

(3) Activitățile Agenției aferente emiterii certificatelor de securitate cibernetică, exercitate în condițiile art. 16 alin. (2), sunt strict separate, din punct de vedere organizatoric și funcțional, de activitățile de supraveghere prevăzute de prezenta lege și se desfășoară independent unele de celelalte.

Articolul 5. Atribuțiile autorității naționale de certificare a securității cibernetice

(1) Agenția, în calitate de autoritate națională de certificare a securității cibernetice, exercită următoarele atribuții:

a) supraveghează și asigură respectarea normelor incluse în sistemele naționale de certificare a securității cibernetice, inclusiv a normelor de monitorizare a conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate cu cerințele certificatelor de securitate cibernetică emise pe teritoriul Republicii Moldova, în cooperare cu alte autorități competente de supraveghere a pieței;

b) monitorizează și asigură respectarea obligațiilor producătorilor și furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate stabiliți pe teritoriul Republicii Moldova care efectuează autoevaluarea conformității, inclusiv a obligațiilor prevăzute la art. 18;

c) asistă și sprijină organismul național de acreditare la monitorizarea și supravegherea activităților organismelor de evaluare a conformității în sensul prezentei legi, fără a aduce atingere competențelor acestuia stabilite prin Legea nr. 235/2011;

d) autorizează organismele de evaluare a conformității în condițiile art. 21 și restricționează, suspendă sau retrage autorizația în cazul în care organismele de evaluare a conformității încalcă cerințele prezentei legi sau ale sistemelor naționale de certificare;

e) examinează plângerile persoanelor fizice sau juridice în condițiile art. 29 și informează reclamantul despre stadiul și rezultatul examinării;

f) elaborează, cu consultarea părților interesate, proiectele sistemelor naționale de certificare a securității cibernetice și le propune spre aprobare în condițiile art. 9;

g) ține evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate și asigură caracterul public al acestuia în condițiile art. 26;

h) cooperează cu autoritățile de certificare a securității cibernetice din alte state, cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu alte structuri europene și internaționale relevante, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate cu cerințele aplicabile;

i) monitorizează evoluțiile relevante din domeniul certificării securității cibernetice, inclusiv evoluția sistemului european de certificare a securității cibernetice;

j) elaborează și publică anual pe pagina sa web oficială un raport de sinteză privind activitatea de certificare a securității cibernetice și măsurile întreprinse în temeiul prezentei legi;

k) promovează certificarea securității cibernetice și informează opinia publică, producătorii, furnizorii și utilizatorii cu privire la beneficiile și condițiile acesteia.

(2) Atribuțiile prevăzute la alin. (1) se exercită în conformitate cu procedurile stabilite de prezenta lege, de sistemele naționale de certificare și de actele normative aprobate în vederea executării prezentei legi.

Articolul 6. Competențele autorității naționale de certificare a securității cibernetice

(1) În vederea exercitării atribuțiilor prevăzute la art. 5, Agenția dispune de următoarele competențe:

a) să solicite organismelor de evaluare a conformității, titularilor de certificate de securitate cibernetică și entităților care emit declarații de conformitate să furnizeze toate informațiile necesare pentru îndeplinirea atribuțiilor sale;

b) să efectueze investigații, sub formă de audituri sau controale, asupra organismelor de evaluare a conformității, a titularilor de certificate de securitate cibernetică și a entităților care emit declarații de conformitate, pentru a verifica respectarea prevederilor prezentei legi și ale sistemelor naționale de certificare;

c) să dispună măsuri adecvate, în conformitate cu legislația, pentru a asigura că organismele de evaluare a conformității, titularii de certificate de securitate cibernetică și entitățile care emit declarații de conformitate respectă prezenta lege și sistemele naționale de certificare;

d) să obțină acces, în condițiile legii, la sediile organismelor de evaluare a conformității și ale titularilor de certificate de securitate cibernetică, în scopul desfășurării investigațiilor prevăzute la lit. b);

e) să retragă, în condițiile prezentei legi și ale sistemelelor naționale de certificare, certificatele de securitate cibernetică emise de Agenție sau de organismele de evaluare a conformității, atunci când acestea nu sunt conforme cu prezenta lege sau cu sistemul națională de certificare;

f) să aplice sancțiuni în condițiile art. 38 și să ceară încetarea imediată a încălcărilor obligațiilor prevăzute de prezenta lege.

(2) Controalele asupra activității de întreprinzător se planifică, se efectuează și se înregistrează în condițiile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător.

Articolul 7. Consiliul consultativ pentru certificarea securității cibernetice

(1) Pe lângă Agenție se constituie Consiliul consultativ pentru certificarea securității cibernetice (în continuare – Consiliul consultativ), organ consultativ fără personalitate juridică, format din reprezentanți ai autorităților publice cu competențe în domeniu, ai organismului național de standardizare, ai mediului de afaceri și asociațiilor profesionale din domeniul tehnologiei informației și comunicațiilor, ai mediului academic și ai societății civile.

(2) Consiliul consultativ exercită următoarele funcții:

a) avizează consultativ proiectele sistemelor naționale de certificare a securității cibernetice;

b) formulează recomandări privind prioritizarea domeniilor pentru care se elaborează sisteme naționale de certificare, ținând cont de nivelul riscurilor și de cererea de pe piață;

c) contribuie la corelarea sistemelor naționale cu standardele europene și internaționale și cu sistemele europene de certificare a securității cibernetice;

d) examinează alte chestiuni relevante pentru dezvoltarea cadrului național de certificare a securității cibernetice.

(3) Activitatea membrilor Consiliului consultativ nu este remunerată.

(4) Regulamentul de organizare și funcționare și componența nominală ale Consiliului consultativ se aprobă prin ordin al directorului Agenției, cu asigurarea reprezentativității echilibrate a părților interesate.

Articolul 8. Cooperarea instituțională

(1) Agenția și organismul național de acreditare cooperează în vederea asigurării funcționării coerente a cadrului național de certificare a securității cibernetice, inclusiv prin informare reciprocă privind acreditarea, autorizarea, suspendarea sau retragerea acreditării ori a autorizației organismelor de evaluare a conformității.

(2) În cazul în care constată că un organism de evaluare a conformității nu mai îndeplinește condițiile prevăzute de prezenta lege sau de sistemul națională de certificare, Agenția informează organismul național de acreditare, care examinează informațiile și decide asupra măsurilor necesare în condițiile Legii nr. 235/2011.

(3) În cazul sistemelor de certificare care implică prelucrarea datelor cu caracter personal, Agenția cooperează cu Centrul Național pentru Protecția Datelor cu Caracter Personal.

(4) Agenția poate încheia, în condițiile legii, acorduri de cooperare cu autoritățile naționale de certificare a securității cibernetice din alte state, precum și acorduri de lucru cu ENISA și cu alte structuri europene și internaționale relevante, inclusiv în vederea schimbului de informații, de experiență și de bune practici.

Capitolul III
SISTEMELE NAȚIONALE DE CERTIFICARE A SECURITĂȚII CIBERNETICE

Articolul 9. Elaborarea și aprobarea sistemelor naționale de certificare

(1) Sistemele naționale de certificare a securității cibernetice se elaborează de Agenție, cu consultarea Consiliului consultativ și a altor părți interesate, și se aprobă de Guvern.

(2) Prioritizarea elaborării sistemelor naționale de certificare se realizează în baza analizei riscurilor de securitate cibernetică, a cererii de certificare de pe piața națională și a evoluției sistemelor europene de certificare a securității cibernetice.

(3) La elaborarea sistemelor naționale de certificare se urmărește asigurarea compatibilității cu sistemele europene de certificare, inclusiv prin utilizarea acelorași niveluri de asigurare, criterii și metode de evaluare, precum și a standardelor europene și internaționale relevante.

(4) Proiectele sistemelor naționale de certificare se supun consultărilor publice în condițiile Legii nr. 239/2008 privind transparența în procesul decizional.

(5) Sistemele naționale de certificare se evaluează și, după caz, se revizuiesc de către Agenție cel puțin o dată la 5 ani, ținându-se cont de evoluția amenințărilor cibernetice, a standardelor aplicabile și a sistemelor europene de certificare.

Articolul 10. Obiectivele de securitate ale sistemelor naționale de certificare pentru produsele TIC, serviciile TIC și procesele TIC

Un sistem național de certificare a securității cibernetice pentru produsele TIC, serviciile TIC sau procesele TIC este conceput pentru a îndeplini, 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 produsului TIC, serviciului TIC sau procesului TIC;

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

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

d) să identifice și să documenteze dependențele și vulnerabilitățile cunoscute;

e) să înregistreze 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 facă 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;

g) să verifice că produsele TIC, serviciile TIC și procesele TIC nu conțin vulnerabilități cunoscute;

h) să restabilească disponibilitatea datelor, serviciilor și funcțiilor și accesul la acestea în timp util în cazul unui incident fizic sau tehnic;

i) să asigure că produsele TIC, serviciile TIC și procesele TIC sunt securizate implicit și începând cu momentul conceperii;

j) să asigure că produsele TIC, serviciile TIC și procesele TC sunt furnizate cu software și hardware actualizate care nu conțin vulnerabilități cunoscute public și că sunt prevăzute cu mecanisme pentru actualizări securizate.

Articolul 11. Obiectivele de securitate ale sistemelor naționale de certificare pentru serviciile de securitate gestionate

Un sistem național de certificare a securității cibernetice pentru serviciile de securitate gestionate este conceput pentru a îndeplini, după caz, cel puțin următoarele obiective de securitate:

a) că serviciile de securitate gestionate sunt furnizate de personal care are competența, expertiza și experiența necesare, inclusiv un nivel suficient și adecvat de cunoștințe tehnice și competențe în domeniul specific, experiență suficientă și adecvată și cel mai înalt grad de integritate profesională;

b) că furnizorul dispune de proceduri interne adecvate pentru a se asigura că serviciile de securitate gestionate sunt furnizate la un nivel suficient și adecvat de calitate în orice moment;

c) că datele accesate, stocate, transmise sau prelucrate în alt mod în legătură cu furnizarea de servicii de securitate gestionate sunt protejate împotriva accesului accidental sau neautorizat, a stocării, a divulgării, a distrugerii, a altor prelucrări, a pierderii, a modificării sau a lipsei disponibilității;

d) că disponibilitatea datelor, a serviciilor și a funcțiilor și accesul la acestea sunt restabilite în timp util în cazul unui incident fizic sau tehnic;

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

f) că se ține o evidență care este disponibilă pentru a se stabili care sunt datele, serviciile sau funcțiile care au fost accesate, utilizate sau procesate în alt mod, precum și în ce moment și de către cine au fost accesate, utilizate sau procesate acestea;

g) că produsele TIC, serviciile TIC și procesele TIC utilizate pentru furnizarea serviciilor de securitate gestionate sunt securizate începând cu momentul conceperii

și în mod implicit și, după caz, includ cele mai recente actualizări de securitate și nu conțin vulnerabilități cunoscute public.

Articolul 12. Elemente ale sistemelor naționale de certificare a securității cibernetice

(1) Un sistem național de certificare a securității cibernetice include cel puțin următoarele elemente:

a) obiectul și sfera de aplicare a sistemului de certificare, inclusiv tipul sau categoriile de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate acoperite;

b) o descriere clară a scopului sistemului și a modului în care standardele selectate, metodele de evaluare și nivelurile de asigurare corespund nevoilor utilizatorilor preconizați ai sistemului;

c) trimiteri la standardele internaționale, europene sau naționale aplicate în cadrul evaluării sau, în cazul în care astfel de standarde nu sunt disponibile sau nu sunt adecvate, la specificații tehnice sau la alte cerințe de securitate cibernetică definite în sistemul european de certificare a securității cibernetice;

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

e) o precizare care indică dacă autoevaluarea conformității este permisă în cadrul sistemului;

f) după caz, cerințe specifice sau suplimentare cărora se supun organismele de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică;

g) criteriile și metodele specifice de evaluare, inclusiv tipurile de evaluări, utilizate pentru a demonstra că sunt îndeplinite obiectivele de securitate aplicabile menționate la art. 10 și 11;

h) după caz, informațiile necesare pentru certificare care trebuie furnizate sau puse în alt mod la dispoziția organismelor de evaluare a conformității de către solicitant;

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

j) normele pentru monitorizarea conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate cu cerințele certificatelor naționale de securitate cibernetică sau ale declarațiilor de conformitate, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate;

k) după caz, condițiile de eliberare, de menținere, de continuare și de reînnoire a certificatelor europene de securitate cibernetică, precum și condițiile de extindere sau de restrângere a domeniului de aplicare a certificării;

l) normele privind consecințele neconformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care au fost certificate

sau pentru care a fost eliberată o declarație de conformitate, dar care nu sunt conforme cu cerințele sistemului;

m) normele privind modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale produselor TIC, serviciilor TIC și proceselor TIC;

n) după caz, normele privind păstrarea evidențelor de către organismele de evaluare a conformității;

o) identificarea sistemelor naționale sau internaționale de certificare a securității cibernetice care se referă la aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare;

p) conținutul și formatul certificatelor europene de securitate cibernetică și ale declarațiilor de conformitate care urmează să fie eliberate;

q) perioada de valabilitate a declarației de conformitate, documentația tehnică și toate celelalte informații relevante care sunt puse la dispoziție de producătorul sau de furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate;

r) perioada maximă de valabilitate a certificatelor naționale de securitate cibernetică eliberate în temeiul sistemului;

s) politica de divulgare pentru certificatele naționale de securitate cibernetică eliberate modificate sau retrase în temeiul sistemului;

t) condițiile pentru recunoașterea reciprocă a sistemelor de certificare cu țări terțe;

u) formatul și procedurile care trebuie urmate de producători sau de furnizori de produse TIC, de servicii TIC sau de procese TIC atunci când furnizează și actualizează informațiile suplimentare privind securitatea cibernetică.

(2) Cerințele specificate ale sistemului național de certificare sunt în concordanță cu cerințele legale aplicabile.

Articolul 13. Nivelurile de asigurare

(1) Un sistem național de certificare a securității cibernetice poate stabili unul sau mai multe dintre următoarele niveluri de asigurare pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate: „de bază”, „substanțial” sau „ridicat”. Nivelul de asigurare este corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat, înțeles ca probabilitate și impact al unui incident cibernetic.

(2) Certificatele naționale de securitate cibernetică și declarațiile de conformitate fac trimitere la orice nivel de asigurare prevăzut în sistemul național de certificare a securității cibernetice în temeiul căruia a fost emis certificatul național de securitate cibernetică sau declarația de conformitate.

(3) Cerințele de securitate corespunzătoare fiecărui nivel de asigurare sunt prevăzute de sistemul național de certificare a securității cibernetice relevant, inclusiv funcțiile de securitate corespunzătoare și rigoarea și profunzimea corespunzătoare ale evaluării asupra produsului TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat.

(4) Certificatul sau declarația de conformitate face trimitere la specificații tehnice, standarde și proceduri conexe acestora, inclusiv controale tehnice, al căror scop este de a diminua riscul de incidente cibernetice sau de a le preîntâmpina.

(5) Un certificat național de securitate cibernetică sau o declarație de conformitate care face trimitere la nivelul de asigurare „de bază” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv sau declarația de conformitate respectivă îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și de atacuri cibernetice. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin o examinare a documentației tehnice. În cazurile în care o astfel de examinare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(6) Un certificat național de securitate cibernetică care face trimitere la nivelul de asigurare „substanțial” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor pentru securitatea cibernetică cunoscute și a riscului de incidente și de atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.

(7) Un certificat național de securitate cibernetică care face trimitere la nivelul de asigurare „ridicat” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public; testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare, la nivel de ultimă generație;

și o evaluare a rezistenței acestora la atacatori competenți prin teste de rezistență la intruziuni. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități înlocuitoare cu efect echivalent.

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

Articolul 14. Corelarea sistemelor naționale cu sistemele europene de certificare

(1) Nu se elaborează și nu se aprobă sisteme naționale de certificare pentru tipurile sau categoriile de produse TIC, servicii TIC, procese TIC ori servicii de securitate gestionate acoperite de un sistem european de certificare a securității cibernetice ale cărei certificate sunt recunoscute în Republica Moldova în condițiile art. 24, cu excepția cazurilor justificate de motive de interes public.

(2) Fiecare sistem național de certificare include clauze de tranziție aplicabile în cazul recunoașterii în Republica Moldova a unui sistem european de certificare care acoperă aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC ori servicii de securitate gestionate, inclusiv privind încetarea, în tot sau în parte, a efectelor sistemului național.

(3) În cazul încetării efectelor unui sistem național de certificare în condițiile alin. (2), certificatele de securitate cibernetică emise anterior în cadrul acesteia rămân valabile până la data expirării lor, fără posibilitatea reînnoirii pentru domeniile acoperite de sistemul european recunoscut.

Capitolul IV
CERTIFICAREA ȘI AUTOEVALUAREA CONFORMITĂȚII

Articolul 15. Certificarea securității cibernetice

(1) Produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care au fost certificate în cadrul unui sistem național de certificare a securității cibernetice sunt considerate a fi conforme cu cerințele acestui sistem.

(2) Certificarea securității cibernetice este voluntară, cu excepția cazurilor în care legislația Republicii Moldova prevede altfel.

(3) Agenția evaluează periodic eficiența și utilizarea sistemelor naționale de certificare a securității cibernetice aprobate și analizează dacă un anumit sistem național de certificare a securității cibernetice trebuie să devină obligatoriu, pentru a se asigura un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate în Republica Moldova și pentru a se îmbunătăți funcționarea pieței interne.

(4) Atunci când pregătește evaluarea, Agenția:

a) ia în considerare impactul măsurilor asupra producătorilor sau furnizorilor de astfel de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, precum și asupra utilizatorilor în ceea ce privește costul măsurilor respective, avantajele societale sau economice care decurg din nivelul sporit de securitate preconizat pentru produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate vizate;

b) ține seama de existența și de punerea în aplicare a sistemelor europene de certificare a securității cibernetice;

c) desfășoară un proces de consultare deschis, transparent și cuprinzător cu toate părțile interesate relevante;

d) ia în considerare termenele de punere în aplicare, precum și măsurile și perioadele de tranziție, în special în ceea ce privește impactul posibil al măsurilor asupra producătorilor sau a furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, inclusiv asupra intereselor și nevoilor specifice ale IMM-urilor, inclusiv ale microîntreprinderilor;

e) propune cea mai rapidă și mai eficace modalitate de punere în aplicare a tranziției de la un sistem de certificare voluntar la unul obligatoriu.

(5) Persoana fizică sau juridică care își supune certificării produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pune la dispoziția Agenției, în cazul în care aceasta este organismul care eliberează certificatul național de securitate cibernetică, sau la dispoziția organismului de evaluare a conformității toate informațiile necesare pentru desfășurarea certificării.

Articolul 16. Emiterea certificatelor de securitate cibernetică

(1) Certificatele de securitate cibernetică care fac trimitere la nivelul de asigurare „de bază” sau „substanțial” se emit de organismele de evaluare a conformității acreditate și, după caz, autorizate în condițiile prezentei legi, pe baza criteriilor incluse în sistemul național de certificare.

(2) Certificatele de securitate cibernetică care fac trimitere la nivelul de asigurare „ridicat” se emit de Agenție sau, în cazurile prevăzute de sistemul național de certificare, de un organism de evaluare a conformității, cu condiția aprobării prealabile a fiecărui certificat de către Agenție ori a delegării generale prealabile a acestei atribuții de către Agenție organismului de evaluare a conformității respectiv.

(3) În cazul în care Agenția emite certificate de securitate cibernetică în condițiile alin. (2), subdiviziunea de certificare a Agenției se acreditează ca organism de evaluare a conformității în condițiile art. 20.

(4) Certificatul de securitate cibernetică se emite în baza criteriilor și a procedurilor stabilite de sistemul național de certificare și a raportului de evaluare a conformității, pentru perioada de valabilitate prevăzută de sistem, cu posibilitatea reînnoirii în condițiile acesteia.

Articolul 17. Menținerea, suspendarea și retragerea certificatelor

(1) Titularul certificatului de securitate cibernetică informează organismul emitent sau, după caz, Agenția cu privire la toate vulnerabilitățile sau neregulile detectate ulterior emiterii certificatului, care privesc securitatea produsului TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat certificat, precum și cu privire la orice modificare care poate afecta conformitatea cu cerințele de certificare.

(2) Organismul emitent sau, după caz, Agenția suspendă certificatul de securitate cibernetică în cazul în care constată că produsul TIC, serviciul TIC, procesul TIC sau serviciul de securitate gestionat certificat nu mai îndeplinește temporar cerințele sistemului de certificare, acordând titularului un termen pentru remedierea neconformităților.

(3) Certificatul de securitate cibernetică se retrage în cazul în care:

a) neconformitățile nu au fost remediate în termenul acordat;

b) certificatul a fost obținut în baza unor informații false sau incomplete;

c) titularul împiedică desfășurarea activităților de monitorizare a conformității;

d) în alte cazuri prevăzute de sistemul național de certificare.

(4) Suspendarea și retragerea certificatelor se aduc la cunoștința publicului în condițiile politicii de divulgare prevăzute de sistemul național de certificare.

Articolul 18. Autoevaluarea conformității și declarația de conformitate

(1) Un sistem național de certificare a securității cibernetice poate permite efectuarea unei autoevaluări a conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate. O astfel de autoevaluare a conformității este permisă numai în cazul produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care prezintă un risc redus corespunzând nivelului de asigurare „de bază”.

(2) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate poate elibera o declarație de conformitate care menționează că s-a demonstrat îndeplinirea cerințelor prevăzute în sistem. Prin eliberarea unei astfel de declarații, producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat cu cerințele stabilite în sistemul respectiv.

(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate pune la dispoziția Agenției, pe durata stabilită în sistemul național de certificare a securității cibernetice corespunzător, declarația de conformitate, documentația tehnică și toate celelalte informații relevante legate de conformitatea cu sistemul a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate.

(4) Emiterea declarației de conformitate este voluntară, cu excepția cazului în care prin lege se prevede altfel.

Articolul 19. Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate

(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC certificate sau de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate pune la dispoziția publicului următoarele informații suplimentare privind securitatea cibernetică:

a) orientări și recomandări care să le servească utilizatorilor finali la configurarea, instalarea, derularea, funcționarea și întreținerea securizate a produselor TIC sau serviciilor TIC;

b) perioada în timpul căreia se oferă asistență în materie de securitate utilizatorilor finali, mai ales în ceea ce privește disponibilitatea actualizărilor legate de securitatea cibernetică;

c) informații de contact ale producătorului sau furnizorului și metode acceptate pentru primirea informațiilor despre vulnerabilitate de la utilizatorii finali și de la cercetători din domeniul securității;

d) o trimitere la registrele online care conțin vulnerabilitățile divulgate public legate de produsul TIC, de serviciul TIC sau de procesul TIC și orice avertismente relevante în materie de securitate cibernetică.

(2) Informațiile menționate la alin. (1) se pun la dispoziție în format electronic și rămân disponibile și se actualizează după cum este necesar cel puțin până la expirarea certificatului național de securitate cibernetică sau a declarației de conformitate aferente.

Capitolul V
ORGANISMELE DE EVALUARE A CONFORMITĂȚII

Articolul 20. Acreditarea organismelor de evaluare a conformității

(1) Organismele de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare a securității cibernetice se acreditează de organismul național de acreditare în conformitate cu Legea nr. 235/2011. Acreditarea se acordă numai organismelor de evaluare a conformității care îndeplinirea cerințelor prevăzute la art. 22.

(2) Acreditarea se acordă pentru o perioadă de 4 ani, cu efectuarea supravegherii periodice pe durata ciclului de acreditare, și poate fi reînnoită în condițiile prevăzute de Legea nr. 235/2011, dacă organismul de evaluare a conformității continuă să îndeplinească cerințele de acreditare.

(3) Organismul național de acreditare ia toate măsurile corespunzătoare, pentru a restrânge, a suspenda sau a retrage acreditarea unui organism de evaluare a conformității în cazul în care condițiile de acreditare nu sunt sau nu mai sunt

îndeplinite ori în cazul în care organismul de evaluare a conformității încalcă prezenta lege.

(4) Organismul național de acreditare informează Agenția, în termen de 3 zile lucrătoare, cu privire la acordarea, restrângerea, suspendarea, retragerea sau reînnoirea acreditării organismelor de evaluare a conformității în domeniul securității cibernetice.

Articolul 21. Autorizarea organismelor de evaluare a conformității

(1) În cazul în care un sistem național de certificare stabilește cerințe specifice sau suplimentare în condițiile art. 12 alin. (1) lit. f), numai organismele de evaluare a conformității care îndeplinesc aceste cerințe sunt autorizate de Agenție pentru îndeplinirea atribuțiilor în temeiul sistemului respectiv.

(2) Procedura de autorizare, documentele necesare, termenele de examinare, precum și temeiurile de restricționare, suspendare și retragere a autorizației se stabilesc prin regulament aprobat de Guvern, cu respectarea principiilor transparenței, imparțialității și proporționalității.

(3) Agenția ține evidența organismelor de evaluare a conformității acreditate, autorizate și recunoscute și o publică pe pagina sa web oficială.

Articolul 22. Cerințe care trebuie îndeplinite de organismele de evaluare a conformității

Organismele de evaluare a conformității care doresc să fie acreditate îndeplinesc 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 care este independent de organizația sau de produsele TIC, de serviciile TIC, de procesele TIC sau de serviciile de securitate gestionate pe care le evaluează.

3) Un organism care aparține unei asociații de întreprinderi sau unei federații profesionale care reprezintă întreprinderile implicate în conceperea, producerea, furnizarea, asamblarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate 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) Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi proiectantul, producătorul, furnizorul, instalatorul, cumpărătorul, proprietarul, utilizatorul sau operatorul de întreținere al produsului TIC, al serviciului TIC, al procesului TIC sau al serviciului de securitate gestionat care este evaluat ori reprezentantul autorizat al vreuneia dintre aceste părți. Această interdicție nu împiedică utilizarea produselor TIC evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea acestor produse TIC în scopuri personale.

5) Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi direct implicate în conceperea, producerea sau construcția, furnizarea, comercializarea, instalarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care sunt evaluate și nu pot reprezenta părțile angajate în acele activități. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu se implică în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității. Această interdicție se aplică în special serviciilor de consultanță.

6) Dacă un organism de evaluare a conformității este deținut sau gestionat de o autoritate sau de o instituție publică, se asigură și se documentează independența și absența oricărui conflict de interese între Agenție, pe de o parte, și organismul de evaluare a conformității, pe de altă parte.

7) Organismele de evaluare a conformității se asigură că activitățile filialelor și ale subcontractanților lor nu afectează confidențialitatea, obiectivitatea sau imparțialitatea activităților lor de evaluare a conformității.

8) Organismele de evaluare a conformității și personalul acestora îndeplinesc activitățile de evaluare a conformității cu cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și nu sunt supuse 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.

9) Un organism de evaluare a conformității trebuie să fie capabil să efectueze toate atribuțiile de evaluare a conformității care îi sunt atribuite în temeiul prezentei legi, indiferent dacă atribuțiile respective sunt realizate în mod direct de organismul de evaluare a conformității sau în numele său și pe răspunderea sa. Orice subcontractare sau consultare a personalului extern este documentată în mod adecvat, nu implică intermediari și face obiectul unui acord scris care vizează, între altele, confidențialitatea și conflictele de interese. Organismul de evaluare a conformității în cauză își asumă întreaga răspundere pentru atribuțiile îndeplinite.

10) În orice moment și pentru fiecare procedură de evaluare a conformității și fiecare tip, categorie sau subcategorie de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, organismul de evaluare a conformității dispune de:

a) personalul necesar având cunoștințele tehnice necesare și experiența suficientă și corespunzătoare pentru a efectua atribuțiile 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.

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 TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat în cauză, precum și de caracterul de serie sau de masă al procesului de producție.

11) Un organism de evaluare a conformității dispune de mijloacele necesare pentru a îndeplini în mod corespunzător atribuțiile tehnice și administrative legate de activitățile de evaluare a conformității și să aibă acces la toate echipamentele sau facilitățile necesare.

12) Personalul responsabil cu îndeplinirea activităților de evaluare a conformității posedă următoarele calități:

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

b) cunoștințe satisfăcătoare ale cerințelor evaluărilor conformității 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 conformității au fost realizate.

13) Se garantează imparțialitatea organismelor de evaluare a conformității, a personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității, precum și a subcontractanților.

14) Remunerația personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu depinde de numărul de evaluări ale conformității realizate sau de rezultatele evaluărilor respective.

15) Organismele de evaluare a conformității încheie o asigurare de răspundere civilă.

16) Organismul de evaluare a conformității și personalul său, comitetele, filialele, subcontractanții și orice organism asociat sau personalul organismelor externe ale unui organism de evaluare a conformității păstrează confidențialitatea și secretul profesional în legătură cu toate informațiile obținute în îndeplinirea atribuțiilor de evaluare a conformității care le revin în temeiul prezentei legi, cu excepția cazului în care divulgarea este cerută de legislație și cu excepția relației cu autoritățile competente. Drepturile de proprietate intelectuală sunt protejate. Organismul de evaluare a conformității dispune de proceduri documentate în ceea ce privește cerințele prezentului punct.

17) Cu excepția pct. 16, cerințele din prezentul articol nu împiedică în schimburile de informații tehnice și de orientări în materie de reglementare între un organism de evaluare a conformității și o persoană care solicită certificarea, sau care intenționează să solicite certificarea.

18) Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termeni și condiții coerente, echitabile și rezonabile, ținând seama de interesele IMM-urilor, în ceea ce privește taxele.

19) Organismele de evaluare a conformității îndeplinesc cerințele standardului relevant, armonizat la nivel național, pentru acreditarea organismelor de evaluare a conformității care efectuează certificarea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate.

20) Organismele de evaluare a conformității se asigură că laboratoarele de testare utilizate în scopul evaluării conformității respectă cerințele standardului relevant, armonizat la nivel național, pentru acreditarea laboratoarelor care efectuează testări.

Articolul 23. Recunoașterea organismelor de evaluare a conformității acreditate în statele membre ale Uniunii Europene

(1) Organismele de evaluare a conformității acreditate de un organism național de acreditare dintr-un stat membru al Uniunii Europene, pot efectua evaluări ale conformității în cadrul sistemelor naționale de certificare a securității cibernetice, cu îndeplinirea cumulativă a următoarelor condiții:

a) acreditarea este valabilă și este emisă pentru domeniul relevant de evaluare a conformității;

b) organismul respectă cerințele aplicabile stabilite de sistemul național de certificare;

c) există mecanisme adecvate de cooperare și de schimb de informații între organism și Agenție;

d) organismul acceptă aplicarea cerințelor de supraveghere și de control prevăzute de prezenta lege și de sistemul național de certificare.

(2) Recunoașterea prevăzută la alin. (1) se efectuează de Agenție, cu consultarea organismului național de acreditare, în condițiile regulamentului aprobat de Guvern.

Capitolul VI
RECUNOAȘTEREA CERTIFICATELOR

Articolul 24. Recunoașterea certificatelor europene de securitate cibernetică

(1) Prin derogare de la art. 31 din Legea nr. 235/2011, certificatele europene de securitate cibernetică și declarațiile de conformitate UE, emise în cadrul sistemelor europene de certificare a securității cibernetice, se recunosc în Republica Moldova fără repetarea procedurilor de evaluare a conformității, în condițiile stabilite de Guvern.

(2) Lista sistemelor europene de certificare ale căror certificate și declarații de conformitate UE se recunosc în Republica Moldova, precum și condițiile și procedura de recunoaștere, se aprobă de Guvern, la propunerea Agenției.

(3) Recunoașterea prevăzută la alin. (1) poate fi întemeiată pe tratatele internaționale la care Republica Moldova este parte sau poate fi instituită unilateral, în baza verificării echivalenței tehnice și procedurale a sistemului european în cauză.

(4) Certificatele europene de securitate cibernetică recunoscute în condițiile prezentului articol produc aceleași efecte juridice ca certificatele de securitate cibernetică emise în cadrul sistemelor naționale de certificare la nivelul de asigurare corespunzător.

Articolul 25. Recunoașterea certificatelor emise în alte state

Certificatele de securitate cibernetică emise în cadrul sistemelor de certificare ale altor state se recunosc în Republica Moldova în temeiul tratatelor internaționale la care Republica Moldova este parte, cu respectarea principiilor reciprocității și echivalenței cerințelor de securitate, a criteriilor și a metodelor de evaluare.

Capitolul VII
TRANSPARENȚĂ, CONFIDENȚIALITATE ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL

Articolul 26. Evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate

(1) Agenția ține evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate și asigură publicarea informațiilor relevante privind acestea pe pagina sa web oficială.

(2) Agenția publică cel puțin următoarele informații:

a) emitentul;

b) titularul;

c) obiectul certificării;

d) sistemul de certificare aplicabil;

e) nivelul de asigurare;

f) perioada de valabilitate;

g) statutul certificatului sau al declarației de conformitate, inclusiv mențiunile privind suspendarea, retragerea ori expirarea acestora.

(3) Organismele de evaluare a conformității și entitățile care emit declarații de conformitate transmit Agenției informațiile necesare pentru ținerea evidenței certificatelor de securitate cibernetică și al declarațiilor de conformitate în termenul stabilit de sistemul național de certificare, dar nu mai târziu de 3 zile lucrătoare de la data emiterii, suspendării, retragerii sau modificării certificatului ori a declarației de conformitate.

Articolul 27. Publicarea sistemelor naționale de certificare

(1) Sistemele naționale de certificare a securității cibernetice, precum și modificările acestora, se publică în Monitorul Oficial al Republicii Moldova și pe pagina web oficială a Agenției.

(2) Agenția publică pe pagina sa web oficială ghiduri și materiale explicative privind aplicarea sistemelor naționale de certificare, adresate producătorilor, furnizorilor, organismelor de evaluare a conformității și utilizatorilor.

Articolul 28. Confidențialitatea și protecția datelor cu caracter personal

(1) Informațiile obținute de Agenție, de organismul național de acreditare și de organismele de evaluare a conformității în exercitarea atribuțiilor prevăzute de prezenta lege se utilizează exclusiv în scopul exercitării acestor atribuții. Informațiile care constituie secret comercial, alte informații confidențiale, precum și drepturile de proprietate intelectuală sunt protejate în condițiile legii.

(2) Fiecare sistem național de certificare stabilește delimitarea dintre informațiile care se publică și informațiile cu caracter confidențial aferente procesului de certificare.

(3) Prelucrarea datelor cu caracter personal în cadrul proceselor de certificare, inclusiv în legătură cu gestionarea cererilor de certificare, ținerea evidenței, examinarea plângerilor și publicarea informațiilor, se efectuează în conformitate cu Legea nr. 195/2024 privind protecția datelor cu caracter personal.

Capitolul VIII
RĂSPUNDEREA JURIDICĂ, PROCEDURA DE CONSTATARE ȘI SANCȚIUNILE

Articolul 29. Dreptul de a depune plângere

(1) Persoanele fizice sau juridice au dreptul să depună o plângere la Agenție în legătură cu potențialele încălcări ale prezentei legi.

(2) Termenul de prescripție pentru depunerea plângerii este de un an de la data la care persoana putea să ia cunoștință de presupusa încălcare, însă nu mai târziu de 3 ani de la data presupusei încălcări.

(3) În cazul unei presupuse încălcări continue sau prelungite, termenul de prescripție începe să curgă de la data săvârșirii ultimei acțiuni sau inacțiuni.

(4) În cazul în care plângerea este depusă după expirarea termenului de prescripție prevăzut la alin. (2) și (3), Agenția o respinge.

(5) Agenția informează autorul plângerii cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a contesta actele acestuia în conformitate cu art. 30.

(6) Plângerea se examinează în termen de 20 de zile lucrătoare de la data depunerii. În cazuri justificate de complexitatea examinării, termenul poate fi prelungit cu cel mult 20 de zile lucrătoare, cu informarea autorului plângerii.

(7) Prevederile Codului administrativ se aplică numai în măsura în care nu contravin prezentei legi

Articolul 30. Dreptul de a contesta acțiunile sau inacțiunile

(1) Acțiunile sau inacțiunile Agenției pot fi contestate direct în instanța de judecată, conform Codului administrativ, fără respectarea procedurii prealabile.

(2) În cazul în care Agenția nu examinează o plângere sau nu informează autorul acesteia în termen de 3 luni cu privire la progresele ori la soluționarea plângerii depuse conform art. 29, persoana afectată poate contesta inacțiunile Agenției direct în instanța de judecată, conform Codului administrativ, fără respectarea procedurii prealabile.

Articolul 31. Inițierea procedurii de constatare

(1) Agenția inițiază procedura de constatare a presupuselor cazuri de încălcare a prezentei legi:

a) la plângerea oricărei persoane afectate; sau

b) din oficiu, în baza informațiilor de care dispune cu privire la presupusa încălcare a prezentei legi.

(2) Procedura de constatare cuprinde:

a) examinarea preliminară; și/sau

b) investigarea.

(3) În orice stadiu al procedurii, părțile pot conveni asupra unei soluții amiabile, confirmată prin încheierea Agenției, care pune capăt procedurii fără a stabili o încălcare, dar cu obligația corectării comportamentului.

(4) Investigarea se dispune atunci când, în urma examinării preliminare, există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi. În celelalte cazuri, etapa investigării este omisă.

Articolul 32. Examinarea preliminară a plângerii

(1) Plângerea depusă la Agenție privind presupuse încălcări ale prezentei legi conține:

a) datele de identificare ale autorului plângerii (numele, prenumele sau denumirea, adresa sau sediul, adresa de poștă electronică);

b) specificarea circumstanțelor de fapt și de drept referitoare la pretinsa încălcare a prezentei legi;

c) informații care permit identificarea entității ce a comis pretinsa încălcare, în măsura în care este posibil;

d) măsurile solicitate a fi întreprinse de Agenție;

e) după caz, informații privind adresările înaintate entității ce a comis pretinsa încălcare, precum și rezultatul acestora;

f) semnătura autorului plângerii sau a reprezentantului său, iar în cazul plângerilor transmise în formă electronică, semnătura electronică.

(2) Examinarea preliminară a plângerii se efectuează în termen de 30 de zile de la data înregistrării. În cadrul acesteia, Agenția determină dacă există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi.

(3) Plângerile anonime sau cele depuse fără indicarea datelor de contact ale autorului nu se examinează.

(4) În cazul în care consideră că, în baza informațiilor prezentate, nu există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi, Agenția respinge motivat plângerea și informează autorul despre acest fapt.

Articolul 33. Investigarea

(1) Investigarea reprezintă activitatea de colectare și administrare a informațiilor cu privire la pretinsa încălcare, acumulate în condițiile prezentei legi.

(2) Dacă după examinarea preliminară se constată că există temeiuri rezonabile pentru a suspecta încălcarea prezentei legi, Agenția emite o dispoziție de inițiere a investigării.

(3) Investigările din oficiu se pot efectua:

a) în baza informațiilor privind presupuse încălcări ale prezentei legi obținute din alte surse, cum ar fi sesizările altor autorități publice, mass-media, rapoarte de audit ale conformității sau orice alte informații care indică în mod rezonabil asupra unei posibile încălcări;

b) în vederea cooperării internaționale în domeniul certificării securității cibernetice.

(4) La efectuarea investigării, Agenția are dreptul:

a) să solicite și să obțină accesul la toate documentele, informațiile, sistemele informatice și datele necesare pentru efectuarea investigării;

b) să solicite și să primească explicații și documente de la entitatea investigată, într-un termen rezonabil stabilit în funcție de complexitatea solicitării;

c) să audieze persoana investigată sau reprezentantul legal al acesteia asupra faptelor relevante pentru obiectul investigării și, după caz, să înregistreze răspunsurile acestora, cu informarea prealabilă a persoanei audiate;

d) să solicite sprijinul altor autorități competente pentru efectuarea investigării.

(5) Pe parcursul efectuării investigării, persoana investigată are dreptul:

a) să obțină o copie a delegației de efectuare a investigării;

b) să prezinte probe și explicații referitoare la obiectul investigării;

c) să fie asistată de avocați sau alți reprezentanți împuterniciți conform legislației;

d) să conteste deciziile Agenției în instanța de judecată competentă.

(6) Toate persoanele juridice de drept public sau de drept privat și persoanele fizice sunt obligate să se conformeze investigării efectuate de Agenție, inclusiv prin asigurarea condițiilor pentru buna desfășurare a acesteia.

(7) Termenul de efectuare a investigării este de până la 6 luni de la data inițierii, cu posibilitatea prelungirii justificate cu câte o lună, dar nu mai mult de 12

luni de la data inițierii, în funcție de complexitatea cauzei, de volumul de informații ce urmează a fi obținute și examinate și de comportamentul participanților la procedura de investigare.

(8) Rezultatul investigării este consemnat într-un proiect de decizie, care prevede constatarea sau lipsa încălcării, măsurile corective și sancțiunile aplicabile. Proiectul de decizie se comunică persoanei investigate, cu acordarea unui termen de 30 de zile pentru înaintarea unor eventuale obiecții.

(9) Confidențialitatea informațiilor obținute pe parcursul investigării este asigurată de către personalul Agenției implicat în procedură.

Articolul 34. Emiterea și comunicarea deciziilor

(1) La finalizarea investigării, Agenția emite decizia motivată cu privire la constatarea sau lipsa încălcării prezentei legi și cu privire la aplicarea măsurilor corective și a sancțiunilor, după caz.

(2) Decizia se comunică persoanei investigate în termen de 10 zile lucrătoare de la data emiterii.

(3) Deciziile Agenției pot fi contestate direct în instanța de judecată competentă, conform Codului administrativ, fără respectarea procedurii prealabile.

(4) Agenția publică rezumatul deciziilor emise, în care reflectă natura încălcărilor depistate, motivarea deciziei, măsurile dispuse, precum și sancțiunile aplicate.

Articolul 35. Executarea deciziilor Agenției

(1) Deciziile Agenției se execută în termenul menționat în ele, cu obligația persoanei investigate de a informa în scris Agenția despre măsurile întreprinse.

(2) Termenul de executare benevolă a amenzii este de cel puțin două luni de la data comunicării deciziei.

(3) Deciziile Agenției se execută silit în conformitate cu prevederile Codului de executare.

Articolul 36. Măsurile corective

(1) În cazul constatării încălcării prezentei legi sau a sistemelor naționale de certificare, Agenția poate dispune, prin decizie motivată, următoarele măsuri corective:

a) suspendarea dreptului de utilizare a certificatului, a mărcii sau a etichetei de certificare;

b) interzicerea referirii la certificare ori la declarația de conformitate în activitatea de promovare sau de comercializare;

c) retragerea certificatului de securitate cibernetică, în condițiile art. 17 alin. (3);

d) informarea publicului, în cazul în care neconformitatea prezintă riscuri pentru utilizatori.

(2) Măsurile corective sunt proporționale cu natura și gravitatea încălcării și pot fi aplicate separat sau cumulativ cu sancțiunile prevăzute la art. 38.

Articolul 37. Sancțiunile

(1) Pentru încălcările prevăzute la art. 38, Agenția aplică amenzi. Amenzile aplicate sunt, în fiecare caz, eficace, proporționale și disuasive și se varsă la bugetul de stat.

(2) La aplicarea amenzii și la determinarea cuantumului acesteia se iau în considerare, în fiecare caz, următoarele circumstanțe:

a) natura, gravitatea și durata încălcării, inclusiv nivelul de asigurare aplicabil și impactul potențial asupra utilizatorilor;

b) caracterul intenționat al încălcării sau comiterea acesteia din neglijență;

c) acțiunile întreprinse pentru a reduce prejudiciul și pentru a remedia încălcarea;

d) eventualele încălcări anterioare relevante;

e) gradul de cooperare cu Agenția pentru remedierea încălcării și atenuarea posibilelor efecte negative;

f) beneficiile financiare dobândite sau pierderile evitate ca urmare a încălcării, în măsura în care acestea pot fi stabilite;

g) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului.

(3) În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi aplicată ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul amenzii.

(4) Sancțiunile se aplică în termen de un an de la data constatării încălcării, dar nu mai târziu de 3 ani de la data comiterii acesteia.

(5) Aplicarea sancțiunii nu exonerează persoana sancționată de obligația de a înceta încălcarea și de a executa măsurile corective dispuse.

Articolul 38. Încălcările pasibile de amendă

(1) Se aplică amenzi de până la 100 000 de lei pentru:

a) utilizarea unui certificat de securitate cibernetică suspendat, retras ori expirat sau referirea falsă la deținerea unui certificat ori a unei declarații de conformitate;

b) utilizarea mărcilor sau a etichetelor de certificare cu încălcarea condițiilor stabilite de sistemul național de certificare;

(2) Se aplică amenzi de până la 200 000 de lei pentru:

a) desfășurarea, în cadrul unui sistem național de certificare a securității cibernetice, a activităților de evaluare a conformității sau emiterea certificatelor de securitate cibernetică de către un organism neacreditat ori, după caz, neautorizat sau nerecunoscut în condițiile prezentei legi;

b) falsificarea rezultatelor evaluării conformității sau emiterea certificatelor în baza unor informații despre care organismul emitent cunoștea că sunt false;

c) împiedicarea desfășurării investigațiilor, a auditurilor sau a controalelor efectuate în condițiile art. 6;

d) neexecutarea măsurilor corective dispuse în condițiile art. 36.

(3) Amenzile se aplică prin decizie a Agenției, care poate fi contestată în condițiile art. 30.

Capitolul IX
DISPOZIȚII FINALE

Articolul 39. Dispoziții finale

(1) Prezenta lege intră în vigoare la expirarea a 18 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Guvernul, în termen de 18 luni de la data publicării prezentei legi:

a) va aproba regulamentul privind procedura de autorizare și de recunoaștere a organismelor de evaluare a conformității în domeniul certificării securității cibernetice;

b) va aproba metodologia de elaborare a sistemelor naționale de certificare a securității cibernetice;

c) va aproba lista sistemelor europene de certificare ale căror certificate se recunosc în Republica Moldova, precum și condițiile și procedura de recunoaștere;

d) va aduce actele sale normative în concordanță cu prezenta lege.

Președintele Parlamentului

NOTĂ DE FUNDAMENTARE
la proiectul de lege privind certificarea securității cibernetice

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ

Proiectul de lege privind certificarea securității cibernetice (în continuare-proiectul de lege) a fost elaborat de către Ministerul Dezvoltării Economice și Digitalizării (în continuare - MDED).

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Prezentul proiect de lege a fost elaborat în vederea punerii în aplicare parțiale a *Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor, precum și de abrogare a Regulamentului (UE) nr. 526/2013 (Cybersecurity Act), așa cum a fost modificat ultima dată prin Regulamentul (UE) 2025/37 al Parlamentului European și al Consiliului din 19 decembrie 2024.*

Necesitatea elaborării proiectului derivă din obligațiile asumate de Republica Moldova în procesul de aderare la Uniunea Europeană și de armonizare progresivă a legislației naționale cu acquis-ul Uniunii Europene în domeniul securității cibernetice.

Armonizarea legislației naționale cu Regulamentului (UE) 2019/881 este prevăzută în Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025, în cadrul Clusterului 3 „Competitivitate și Creștere Incluzivă", capitolul 10 „Societatea informațională și mass-media", acțiunea normativă 37, termen de realizare decembrie 2026, care stabilește măsurile necesare pentru alinierea cadrului normativ național la legislația Uniunii Europene în domeniul securității cibernetice, inclusiv acțiunea privind instituirea unui mecanism național de certificare a securității cibernetice, care să includă un set de norme, cerințe tehnice, standarde și proceduri aplicabile certificării sau evaluării conformității produselor TIC, serviciilor TIC și proceselor TIC.

Prin urmare, proiectul de lege reprezintă instrumentul normativ necesar pentru instituirea cadrului juridic privind certificarea securității cibernetice în Republica Moldova, asigurând compatibilitatea cu sistemul european de certificare a securității cibernetice și creând premisele recunoașterii și aplicării schemelor europene de certificare la nivel național.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Republica Moldova dispune de un cadru normativ și instituțional care reglementează guvernanța securității cibernetice, însă acesta nu acoperă domeniul certificării securității cibernetice. Prin adoptarea Legii nr. 48/2023 privind securitatea cibernetică, care transpune Directiva (UE) 2022/2555 (NIS 2), au fost instituite cerințe privind gestionarea riscurilor de securitate cibernetică, notificarea incidentelor și supravegherea entităților esențiale și importante. Totodată, în temeiul Legii nr. 48/2023 și al Hotărârii Guvernului nr. 1028/2023, a fost constituită Agenția pentru Securitate Cibernetică, care exercită atribuțiile de autoritate competentă și de echipă națională de răspuns la incidente de securitate cibernetică (CSIRT), asigurând funcționalități instituționale comparabile cu cele prevăzute de Regulamentul (UE) 2019/881 în domeniul guvernanței securității cibernetice.

Cu toate acestea, cadrul normativ național nu reglementează componenta privind certificarea securității cibernetice, reglementată prin Titlul III al Regulamentului (UE) 2019/881. În consecință, legislația Republicii Moldova nu instituie mecanismele juridice și instituționale necesare implementării unui sistem național de certificare a securității cibernetice compatibil cu sistemul european.

Analiza cadrului normativ național în raport cu prevederile Regulamentului (UE) 2019/881 a evidențiat următoarele deficiențe și lacune normative principale:

1. Nu este desemnată o autoritate națională de certificare a securității cibernetice, învestită cu atribuțiile prevăzute la art. 58 din Regulamentul (UE) 2019/881, inclusiv în ceea ce privește supravegherea aplicării sistemelor de certificare, autorizarea organismelor de evaluare a conformității, examinarea plângerilor, suspendarea sau retragerea certificatelor și aplicarea măsurilor de executare.

2. Nu există un cadru juridic privind sistemele de certificare a securității cibernetice, inclusiv proceduri privind elaborarea, aprobarea, implementarea, monitorizarea și revizuirea acestora.

3. Nu sunt reglementate nivelurile de asigurare a securității cibernetice („de bază", „substanțial" și „ridicat"), precum și cerințele și procedurile de evaluare corespunzătoare fiecărui nivel, în conformitate cu art. 52 din Regulamentul (UE) 2019/881.

4. Nu este reglementat mecanismul de autoevaluare a conformității și declarația UE de conformitate în domeniul securității cibernetice, prevăzute la art. 53 din Regulamentul (UE) 2019/881.

5. Terminologia specifică domeniului certificării securității cibernetice (produs TIC, serviciu TIC, proces TIC, serviciu de securitate gestionat, sistem european de certificare a securității cibernetice, nivel de asigurare, certificat european de securitate cibernetică etc.) este parțial definită în legislația națională.

6. Nu sunt instituite mecanismele necesare implementării și supravegherii certificării, inclusiv o evidență a certificatelor de securitate cibernetică, norme privind transparența și confidențialitatea informațiilor aferente procesului de certificare, un regim sancționator specific și mecanisme de recunoaștere și valorificare pe teritoriul Republicii Moldova a certificatelor emise în cadrul sistemelor europene de certificare a securității cibernetice.

Deficiențele menționate împiedică instituirea și funcționarea unui mecanism național de certificare a securității cibernetice compatibil cu sistemul european și nu permit recunoașterea și valorificarea certificatelor europene de securitate cibernetică pe teritoriul Republicii Moldova.

Totodată, analiza relevă existența unor premise instituționale favorabile implementării noului cadru normativ. Republica Moldova dispune deja de infrastructura națională de acreditare și evaluare a conformității, reglementată prin Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, inclusiv de mecanismul recunoașterii în vederea notificării prevăzut de Capitolul IV[1] al acesteia. De asemenea, cadrul național de standardizare este reglementat prin Legea nr. 20/2016 cu privire la standardizarea națională, iar legislația națională stabilește deja mecanisme de certificare într-un domeniu conex, respectiv certificarea în materia protecției datelor cu caracter personal, reglementată de art. 42–43 din Legea nr. 195/2024 privind protecția datelor cu caracter personal. Aceste elemente demonstrează că Republica Moldova dispune de infrastructura instituțională necesară pentru implementarea unui sistem național de certificare a securității cibernetice, fiind necesară instituirea cadrului juridic specific și atribuirea competențelor corespunzătoare autorităților implicate.

Absența unui cadru juridic privind certificarea securității cibernetice produce efecte negative atât asupra autorităților publice și utilizatorilor de produse, servicii și procese TIC, cât și asupra mediului de afaceri. În lipsa unor mecanisme de certificare recunoscute, autoritățile contractante și ceilalți beneficiari nu dispun de un instrument obiectiv pentru verificarea nivelului de securitate al produselor, serviciilor și proceselor TIC pe care le utilizează sau le achiziționează. Totodată, producătorii și furnizorii din Republica Moldova nu beneficiază de posibilitatea obținerii unei certificări compatibile cu cadrul european pe piața națională, ceea ce le reduce competitivitatea pe piața Uniunii Europene și poate genera costuri suplimentare de conformare. În același timp, lipsa unor dispoziții privind recunoașterea certificatelor europene de securitate cibernetică creează incertitudine juridică și riscul duplicării procedurilor de evaluare a conformității.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul de lege urmărește instituirea, pentru prima dată în Republica Moldova, a cadrului juridic și instituțional privind certificarea securității cibernetice a produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, în conformitate cu principiile și cerințele stabilite de Titlul III al Regulamentului (UE) 2019/881 privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor.

Proiectul instituie un mecanism național de certificare a securității cibernetice, stabilește autoritățile și entitățile implicate, procedurile de certificare și evaluare a conformității, condițiile de recunoaștere a certificatelor europene, precum și măsurile necesare pentru supravegherea și asigurarea respectării cerințelor aplicabile.

Proiectul de lege este structurat în 9 capitole, după cum urmează:

Capitolul I „Dispoziții generale” (art. 1–3) stabilește obiectul, scopul și domeniul de aplicare al legii, precum și principalele noțiuni utilizate în domeniul certificării securității cibernetice. Sunt introduse noțiuni armonizate cu Regulamentul (UE) 2019/881, inclusiv cele privind serviciile de securitate gestionate, nivelurile de asigurare, autoevaluarea conformității, certificatele de securitate cibernetică și sistemele de certificare.

Capitolul II „Cadrul instituțional” (art. 4–8) desemnează Agenția pentru Securitate Cibernetică în calitate de autoritate națională de certificare a securității cibernetice și stabilește atribuțiile acesteia. Sunt instituite garanții privind independența și separarea funcțională dintre activitățile de certificare și cele de supraveghere. Totodată, sunt reglementate mecanismele de cooperare cu MOLDAC, autoritățile de protecție a datelor cu caracter personal, autoritățile de supraveghere a pieței și organismele europene relevante.

Capitolul III „Sistemele naționale de certificare a securității cibernetice” (art. 9–14) reglementează elaborarea, aprobarea și aplicarea sistemelor naționale de certificare. Sunt stabilite obiectivele de securitate pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate, elementele obligatorii ale sistemelor de certificare, precum și nivelurile de asigurare „de bază”, „substanțial” și „ridicat”. Totodată, sunt prevăzute mecanismele de corelare a sistemelor naționale cu sistemele europene de certificare.

Capitolul IV „Certificarea și autoevaluarea conformității” (art. 15–19) stabilește caracterul voluntar al certificării, condițiile în care aceasta poate deveni obligatorie prin lege, procedurile de emitere, suspendare și retragere a certificatelor, precum și mecanismul de autoevaluare a conformității pentru nivelul de asigurare „de bază”. Sunt stabilite obligații privind informarea utilizatorilor cu privire la caracteristicile de securitate ale produselor și serviciilor certificate.

Capitolul V „Organismele de evaluare a conformității” (art. 20–23) reglementează acreditarea și autorizarea organismelor care efectuează evaluarea conformității, cerințele privind independența, imparțialitatea, competența tehnică și confidențialitatea acestora, precum și mecanismele de recunoaștere a organismelor acreditate în statele membre ale Uniunii Europene.

Capitolul VI „Recunoașterea certificatelor” (art. 24–25) instituie mecanismul de recunoaștere în Republica Moldova a certificatelor europene de securitate cibernetică și a declarațiilor UE de conformitate, fără repetarea procedurilor de evaluare, precum și condițiile de recunoaștere a certificatelor emise în alte state.

Capitolul VII „Transparență, confidențialitate și protecția datelor cu caracter personal” (art. 26–28) stabilește obligațiile privind publicitatea sistemelor de certificare și reglementează protecția informațiilor confidențiale și a datelor cu caracter personal.

Capitolul VIII „Răspunderea juridică, procedura de constatare și sancțiunile” (art. 29–38) instituie mecanismele de examinare a plângerilor, efectuare a investigațiilor, aplicare a măsurilor corective și sancțiunilor pentru încălcarea prevederilor legii. Capitolul stabilește garanțiile procedurale aplicabile persoanelor investigate și posibilitatea contestării directe în instanța de judecată a actelor emise de Agenție.

Capitolul IX „Dispoziții finale” (art.39) stabilește termenul de intrare în vigoare a legii, precum și obligațiile Guvernului privind aprobarea actelor normative necesare implementării acesteia.

Elementele de noutate ale proiectului constau în:

1. instituirea, pentru prima dată, a unui cadru juridic național privind certificarea securității cibernetice, compatibil cu cadrul european;
2. desemnarea Agenției pentru Securitate Cibernetică în calitate de autoritate națională de certificare și stabilirea atribuțiilor acesteia;
3. introducerea mecanismelor de certificare pentru produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate;
4. introducerea nivelurilor de asigurare a securității cibernetice și a mecanismului de autoevaluare a conformității;
5. stabilirea mecanismului de recunoaștere a certificatelor europene de securitate cibernetică;
6. instituirea unui mecanism complet de supraveghere, control și sancționare a încălcărilor în domeniul certificării securității cibernetice.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În cadrul procesului de elaborare a proiectului de lege și în baza Raportului de analiză a deficiențelor legislative, au fost examinate mai multe opțiuni de intervenție normativă pentru instituirea cadrului juridic privind certificarea securității cibernetice.

Opțiunea I – completarea Legii nr. 48/2023 privind securitatea cibernetică cu un capitol dedicat certificării securității cibernetice.

Această opțiune nu a fost selectată, întrucât domeniul certificării securității cibernetice are un obiect de reglementare distinct față de mecanismele generale de guvernanță a securității cibernetice instituite prin Legea nr. 48/2023. Certificarea implică reglementarea unor aspecte specifice privind evaluarea conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, acreditarea și autorizarea organismelor de evaluare a conformității, recunoașterea certificatelor și supravegherea aplicării sistemelor de certificare.

Totodată, includerea acestor norme în Legea nr. 48/2023 ar fi condus la extinderea substanțială a obiectului acesteia și la combinarea a două domenii de reglementare cu finalități diferite: gestionarea riscurilor și a incidentelor de securitate cibernetică, pe de o parte, și evaluarea și certificarea nivelului de securitate al produselor, serviciilor și proceselor TIC, pe de altă parte. O astfel de abordare ar putea afecta coerența și claritatea cadrului normativ existent.

Opțiunea II – menținerea situației actuale (statu-quo), cu eventuala recunoaștere informală a certificatelor europene de securitate cibernetică.

Această opțiune nu a fost selectată, întrucât menținerea cadrului normativ actual nu ar permite instituirea unui mecanism național de certificare compatibil cu Regulamentul (UE) 2019/881 și nu ar asigura un temei juridic pentru recunoașterea certificatelor europene de securitate cibernetică.

O asemenea abordare ar menține incertitudinea juridică pentru producătorii, furnizorii și utilizatorii de produse și servicii TIC, nu ar permite exercitarea unor atribuții de supraveghere de către o autoritate desemnată și nu ar asigura realizarea angajamentelor asumate de Republica Moldova în procesul de aderare la Uniunea Europeană.

Opțiunea selectată – adoptarea unei legi speciale privind certificarea securității cibernetice, completată de acte normative subordonate pentru punerea în aplicare.

Această opțiune asigură un cadru juridic previzibil și complet pentru instituirea sistemului național de certificare a securității cibernetice, permite delimitarea clară a competențelor instituționale și asigură compatibilitatea cu mecanismele europene de certificare.

Totodată, soluția valorifică infrastructura instituțională existentă în domeniul acreditării și evaluării conformității, inclusiv rolul MOLDAC, precum și experiența acumulată prin mecanismele de certificare instituite în alte domenii, inclusiv prin Legea nr. 195/2024 privind protecția datelor cu caracter personal.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Implementarea proiectului de lege va genera un impact instituțional asupra sectorului public prin atribuirea Agenției pentru Securitate Cibernetică a unei funcții noi, cea de autoritate națională de certificare a securității cibernetice.

Exercitarea acestei funcții va presupune dezvoltarea unor capacități instituționale suplimentare, inclusiv:

1. elaborarea și gestionarea sistemelor naționale de certificare a securității cibernetice;
2. asigurarea supravegherii aplicării acestora;
3. examinarea plângerilor și a sesizărilor privind activitățile de certificare;
4. evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate;
5. exercitarea atribuțiilor de control și aplicarea măsurilor prevăzute de cadrul normativ.

În acest context, va fi necesară ajustarea cadrului organizatoric și funcțional al Agenției pentru Securitate Cibernetică, inclusiv a Regulamentului privind organizarea și funcționarea Agenției, aprobat prin Hotărârea Guvernului nr. 1028/2023, prin instituirea capacităților necesare exercitării noilor atribuții și asigurarea separării organizatorice și funcționale a activităților de certificare de cele de supraveghere. De asemenea, vor fi necesare ajustări ale structurii și efectivului-limită al Agenției, în conformitate cu procedurile aplicabile.

Implementarea proiectului va avea impact și asupra Centrului Național de Acreditare MOLDAC, care își va extinde domeniul de activitate prin dezvoltarea și aplicarea schemelor de acreditare pentru organismele de evaluare a conformității care vor activa în domeniul certificării securității cibernetice. Aceste activități se încadrează în mandatul existent al MOLDAC, stabilit prin Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, și vor fi realizate în baza standardelor europene și internaționale aplicabile.

Totodată, Guvernul și autoritățile administrației publice centrale responsabile vor asigura elaborarea și aprobarea actelor normative subordonate necesare punerii în aplicare a prevederilor legii, inclusiv a celor referitoare la procedurile de certificare, recunoașterea certificatelor europene și aplicarea sistemelor naționale de certificare.

Pe termen mediu și lung, instituirea cadrului național de certificare a securității cibernetice va produce efecte pozitive asupra sectorului public în calitate de utilizator și beneficiar al produselor, serviciilor și proceselor TIC. Autoritățile publice vor dispune de un instrument obiectiv pentru evaluarea nivelului de securitate cibernetică al soluțiilor TIC utilizate sau achiziționate, ceea ce va contribui la reducerea riscurilor asociate utilizării tehnologiilor digitale și la consolidarea securității infrastructurilor informaționale de stat.

4.2. Impactul financiar și argumentarea costurilor estimative

Proiectul de lege atribuie Agenției pentru Securitate Cibernetică un mandat nou, distinct de cel exercitat în prezent în temeiul Legii nr. 48/2023 privind securitatea cibernetică, și anume cel de autoritate națională de certificare a securității cibernetice (art. 4–6 din proiect). Atribuțiile aferente acestui mandat nu se regăsesc în Regulamentul de organizare și funcționare a Agenției, aprobat prin Hotărârea Guvernului nr. 1028/2023, și nici în fișele de post ale personalului existent. Este vorba, în special, de: elaborarea, consultarea, aprobarea și revizuirea periodică a sistemelor naționale de certificare; autorizarea și monitorizarea organismelor de evaluare a conformității, în cooperare cu MOLDAC; supravegherea titularilor de certificate și a producătorilor/furnizorilor care emit declarații de conformitate; recunoașterea certificatelor europene de securitate cibernetică; evidența certificatelor și al declarațiilor de conformitate; examinarea plângerilor, efectuarea investigațiilor, aplicarea măsurilor corective și a sancțiunilor (Capitolul VIII); cooperarea cu MOLDAC, ENISA și autoritățile naționale de certificare din statele membre ale UE; asigurarea secretariatului Consiliului consultativ pentru certificarea securității cibernetice și elaborarea raportului anual de sinteză.

În vederea exercitării atribuțiilor de autoritate națională de certificare a securității cibernetice și a responsabilităților conexe Agenția pentru Securitate Cibernetică va necesita suplimentarea efectivului-limită cu o subdiviziune specializată, estimată la 4 unități de personal: 1 șef de secție și 3 specialiști principali.

Necesarul de resurse umane și costurile salariale lunare estimate, calculate în baza grilelor de salarizare stabilite de Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar (sumele incluzând salariul de bază, sporul de performanță de 10% și sporul specific de 120% pentru fiecare funcție), se prezintă după cum urmează:

Funcția	**Salariul lunar estimat (lei)**
Șef secție	35 294
Specialist principal	22 759

Specialist principal	22 759
Specialist principal	22 759
TOTAL lunar	**103 571**

Costul anual estimat al fondului de salarizare pentru subdiviziunea nou-creată este de aproximativ 1 242 852 lei (103 571 lei x 12 luni), sumă la care se adaugă contribuțiile de asigurări sociale și medicale obligatorii datorate de angajator, potrivit legislației în vigoare.

Necesitatea unei subdiviziuni distincte, cu personal propriu, rezultă direct din cerințele de independență și separare stabilite de proiect, preluate din art. 58 alin. (3) și (4) din Regulamentul (UE) 2019/881. Potrivit art. 4 alin. (3) și (4) din proiect, activitățile Agenției aferente emiterii certificatelor sunt strict separate, din punct de vedere organizatoric și funcțional, de activitățile de supraveghere și se desfășoară independent unele de celelalte. Totodată, potrivit art. 16 alin. (3) din proiect, în cazul în care Agenția emite certificate de nivel „ridicat", subdiviziunea sa de certificare se acreditează ca organism de evaluare a conformității, ceea ce presupune respectarea cerințelor de imparțialitate, competență și documentare a personalului prevăzute în anexa la Regulament și în standardul SM EN ISO/IEC 17065. Aceste cerințe exclud posibilitatea cumulării noilor atribuții de către personalul care exercită în prezent funcții de supraveghere a entităților esențiale și importante sau de răspuns la incidente, întrucât o asemenea cumulare ar genera conflicte de interese și ar compromite atât independența cerută de lege, cât și eligibilitatea pentru acreditare.

Efectivul de 4 unități reprezintă dimensiunea minimă care permite exercitarea separată a celor trei linii funcționale ale mandatului (cadrul normativ și sistemele de certificare; organismele de evaluare a conformității și evidența certificatelor/declarațiilor; supravegherea, plângerile și executarea), sub o coordonare unică, precum și asigurarea continuității activității în caz de absență a unui angajat. Repartizarea atribuțiilor pe funcții se prezintă după cum urmează:

Funcția	Atribuții principale
Șef secție	Coordonarea subdiviziunii; elaborarea actelor normative subordonate și a metodologiilor (art. 39 alin. (2) din proiect); cooperarea cu MOLDAC, ENISA și autoritățile de certificare din statele membre; secretariatul Consiliului consultativ; raportul anual de sinteză; asigurarea separării funcționale.
Specialist principal (sisteme de certificare)	Elaborarea și revizuirea sistemelor naționale de certificare; monitorizarea standardelor europene și internaționale relevante (ISO/IEC 15408, EN 17640, schema EUCC); organizarea consultărilor publice; corelarea cu sistemele europene și recunoașterea certificatelor europene (art. 14, 24–25).
Specialist principal (organisme de evaluare și evidența certificatelor/declarațiilor)	Autorizarea și monitorizarea organismelor de evaluare a conformității, în cooperare cu MOLDAC; evidența declarațiilor de conformitate; ținerea și actualizarea evidenței certificatelor/declarațiilor, precum și publicarea informațiilor despre acestea; verificarea informațiilor suplimentare puse la dispoziție de titulari.
Specialist principal (supraveghere și executare)	Examinarea plângerilor; efectuarea investigațiilor și auditurilor; aplicarea măsurilor corective, suspendarea și retragerea certificatelor; constatarea încălcărilor și aplicarea sancțiunilor; reprezentarea Agenției în litigii.

Structura propusă corespunde practicii statelor membre ale Uniunii Europene, în care atribuțiile de autoritate națională de certificare a securității cibernetice sunt exercitate, de regulă, de subdiviziuni dedicate din cadrul agențiilor naționale de securitate cibernetică (de exemplu, Direcția Evaluare și Certificare Securitate Cibernetică Noi Tehnologii, Produse și Servicii (EVAL) - Directoratul Național de Securitate Cibernetică (DNSC) - România, Certification and Compliance Division - Government Office of the Republic of Slovenia for Information Security (GISO), National Cybersecurity Certification Unit - National Security Authority (NBU) - Slovacia; National Cybersecurity Certification Authority (NCCA) - Centre for Cybersecurity Belgium (CCB) etc.). În etapa inițială, se preconizează ca certificatele de nivel „ridicat" să fie emise preponderent prin delegare către organisme de evaluare a conformității, în condițiile art. 16 alin. (2) din proiect; în cazul în care volumul activității de emitere a certificatelor de către Agenție o va justifica, necesarul de personal va fi reevaluat.

La momentul actual, în cadrul Agenției pentru Securitate Cibernetică sunt prevăzute 44 de funcții, dintre care 31 sunt ocupate, iar 13 sunt vacante, ceea ce reprezintă o rată de încadrare de 70,5%. Acest nivel de ocupare nu indică existența unui surplus de personal, ci reflectă etapa de consolidare instituțională a Agenției, care este o autoritate relativ recent constituită și devenită funcțională în anul 2024. De la constituire și până în prezent, Agenția și-a consolidat treptat capacitatea administrativă și operațională, iar procesul de recrutare a personalului continuă, fiind planificate noi angajări în vederea ocupării funcțiilor vacante și asigurării capacității necesare pentru exercitarea integrală a atribuțiilor stabilite prin lege.

Funcțiile vacante existente în cadrul Agenției sunt destinate exercitării atribuțiilor deja stabilite prin Legea nr. 48/2023 și Hotărârea Guvernului nr. 1028/2023, în special celor privind supravegherea entităților esențiale și importante, funcționarea echipei naționale de răspuns la incidente de securitate cibernetică (CSIRT), precum și gestionarea incidentelor și a crizelor de securitate cibernetică. Volumul acestor activități este în creștere, inclusiv ca urmare a extinderii obligațiilor ce decurg din procesul de transpunere și implementare a Directivei (UE) 2022/2555 (NIS 2). În aceste condiții, ocuparea funcțiilor vacante este necesară pentru asigurarea capacității Agenției de a-și exercita în mod corespunzător mandatul existent.

Redirecționarea funcțiilor vacante către exercitarea noilor atribuții în domeniul certificării securității cibernetice nu ar conduce la acoperirea necesarului real de personal, ci la transferarea deficitului de resurse umane de la atribuțiile existente către noile atribuții. O asemenea soluție ar diminua capacitatea Agenției de a asigura supravegherea entităților reglementate, răspunsul la incidente și gestionarea crizelor cibernetice, domenii care prezintă, de asemenea, o importanță directă în contextul procesului de integrare europeană.

Prin urmare, noile atribuții instituite prin proiect nu pot fi acoperite nici prin redistribuirea personalului existent, nici prin utilizarea funcțiilor vacante prevăzute pentru consolidarea capacității Agenției în domeniile deja reglementate. Personalul care urmează a fi recrutat pentru ocuparea acestor funcții este necesar pentru exercitarea atribuțiilor existente și nu reprezintă o rezervă de personal disponibilă pentru preluarea unor competențe suplimentare.

În plus, exercitarea atribuțiilor de certificare a securității cibernetice presupune competențe profesionale specializate, distincte de cele necesare pentru supravegherea entităților și răspunsul la incidente. Acestea includ, după caz, competențe în domeniul evaluării conformității, standardelor ISO/IEC 17065 și ISO/IEC 17025, metodologiilor Common Criteria și EN 17640, precum și al standardizării și al schemelor europene de certificare a securității cibernetice. Prin urmare, pentru exercitarea efectivă și corespunzătoare a noilor atribuții este necesară alocarea unor resurse umane distincte, cu profil profesional adecvat domeniului certificării.

Cu referire la impactul asupra activității Centrului Național de Acreditare MOLDAC, acreditarea organismelor de evaluare a conformității care vor activa în cadrul schemelor naționale de certificare a securității cibernetice se încadrează în mandatul existent al MOLDAC, stabilit prin Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității. Acreditarea acestora se va realiza în baza standardelor aplicabile deja de MOLDAC, inclusiv SM EN ISO/IEC 17065, pentru organismele de certificare a produselor, proceselor și serviciilor, și SM EN ISO/IEC 17025, pentru laboratoarele de încercări și etalonări, completate, după caz, cu cerințele specifice prevăzute de schemele naționale de certificare a securității cibernetice. Prin urmare, proiectul nu atribuie MOLDAC o funcție instituțională nouă, ci extinde domeniul de aplicare al activităților de acreditare în limitele mandatului său legal, fără a impune, în această etapă, majorarea efectivului-limită al instituției.

Impactul financiar asupra MOLDAC va consta, în principal, în costuri inițiale aferente dezvoltării capacității de acreditare în domeniul securității cibernetice, inclusiv elaborării și implementării programelor de acreditare, precum și instruirii și calificării personalului și evaluatorilor implicați. În cazul evaluărilor care necesită expertiză tehnică specializată și care nu este disponibilă la nivel național, MOLDAC va putea recurge, în condițiile legii și ale regulilor aplicabile, la experți tehnici din cadrul organismelor naționale de acreditare membre ale Cooperării Europene pentru Acreditare (EA). Costurile aferente implicării unor asemenea experți vor fi incluse în costul serviciilor de acreditare și suportate de solicitant, potrivit tarifelor aplicabile.

Cheltuielile inițiale necesare dezvoltării capacităților MOLDAC în acest domeniu vor putea fi acoperite din sursele financiare disponibile instituției și, după caz, din programe de asistență tehnică externă destinate dezvoltării infrastructurii calității și consolidării capacităților de evaluare a conformității.

Serviciile de acreditare a organismelor de evaluare a conformității în domeniul securității cibernetice vor fi prestate contra cost, în baza tarifelor aprobate de MOLDAC în condițiile legii. Acestea vor acoperi, după caz, etapele aferente examinării cererii, evaluării documentare, evaluării la fața locului, supravegherii și reacreditării, în conformitate cu cadrul normativ aplicabil. Acreditarea va fi acordată pentru perioada și în condițiile prevăzute de cadrul legal și de regulile de acreditare aplicabile.

Având în vedere dimensiunea actuală a pieței naționale și caracterul voluntar al certificării, se estimează că, în primii 3–5 ani de la intrarea în vigoare a legii, numărul organismelor de evaluare a conformității care vor solicita acreditarea în domeniul securității cibernetice va fi unul redus. În consecință, impactul suplimentar asupra activității și resurselor MOLDAC este estimat a fi unul limitat și gradual. Cuantumul exact al veniturilor și al cheltuielilor aferente exercitării acestor activități urmează a fi determinat în cadrul procedurii de avizare, în baza informațiilor și estimărilor prezentate de MOLDAC.

4.3. Impactul asupra sectorului privat

Proiectul de lege are un impact preponderent pozitiv asupra sectorului privat, prin instituirea unui cadru juridic predictibil și armonizat cu mecanismele europene de certificare a securității cibernetice. Certificarea securității cibernetice este instituită ca mecanism voluntar, astfel încât proiectul nu introduce obligații generale de certificare pentru producătorii, furnizorii sau prestatorii de servicii din domeniul tehnologiilor informației și comunicațiilor și nu generează costuri obligatorii de conformare pentru întregul mediu de afaceri.

Caracterul voluntar al certificării reprezintă un principiu fundamental preluat din Regulamentul (UE) 2019/881 (art. 56), menit să evite impunerea unor sarcini disproporționate asupra operatorilor economici încă din etapa inițială de instituire a mecanismului. Potrivit art. 15 alin. (2)–(4) din proiectul de lege, certificarea rămâne voluntară, cu excepția cazurilor în care legislația Republicii Moldova prevede altfel. Agenția pentru Securitate Cibernetică evaluează periodic eficiența și gradul de utilizare a fiecărui sistem național de certificare aprobat și analizează necesitatea trecerii acestuia la caracter obligatoriu, exclusiv atunci când o asemenea măsură este necesară pentru asigurarea unui nivel adecvat de securitate cibernetică a produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate vizate și pentru îmbunătățirea funcționării pieței interne.

Decizia de a propune trecerea de la caracterul voluntar la cel obligatoriu al unui sistem de certificare nu poate fi luată în mod discreționar, fiind condiționată de o evaluare care ia în considerare, cumulativ, conform art. 15 alin. (4) din proiect: impactul măsurii asupra producătorilor și furnizorilor vizați, precum și asupra utilizatorilor, raportat la avantajele economice generate de nivelul sporit de securitate preconizat; existența și gradul de aplicare a sistemelor europene de certificare echivalente; rezultatele unui proces de consultare deschis, transparent și cuprinzător cu toate părțile interesate relevante; termenele și măsurile de tranziție adecvate, cu luarea în considerare specifică a intereselor și nevoilor întreprinderilor mici și mijlocii, inclusiv ale microîntreprinderilor; precum și identificarea celei mai rapide și eficace modalități de punere în aplicare a tranziției. Orice propunere de introducere a caracterului obligatoriu al certificării pentru o categorie determinată de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate va necesita, prin urmare, o intervenție normativă distinctă, adoptată cu respectarea procedurilor legislative aplicabile, inclusiv a cerințelor de consultare publică.

Din perspectiva mediului de afaceri, experiența statelor membre ale Uniunii Europene indică o variație semnificativă a costurilor asociate certificării securității cibernetice, în funcție de nivelul de asigurare vizat și de complexitatea produsului evaluat. Evaluările complete de tip Common Criteria la niveluri de asigurare ridicate, utilizate în mod tradițional pentru produse cu profil de risc ridicat (de exemplu, componente hardware securizate, carduri inteligente, dispozitive critice), pot atinge, potrivit datelor de piață disponibile, costuri de ordinul a 100 000–300 000 euro per produs, ținând cont de complexitatea documentației tehnice și de profunzimea testelor de penetrare necesare. Pentru a răspunde nevoilor operatorilor de dimensiuni mai mici, la nivel european a fost dezvoltată metodologia de evaluare cu durată fixă (FiTCEM, standardul EN 17640), care limitează, de regulă, durata evaluării la 25–35 de zile-persoană, oferind o alternativă considerabil mai accesibilă din punct de vedere al costurilor și termenelor, adaptată în special întreprinderilor mici și mijlocii. Diferența semnificativă dintre aceste două abordări confirmă necesitatea ca sistemele naționale de certificare care urmează a fi elaborate în temeiul prezentului proiect de lege să prevadă, acolo unde este posibil, metodologii de evaluare proporționale cu nivelul de risc și cu capacitatea financiară a operatorilor economici vizați, inclusiv prin preluarea unor metodologii europene cu durată și cost previzibile.

Costurile aferente certificării vor interveni exclusiv în cazul entităților care vor decide să solicite certificarea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate, în funcție de necesitățile comerciale, de cerințele beneficiarilor sau de avantajele competitive urmărite. Aceste costuri reprezintă investiții voluntare în demonstrarea nivelului de securitate al soluțiilor oferite și nu constituie sarcini administrative impuse tuturor operatorilor economici.

Pentru producătorii și furnizorii naționali de produse și servicii TIC, proiectul creează posibilitatea utilizării unui mecanism oficial de confirmare a caracteristicilor de securitate ale soluțiilor dezvoltate sau furnizate. Obținerea unui certificat de securitate cibernetică va permite

acestor entități să demonstreze clienților, partenerilor comerciali și autorităților contractante existența unor niveluri verificate de securitate, sporind încrederea în produsele și serviciile oferite.

Instituirea unui sistem național compatibil cu cadrul european de certificare va contribui, de asemenea, la creșterea competitivității operatorilor economici autohtoni pe pieţele externe, prin reducerea barierelor tehnice și facilitarea recunoașterii certificărilor obținute în Republica Moldova în contexte economice internaționale. În special, alinierea la cerințele Regulamentului (UE) 2019/881 creează premise pentru integrarea graduală a furnizorilor naționali de produse și servicii TIC în lanțurile europene de furnizare a soluțiilor digitale securizate.

Proiectul va avea efecte pozitive și asupra sectorului prestatorilor de servicii specializate în domeniul evaluării conformității și securității cibernetice. Instituirea mecanismelor de acreditare și autorizare a organismelor de evaluare a conformității va crea condiții pentru dezvoltarea unei noi piețe de servicii, inclusiv pentru organismele de certificare, laboratoarele de testare și experții tehnici care vor participa la procesele de evaluare a securității produselor, serviciilor și proceselor TIC.

În același timp, proiectul asigură premise pentru reducerea costurilor indirecte suportate de operatorii economici care activează pe mai multe piețe. Recunoașterea certificatelor europene de securitate cibernetică și a declarațiilor de conformitate emise în cadrul sistemelor europene de certificare va evita repetarea procedurilor de evaluare și va diminua riscul efectuării unor evaluări paralele pentru aceleași produse sau servicii.

Un element important pentru mediul de afaceri îl constituie asigurarea accesibilității mecanismului de certificare, inclusiv pentru întreprinderile mici și mijlocii. În acest sens, proiectul stabilește cerințe privind aplicarea unor condiții echitabile și rezonabile de tarifare a serviciilor de evaluare a conformității, cu luarea în considerare a capacităților și intereselor IMM-urilor, astfel încât certificarea să nu devină o barieră disproporționată pentru operatorii economici de dimensiuni reduse.

Totodată, proiectul instituie un regim previzibil de supraveghere și răspundere juridică, aplicabil entităților implicate în procesul de certificare. Procedurile privind examinarea plângerilor, efectuarea investigațiilor și aplicarea măsurilor corective includ garanții procesuale pentru persoanele investigate, inclusiv dreptul de a prezenta obiecții, dreptul la apărare și posibilitatea contestării actelor emise de Agenția pentru Securitate Cibernetică în instanța de judecată.

Regimul sancționator instituit prin proiect urmărește asigurarea unui nivel adecvat de respectare a cerințelor de certificare, fără a crea o povară disproporționată asupra mediului de afaceri. Stabilirea criteriilor de individualizare a sancțiunilor, aplicarea principiilor eficacității, proporționalității și caracterului disuasiv, precum și delimitarea clară a faptelor sancționabile contribuie la asigurarea unui echilibru între protejarea securității cibernetice și menținerea unui climat favorabil activității economice.

În ansamblu, proiectul creează premise pentru dezvoltarea unui ecosistem național de certificare a securității cibernetice, creșterea încrederii în produsele și serviciile digitale furnizate pe piața Republicii Moldova, stimularea inovării și facilitarea integrării operatorilor economici naționali în economia digitală europeană.

4.4. Impactul social

Proiectul de lege produce un impact social pozitiv, în principal prin creșterea nivelului de securitate și de încredere în produsele, serviciile și procesele TIC utilizate de cetățeni, autorități publice și organizații private.

Instituirea unui mecanism transparent și verificabil de certificare a securității cibernetice va permite utilizatorilor finali să identifice soluțiile digitale care corespund unor niveluri determinate de securitate, contribuind la creșterea gradului de încredere în utilizarea tehnologiilor informației și comunicațiilor.

Impactul este relevant în special în contextul extinderii serviciilor publice electronice și al creșterii dependenței societății de infrastructurile digitale. Prin reducerea riscurilor asociate utilizării unor produse și servicii TIC vulnerabile, proiectul contribuie indirect la protejarea utilizatorilor împotriva incidentelor de securitate cibernetică și la consolidarea rezilienței digitale a societății.

Totodată, cadrul de certificare instituit va contribui la creșterea gradului de conștientizare privind importanța securității cibernetice și la promovarea unor practici mai sigure de dezvoltare, furnizare și utilizare a soluțiilor digitale.

4.4.1. Impactul asupra datelor cu caracter personal

Implementarea proiectului de lege implică prelucrarea unui volum limitat de date cu caracter personal, necesare pentru realizarea atribuțiilor prevăzute de lege, inclusiv gestionarea cererilor de certificare, evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate, examinarea plângerilor și exercitarea atribuțiilor de supraveghere.

Art. 28 din proiect stabilește expres obligația efectuării prelucrărilor de date cu caracter personal în conformitate cu prevederile Legii nr. 195/2024 privind protecția datelor cu caracter personal, cu respectarea principiilor legalității, transparenței, limitării scopului și minimizării datelor.

Evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate va conține, în principal, informații referitoare la persoane juridice, titularii certificatelor, producătorii, furnizorii și organismele de evaluare a conformității. Datele referitoare la persoane fizice vor fi incluse doar în măsura în care sunt necesare pentru identificarea persoanelor responsabile sau pentru exercitarea atribuțiilor legale ale Agenției pentru Securitate Cibernetică.

Totodată, fiecare sistem național de certificare va stabili delimitarea dintre informațiile destinate publicării și informațiile confidențiale, asigurând un echilibru între necesitatea transparenței procesului de certificare și protejarea informațiilor care constituie secret comercial sau date cu caracter personal.

4.4.2. Impactul asupra echității și egalității de gen

Proiectul de lege are caracter neutru din perspectiva egalității de gen și nu instituie tratamente diferențiate în funcție de sex sau de alte criterii protejate. Accesul la certificare, la acreditare și la activitățile de evaluare a conformității este deschis, în condiții egale, tuturor persoanelor care îndeplinesc cerințele legale.

4.5. Impactul asupra mediului

Proiectul de lege nu are un impact negativ direct asupra mediului înconjurător și nu implică activități cu potențial de poluare sau de afectare a echilibrului ecologic.

4.6. Alte impacturi și informații relevante

Proiectul de lege contribuie la consolidarea rezilienței cibernetice naționale, dezvoltarea ecosistemului de securitate cibernetică și apropierea cadrului normativ național de acquis-ul Uniunii Europene în domeniu.

Instituirea unui mecanism național de certificare compatibil cu Regulamentul (UE) 2019/881 va crea premise pentru dezvoltarea capacităților instituționale și economice necesare participării Republicii Moldova la mecanismele europene de certificare a securității cibernetice.

Prevederile privind corelarea sistemelor naționale de certificare cu sistemele europene și recunoașterea certificatelor europene asigură continuitatea juridică și tehnică a mecanismului instituit, evitând apariția unor sisteme paralele și reducând riscul unor costuri suplimentare pentru autorități și mediul privat în procesul de integrare europeană.

În ansamblu, proiectul reprezintă o componentă importantă a procesului de aliniere a Republicii Moldova la standardele europene privind securitatea digitală și contribuie la crearea unui spațiu digital mai sigur și mai de încredere pentru cetățeni, autorități și mediul de afaceri.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Proiectul nu transpune directive ale Uniunii Europene. Potrivit pct. 82 din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, aprobat prin Hotărârea Guvernului nr. 497/2026, informațiile privind punerea în aplicare a Regulamentului (UE) 2019/881 sunt prezentate la compartimentul 5.2.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Proiectul de lege pune în aplicare parțial, prin măsuri naționale, *Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), publicat în Jurnalul Oficial al Uniunii Europene L 151 din 7 iunie 2019, CELEX: 32019R0881, așa cum a fost modificat ultima dată prin Regulamentul (UE) 2025/37 al Parlamentului European și al Consiliului din 19 decembrie 2024 de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 2025/37 din 15 ianuarie 2025, CELEX: 32025R0037.*

Având în vedere natura juridică a regulamentelor Uniunii Europene, care sunt acte cu aplicabilitate directă în statele membre, proiectul nu transpune Regulamentul (UE) 2019/881, ci asigură punerea în aplicare a acestuia prin măsuri naționale, potrivit subpct. 44.1 din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, aprobat prin Hotărârea Guvernului nr. 497/2026: preia fidel prevederile materiale ale Titlului III al Regulamentului, necesare aplicării efective a acestora în perioada anterioară aderării, desemnează autoritatea competentă și stabilește atribuțiile, procedurile, sancțiunile și mecanismele de cooperare și control necesare.

Titlul III al Regulamentului instituie cadrul european de certificare a securității cibernetice, în scopul îmbunătățirii condițiilor de funcționare a pieței interne prin creșterea nivelului de securitate cibernetică și prin permiterea unei abordări armonizate la nivelul Uniunii a sistemelor europene de certificare a securității cibernetice, în vederea creării unei piețe unice digitale pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate. Prevederile Titlului III al Regulamentului nu au constituit anterior obiect al armonizării legislației naționale.

În acest sens, proiectul preia fidel, cu adaptările minime necesare integrării în ordinea juridică națională, în special, următoarele elemente ale cadrului european:

1. noțiunile și conceptele fundamentale prevăzute la art. 2 din Regulament, inclusiv cele privind produsul TIC, serviciul TIC, procesul TIC, serviciul de securitate gestionat, nivelul de asigurare, autoevaluarea conformității și sistemele de certificare a securității cibernetice;
2. obiectivele de securitate ale sistemelor de certificare aplicabile produselor TIC, serviciilor TIC și proceselor TIC (art. 51), precum și serviciilor de securitate gestionate (art. 51a);
3. nivelurile de asigurare „de bază", „substanțial" și „ridicat" și activitățile minime de evaluare corespunzătoare (art. 52);
4. mecanismul de autoevaluare a conformității și declarația de conformitate pentru nivelurile de asigurare corespunzătoare (art. 53);
5. elementele obligatorii ale sistemelor de certificare (art. 54) și obligațiile privind furnizarea informațiilor suplimentare referitoare la securitatea cibernetică (art. 55);
6. principiul caracterului voluntar al certificării și condițiile în care aceasta poate deveni obligatorie (art. 56);
7. regulile privind relația dintre sistemele naționale și sistemele europene de certificare (art. 57);
8. statutul, atribuțiile și competențele autorității naționale de certificare a securității cibernetice (art. 58);
9. cerințele privind acreditarea organismelor de evaluare a conformității (art. 60);
10. mecanismele privind depunerea plângerilor și asigurarea unei căi de atac efective (art. 63 și 64);
11. obligația instituirii unui regim sancționator eficace, proporțional și disuasiv (art. 65);
12. cerințele aplicabile organismelor de evaluare a conformității stabilite în anexa la Regulament.

Totodată, proiectul nu preia prevederile Regulamentului (UE) 2019/881 care reglementează exclusiv mecanisme instituționale interne ale Uniunii Europene și care nu sunt aplicabile unui stat care nu este membru al Uniunii Europene. În această categorie se includ, în special, dispozițiile privind organizarea și funcționarea ENISA (Titlul II), programul de activitate al Uniunii și procedura de adoptare a sistemelor europene de certificare de către Comisia Europeană (art. 46–50), evaluarea inter pares între autoritățile naționale de certificare ale statelor membre (art. 59), notificarea către Comisia Europeană (art. 61), Grupul european pentru certificarea securității cibernetice (ECCG) (art. 62), precum și dispozițiile finale referitoare la aplicarea regulamentului în cadrul Uniunii Europene. În tabelul de concordanță, aceste prevederi sunt reflectate cu calificativele „prevederi UE neaplicabile" sau, după caz, „prevederi UE direct aplicabile la aderare".

Principiile relevante ale acestor mecanisme au fost valorificate prin soluții naționale echivalente, inclusiv instituirea Consiliului consultativ pentru certificarea securității cibernetice, stabilirea mecanismelor de cooperare instituțională și internațională și posibilitatea cooperării cu ENISA.

Gradul de compatibilitate a proiectului cu Regulamentul (UE) 2019/881 este „pus în aplicare parțial", corespunzător clauzei de armonizare, și este reflectat în tabelul de concordanță întocmit conform modelului 2 din anexa nr. 2 la Regulamentul aprobat prin Hotărârea Guvernului nr. 497/2026, care însoțește proiectul de lege și se actualizează în funcție de modificările operate în textul proiectului până la adoptarea finală a acestuia.

Proiectul de lege urmărește crearea cadrului juridic intern necesar pentru aplicarea principiilor și mecanismelor europene privind certificarea securității cibernetice și pentru asigurarea unei tranziții eficiente către cadrul juridic al Uniunii Europene în domeniu.

În acest sens, proiectul instituie mecanismele naționale necesare pentru:

1. funcționarea unui sistem național de certificare a securității cibernetice bazat pe aceleași principii, niveluri de asigurare și cerințe tehnice aplicabile în cadrul european;

2. recunoașterea certificatelor europene de securitate cibernetică și a declarațiilor de conformitate emise în cadrul sistemelor europene de certificare;

3. recunoașterea organismelor de evaluare a conformității acreditate în statele membre ale Uniunii Europene, în condițiile stabilite de cadrul normativ național;

4. integrarea progresivă a mecanismului național în cadrul european de certificare a securității cibernetice la momentul aderării Republicii Moldova la Uniunea Europeană.

Prin instituirea acestor mecanisme, proiectul asigură evitarea creării unor sisteme paralele de certificare și protejarea investițiilor realizate de autorități și operatorii economici în dezvoltarea capacităților de certificare și evaluare a conformității.

La momentul aderării Republicii Moldova la Uniunea Europeană, prevederile Regulamentului (UE) 2019/881 vor deveni aplicabile în mod direct, iar, potrivit subpct. 38.2 din Regulamentul aprobat prin Hotărârea Guvernului nr. 497/2026, legea urmează a fi abrogată și înlocuită cu un act normativ care stabilește cadrul național de aplicare, cu trimitere directă la actul Uniunii Europene, fără preluarea prevederilor materiale ale acestuia.

6. Avizarea și consultarea publică a proiectului actului normativ

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării proiectului de hotărâre a fost publicat pe portalul guvernamental www.particip.gov.md, la următorul link: (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-elaborarii-proiectului-de-lege-cu-privire-la-aprobarea-sistemului-national-d/16524).

Totodată, proiectul de lege urmează a fi supus avizării și consultării publice în conformitate cu art. 32 din Legea nr. 100/2017 cu privire la actele normative, prin expedierea acestuia tuturor autorităților publice implicate în procesul de avizare , Cancelaria de Stat (Centrul de Armonizare a Legislației); Ministerul Justiției; Ministerul Infrastructurii și Dezvoltării Regionale; Ministerul Afacerilor Externe; Ministerul Finanțelor; Ministerul Educației și Cercetării; Ministerul Energiei, Ministerul Mediului, Ministerul Agriculturii și Industriei Alimentare, Ministerul Muncii și Protecției Sociale, Ministerul Afacerilor Interne, Ministerul Sănătății, Ministerul Culturii, IP Agenția Servicii Publice; Centrul Național pentru Protecția Datelor cu Caracter Personal; IP Serviciul Tehnologia Informației și Securitate Cibernetică, Biroul de Investigare a Accidentelor și Incidentelor în Transporturi, Compania Națională de Asigurări în Medicină, Casa Națională de Asigurări Sociale, Biroul Național de Statistică, Agenția Proprietății Publice, Agenția Națională pentru Siguranța Alimentelor, Agenția Medicamentului și Dispozitivelor Medicale, Agenția Geodezie, Cartografie și Cadastru, Agenția de Stat pentru Proprietatea Intelectuală, Agenția Națională pentru Reglementare în Comunicații inclusiv Agenției pentru Securitate Cibernetică, Centrului Național de Acreditare (MOLDAC), Institutului de Standardizare din Moldova, precum și asociațiilor profesionale din domeniul tehnologiei informației și comunicațiilor și mediului academic. Sinteza obiecțiilor și propunerilor va fi întocmită și publicată în condițiile legii.

7. Concluziile expertizelor

Conform art. 36 și 37 din Legea nr. 100/2017 cu privire la actele normative, proiectul va fi supus expertizei anticorupție și expertizei juridice, obiecțiile și propunerile urmând a fi luate în considerare la definitivarea acestuia.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul de lege se integrează în cadrul normativ existent prin instituirea unui regim juridic special privind certificarea securității cibernetice, complementar cadrului general de guvernanță a securității cibernetice instituit prin Legea nr. 48/2023 privind securitatea cibernetică.

Proiectul nu modifică principiile și mecanismele generale stabilite prin Legea nr. 48/2023, ci dezvoltă o componentă distinctă a acestora, referitoare la evaluarea și confirmarea nivelului de securitate al produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate. Proiectul nu implică abrogarea actelor normative în vigoare.

Aplicarea prevederilor proiectului va fi realizată în corelare cu următoarele acte normative:

1. Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește cadrul instituțional general în domeniul securității cibernetice, atribuțiile Agenției pentru Securitate Cibernetică și terminologia de bază utilizată;

2. Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, în ceea ce privește acreditarea organismelor de evaluare a conformității și rolul organismului național de acreditare (MOLDAC);

3. Legea nr. 20/2016 cu privire la standardizarea națională, în ceea ce privește utilizarea standardelor naționale și internaționale aplicabile proceselor de evaluare a conformității;

4. Legea nr. 195/2024 privind protecția datelor cu caracter personal, în ceea ce privește prelucrarea datelor cu caracter personal în cadrul procedurilor de certificare, ținerea registrelor și aplicarea măsurilor de supraveghere;

5. Codul administrativ nr. 116/2018, în ceea ce privește procedura administrativă, emiterea actelor administrative și exercitarea căilor de atac;

6. Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător, în ceea ce privește efectuarea controalelor și exercitarea atribuțiilor de supraveghere de către Agenția pentru Securitate Cibernetică;

7. Legea nr. 239/2008 privind transparența în procesul decizional, în ceea ce privește consultarea publică a proiectelor sistemelor naționale de certificare și a actelor normative subordonate.

Pentru implementarea efectivă a legii vor fi necesare elaborarea și aprobarea actelor normative subordonate prevăzute în dispozițiile finale ale proiectului, inclusiv cele referitoare la:

1. procedura de autorizare și recunoaștere a organismelor de evaluare a conformității;

2. metodologia de elaborare și aprobare a sistemelor naționale de certificare a securității cibernetice;

3. procedura de recunoaștere a certificatelor europene de securitate cibernetică.

Totodată, va fi necesară ajustarea cadrului instituțional aferent Agenției pentru Securitate Cibernetică, inclusiv a Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, în vederea reflectării noilor atribuții privind certificarea securității cibernetice și asigurării separării funcționale dintre activitățile de certificare și cele de supraveghere.

9. Măsuri necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea legii presupune realizarea, în mod etapizat, a unui set de măsuri normative, instituționale și operaționale, după cum urmează:

1. În termen de 18 luni de la data publicării legii, elaborarea și aprobarea de către Guvern a actelor normative necesare punerii în aplicare a prevederilor legii, inclusiv:

a) regulamentul privind procedura de autorizare și recunoaștere a organismelor de evaluare a conformității;

b) metodologia de elaborare, aprobare și revizuire a sistemelor naționale de certificare a securității cibernetice;

c) lista sistemelor europene de certificare ale căror certificate și declarații de conformitate sunt recunoscute în Republica Moldova, precum și condițiile și procedura de recunoaștere;

d) ajustarea cadrului normativ privind organizarea și funcționarea Agenției pentru Securitate Cibernetică, inclusiv a Hotărârii Guvernului nr. 1028/2023.

2. Consolidarea capacităților instituționale ale Agenției pentru Securitate Cibernetică, prin instituirea subdiviziunii responsabile de certificarea securității cibernetice, asigurarea separării organizatorice și funcționale a activităților de certificare de cele de supraveghere, precum și prin asigurarea încadrării cu personal calificat și dezvoltarea competențelor necesare.

3. Dezvoltarea capacităților organismului național de acreditare (MOLDAC) pentru aplicarea mecanismelor de acreditare în domeniul certificării securității cibernetice, inclusiv elaborarea și aplicarea schemelor de acreditare pentru organismele de evaluare a conformității, în cooperare cu Agenția pentru Securitate Cibernetică.

4. Instituirea Consiliului consultativ pentru certificarea securității cibernetice și aprobarea cadrului organizatoric necesar funcționării acestuia, în vederea asigurării participării autorităților publice, mediului de afaceri, mediului academic și altor părți interesate la dezvoltarea cadrului național de certificare.

5. Elaborarea și aprobarea primelor sisteme naționale de certificare a securității cibernetice, cu prioritizarea domeniilor TIC cu nivel ridicat de risc, relevanță strategică sau importanță pentru funcționarea serviciilor esențiale, precum și elaborarea ghidurilor și materialelor metodologice de aplicare.

6. Desfășurarea activităților de informare, instruire și promovare a mecanismului de certificare, adresate producătorilor, furnizorilor de produse și servicii TIC, organismelor de evaluare a conformității, autorităților publice și utilizatorilor finali, în vederea asigurării unei aplicări uniforme a noilor prevederi.

7. Monitorizarea și evaluarea implementării cadrului de certificare, inclusiv prin elaborarea și publicarea raportului anual de sinteză de către Agenția pentru Securitate Cibernetică, precum și prin evaluarea periodică a eficienței și utilizării sistemelor naționale de certificare, cu revizuirea acestora cel puțin o dată la 5 ani sau ori de câte ori evoluțiile tehnologice și de reglementare o impun.

Secretar de stat **Natalia Selevestru**

TABEL DE CONCORDANȚĂ

1. Titlul actului Uniunii Europene
Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (Text cu relevanță pentru SEE), CELEX: 32019R0881, așa cum a fost modificat ultima dată prin Regulamentul (UE) 2025/37 al Parlamentului European și al Consiliului din 19 decembrie 2024 de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate, CELEX: 32025R0037.
2. Titlul actului normativ național
Proiectul de lege privind certificarea securității cibernetice
3. Gradul de compatibilitate – pus în aplicare parțial
4. Autoritatea/persoana responsabilă - Ministerul Dezvoltării Economice și Digitalizării /
5. 2026
6.

Actul UE în limba română **7**	**Actul UE în limba engleză** **8**	**Actul/actele normativ/e național/e în limba română** **9**	**Traducerea actului/actelor normativ/e în limba engleză** **10**	**Gradul de compatibilitate** **11**	**Observațiile Republicii Moldova** **12**	**Observațiile Comisiei Europene** **13**
TITLUL I **DISPOZIȚII GENERALE**	**TITLE I** **GENERAL PROVISIONS**	**Capitolul I** **DISPOZIȚII GENERALE**				
Articolul 1 **Obiect și domeniu de aplicare**	**Article 1** **Subject matter and scope**	**Articolul 1. Obiect**				
(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 stabilește: (a) obiectivele, atribuțiile și aspectele organizaționale legate de ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică); și (b) un cadru pentru instituirea de sisteme europene de certificare a securității cibernetice cu scopul de a asigura un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate în Uniune, precum și cu scopul de a evita fragmentarea pieței interne în ceea ce privește sistemele de	(1) With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down: (a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and (b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services, ICT processes, and managed security services in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.	(1) Prezenta lege stabilește cadrul juridic și instituțional privind certificarea securității cibernetice a produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, inclusiv privind: a) elaborarea, aprobarea, administrarea și revizuirea sistemelor naționale de certificare a securității cibernetice; b) desemnarea, atribuțiile și competențele autorității naționale de certificare a securității cibernetice; c) acreditarea, autorizarea, recunoașterea și supravegherea organismelor de evaluare a conformității; d) emiterea, menținerea, suspendarea, retragerea și reînnoirea certificatelor de securitate cibernetică, precum și autoevaluarea conformității și declarația de conformitate;		Compatibil		

certificare a securității cibernetice din Uniune. Cadrul menționat la primul paragraf litera (b) se aplică fără a aduce atingere dispozițiilor specifice cuprinse în alte acte juridice ale Uniunii privind certificarea voluntară sau obligatorie.	The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification.	e) recunoașterea certificatelor europene de securitate cibernetică, a declarațiilor de conformitate UE și a rezultatelor evaluării conformității; f) transparența, supravegherea, răspunderea și căile de atac în domeniul certificării securității cibernetice. (2) Scopul prezentei legi constă în asigurarea unui nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate puse la dispoziție pe piața Republicii Moldova. **Articolul 2. Domeniul de aplicare** (1) Prezenta lege se aplică certificării securității cibernetice și autoevaluării conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate, efectuate în cadrul sistemelor naționale de certificare a securității cibernetice, precum și recunoașterii certificatelor și a declarațiilor de conformitate emise în cadrul sistemelor europene de certificare a securității cibernetice. (2) Prezenta lege se aplică producătorilor și furnizorilor de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate, indiferent de locul înregistrării acestora, în măsura în care produsele, serviciile sau procesele respective sunt puse la dispoziție pe piața Republicii Moldova ori sunt certificate, la cerere, în cadrul unui sistem național, precum și organismelor de evaluare a conformității care				

		desfășoară activități de evaluare în cadrul sistemelor naționale de certificare.				
(2) Prezentul regulament nu aduce atingere competențelor statelor membre în ceea ce privește activitățile aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.	(2) This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law.	(3) Prezenta lege nu aduce atingere competențelor autorităților publice în ceea ce privește activitățile aferente securității publice, apărării, securității naționale și nici activităților statului din domeniul dreptului penal.		Compatibil		
Articolul 2 Definiții	**Article 2 Definitions**	**Articolul 3. Noțiuni**				
În sensul prezentului regulament, se aplică următoarele definiții:	For the purposes of this Regulation, the following definitions apply:	În sensul prezentei legi, următoarele noțiuni semnifică:		Compatibil		
1. „securitate cibernetică” înseamnă activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane afectate de amenințări cibernetice;	1. ‘cybersecurity’ means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;	securitate cibernetică - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		
2. „rețea și sistem informatic” înseamnă rețea și sistem informatic astfel cum sunt definite la articolul 4 punctul 1 din Directiva (UE) 2016/1148;	2. ‘network and information system’ means a network and information system as defined in point (1) of Article 4 of Directive (EU) 2016/1148;	Art. 2 din Legea nr. 48/2023 privind securitatea cibernetică (noțiunea „rețea și sistem informatic”).		Compatibil	Noțiunea nu este preluată distinct în proiect, fiind definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică, la care trimit noțiunile de securitate cibernetică, produs TIC, serviciu TIC și proces TIC din art. 3 din proiect.	
3. „strategie națională privind securitatea rețelelor și a sistemelor informatice” înseamnă o strategie națională privind securitatea rețelelor și a sistemelor informatice astfel cum este definită la articolul 4 punctul 3 din Directiva (UE) 2016/1148;	3. ‘national strategy on the security of network and information systems’ means a national strategy on the security of network and information systems as defined in point (3) of Article 4 of Directive (EU) 2016/1148;			Prevederi UE direct aplicabile la aderare	Noțiunea respectivă se utilizează în prevederi ale Regulamentului UE care nu pot fi puse în aplicare de către Republica Moldova în calitate de stat candidat, având în vedere că acestea sunt concepute pentru statele membre ale Uniunii Europene și va deveni direct aplicabilă Republicii	

					Moldova de la data aderării la Uniunea Europeană.	
4. „operator de servicii esențiale” înseamnă un operator de servicii esențiale astfel cum este definit la articolul 4 punctul 4 din Directiva (UE) 2016/1148;	4. ‘operator of essential services’ means an operator of essential services as defined in point (4) of Article 4 of Directive (EU) 2016/1148;			Prevederi UE direct aplicabile la aderare	Noțiunea respectivă se utilizează în prevederi ale Regulamentului UE care nu pot fi puse în aplicare de către Republica Moldova în calitate de stat candidat, având în vedere că acestea sunt concepute pentru statele membre ale Uniunii Europene și va deveni direct aplicabilă Republicii Moldova de la data aderării la Uniunea Europeană.	
5. „furnizor de servicii digitale” înseamnă un furnizor de servicii digitale astfel cum este definit la articolul 4 punctul 6 din Directiva (UE) 2016/1148;	5. ‘digital service provider’ means a digital service provider as defined in point (6) of Article 4 of Directive (EU) 2016/1148;	furnizor de servicii digitale - persoană juridică care furnizează un serviciu digital;		Compatibil		
6. „incident” înseamnă un incident astfel cum este definit la articolul 4 punctul 7 din Directiva (UE) 2016/1148;	6. ‘incident’ means an incident as defined in point (7) of Article 4 of Directive (EU) 2016/1148;	incident cibernetic - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		
7. „administrarea incidentului” înseamnă o administrare a incidentului astfel cum este definită la articolul 4 punctul 8 din Directiva (UE) 2016/1148;	7. ‘incident handling’ means incident handling as defined in point (8) of Article 4 of Directive (EU) 2016/1148;	administrarea incidentului - procedurile utilizate pentru detectarea, analiza și limitarea unui incident cibernetic și răspunsul la acesta;		Compatibil		
8. „amenințare cibernetică” înseamnă orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora;	8. ‘cyber threat’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;	amenințare cibernetică - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		
9. „sistem european de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe	9. ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements,	sistem european de certificare a securității cibernetice - set cuprinzător de norme, cerințe tehnice, standarde și proceduri,		Compatibil		

tehnice, standarde și proceduri, instituite la nivelul Uniunii, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate;	standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services, ICT processes or managed security services;	instituite la nivelul Uniunii, care se aplică certificării sau evaluării conformității anumitor produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate;				
10. „sistem național de certificare a securității cibernetice” înseamnă un set cuprinzător de norme, cerințe tehnice, standarde și proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care intră în domeniul de aplicare al sistemului în cauză;	10. ‘national cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures developed and adopted by a national public authority and that apply to the certification or conformity assessment of ICT products, ICT services, ICT processes or managed security services falling under the scope of the specific scheme;	sistem național de certificare a securității cibernetice - set cuprinzător de norme, cerințe tehnice, standarde și proceduri elaborate și adoptate de o autoritate națională publică, care se aplică certificării sau evaluării conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care intră în domeniul de aplicare al sistemului în cauză;		Compatibil		
11. „certificat european de securitate cibernetică” înseamnă un document emis de un organism relevant prin care se atestă că un anumit produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat a fost evaluat în scopul verificării conformității cu cerințele de securitate specifice prevăzute în cadrul unui sistem european de certificare a securității cibernetice;	11. ‘European cybersecurity certificate’ means a document issued by a relevant body, attesting that a given ICT product, ICT service, ICT process or managed security service has been evaluated for compliance with specific security requirements laid down in a European cybersecurity certification scheme;	certificat de securitate cibernetică – document emis de un organism relevant prin care se atestă că un anumit produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat a fost evaluat în scopul verificării conformității cu cerințele de securitate specifice prevăzute în cadrul unui sistem de certificare a securității cibernetice;		Compatibil		
12. „produs TIC” înseamnă un element sau un grup de elemente al unei rețele sau al unui sistem informatic;	12. ‘ICT product’ means an element or a group of elements of a network or information system;	produs al tehnologiei informației și comunicațiilor (produs TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		
13. „serviciu TIC” înseamnă un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice;	13. ‘ICT service’ means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;	serviciu al tehnologiei informației și comunicațiilor (serviciu TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		

14. „proces TIC” înseamnă un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC;	14. ‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;	proces al tehnologiei informației și comunicațiilor (proces TIC) - astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;		Compatibil		
14a. „serviciu de securitate gestionat” înseamnă un serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor, testele de rezistență la intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate, în legătură cu asistența tehnică;	14a. ‘managed security service’ means a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice, related to technical support;	serviciu de securitate gestionat - serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor cibernetice, testele de rezistență la intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate, în legătură cu asistența tehnică;		Compatibil		
15. „acreditare” înseamnă acreditare astfel cum este definită la articolul 2 punctul 10 din Regulamentul (CE) nr. 765/2008;	15. ‘accreditation’ means accreditation as defined in point (10) of Article 2 of Regulation (EC) No 765/2008;	acreditare - astfel cum este definit la art. 2 din Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității;		Compatibil		
16. „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;	16. ‘national accreditation body’ means a national accreditation body as defined in point (11) of Article 2 of Regulation (EC) No 765/2008;	organism național de acreditare - astfel cum este definit la art. 2 din Legea nr. 235/2011;		Compatibil		
17. „evaluare a conformității” înseamnă o evaluare a conformității astfel cum este definită la articolul 2 punctul 12 din Regulamentul (CE) nr. 765/2008;	17. ‘conformity assessment’ means a conformity assessment as defined in point (12) of Article 2 of Regulation (EC) No 765/2008;	evaluare a conformității - astfel cum este definit la art. 2 din Legea nr. 235/2011;		Compatibil		
18. „organism de evaluare a conformității” înseamnă un organism de evaluare a conformității astfel cum este definit la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008;	18. ‘conformity assessment body’ means a conformity assessment body as defined in point (13) of Article 2 of Regulation (EC) No 765/2008;	organism de evaluare a conformității - astfel cum este definit la art. 2 din Legea nr. 235/2011;		Compatibil		
19. „standard” înseamnă un standard astfel cum este definit la articolul 2 punctul 1 din	19. ‘standard’ means a standard as defined in point (1) of Article 2 of Regulation (EU) No 1025/2012;	standard - astfel cum este definit la art. 2 din Legea nr. 20/2016 cu privire la standardizarea națională.		Compatibil		

Regulamentul (UE) nr. 1025/2012;						
20. „specificație tehnică” înseamnă un document care stabilește cerințele tehnice pe care trebuie să le îndeplinească un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, ori procedurile de evaluare a conformității referitoare la acestea;	20. ‘technical specification’ means a document that prescribes the technical requirements to be met by, or conformity assessment procedures relating to, an ICT product, ICT service, ICT process or managed security service;	specificație tehnică - document care stabilește cerințele tehnice pe care trebuie să le îndeplinească un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, ori procedurile de evaluare a conformității referitoare la acestea;		Compatibil		
21. „nivel de asigurare” înseamnă temeiul încrederii că un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat întrunește cerințele de securitate ale unui sistem european de certificare a securității cibernetice specific și indică nivelul la care a fost evaluat un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, dar care nu măsoară ca atare securitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat în cauză;	21. ‘assurance level’ means a basis for confidence that an ICT product, ICT service, ICT process or managed security service meets the security requirements of a specific European cybersecurity certification scheme, and indicates the level at which an ICT product, ICT service, ICT process or managed security service has been evaluated but as such does not measure the security of the ICT product, ICT service, ICT process or managed security service concerned;	nivel de asigurare - temeiul încrederii că un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat întrunește cerințele de securitate ale unui sistem de certificare a securității cibernetice specific și indică nivelul la care a fost evaluat un produs TIC, un serviciu TIC, un proces TIC sau un serviciu de securitate gestionat, dar care nu măsoară ca atare securitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat în cauză;		Compatibil		
22. „autoevaluare a conformității” înseamnă o acțiune desfășurată de un producător sau de un furnizor de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate care evaluează dacă respectivele produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate îndeplinesc cerințele unui sistem european de certificare a securității cibernetice specific.	22. ‘conformity self-assessment’ means an action carried out by a manufacturer or provider of ICT products, ICT services, ICT processes or managed security services, which evaluates whether those ICT products, ICT services, ICT processes or managed security services meet the requirements of a specific European cybersecurity certification scheme.	autoevaluare a conformității - acțiune desfășurată de un producător sau de un furnizor de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate care evaluează dacă respectivele produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate îndeplinesc cerințele unui sistem de certificare a securității cibernetice specific;		Compatibil		
TITLUL II ENISA (AGENȚIA UNIUNII EUROPENE PENTRU SECURITATE CIBERNETICĂ)	**TITLE II ENISA (THE EUROPEAN UNION AGENCY FOR CYBERSECURITY)**				Prevederile titlului II (art. 3–45) reglementează mandatul, obiectivele, atribuțiile, organizarea	

					și funcționarea ENISA și, prin obiectul lor, nu necesită măsuri naționale de punere în aplicare.	
CAPITOLUL I **Mandat și obiective**	**CHAPTER I** **Mandate and objectives**					
Articolul 3 **Mandat**	**Article 3** **Mandate**					
(1) ENISA îndeplinește atribuțiile care îi sunt încredințate în temeiul prezentului regulament în scopul de a asigura un nivel comun ridicat de securitate cibernetică în întreaga Uniune, inclusiv sprijinind în mod activ statele membre și instituțiile, organele, oficiile și agențiile Uniunii pentru a-și îmbunătăți securitatea cibernetică. ENISA servește drept punct de referință în ceea ce privește consilierea și expertiza în materie de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile Uniunii, precum și pentru alte părți interesate relevante din Uniune. ENISA contribuie la reducerea fragmentării pe piața internă prin îndeplinirea atribuțiilor care îi sunt încredințate în temeiul prezentului regulament.	(1) ENISA shall carry out the tasks assigned to it under this Regulation for the purpose of achieving a high common level of cybersecurity across the Union, including by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. ENISA shall act as a reference point for advice and expertise on cybersecurity for Union institutions, bodies, offices and agencies as well as for other relevant Union stakeholders. ENISA shall contribute to reducing the fragmentation of the internal market by carrying out the tasks assigned to it under this Regulation.			Prevederi UE neaplicabile		
(2) ENISA îndeplinește atribuțiile care îi sunt încredințate prin acte juridice ale Uniunii care stabilesc măsuri de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre care au legătură cu securitatea cibernetică.	(2) ENISA shall carry out the tasks assigned to it by Union legal acts that set out measures for approximating Member State laws, regulations and administrative provisions which are related to cybersecurity.			Prevederi UE neaplicabile		
(3) În îndeplinirea atribuțiilor sale, ENISA acționează în mod independent, evitând să dubleze activitățile statelor membre și	(3) When carrying out its tasks, ENISA shall act independently while avoiding the duplication of Member State activities and taking into			Prevederi UE neaplicabile		

ținând seama de expertiza pe care o au deja statele membre.	consideration existing Member State expertise.					
(4) ENISA își dezvoltă propriile resurse, inclusiv capacitățile și competențele tehnice și umane, necesare pentru a îndeplini atribuțiile care îi sunt încredințate în temeiul prezentului regulament.	(4) ENISA shall develop its own resources, including technical and human capabilities and skills, necessary to perform the tasks assigned to it under this Regulation.			Prevederi UE neaplicabile		
Articolul 4 **Obiective**	**Article 4** **Objectives**					
(1) ENISA este un centru de expertiză în materie de securitate cibernetică, datorită independenței sale, calității științifice și tehnice a consilierii și asistenței acordate și a informațiilor furnizate, transparenței procedurilor de operare și metodelor de funcționare, precum și a diligenței cu care își îndeplinește atribuțiile.	(1) ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.			Prevederi UE neaplicabile		
(2) ENISA oferă asistență instituțiilor, organelor, oficiilor și agențiilor 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.	(2) ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.			Prevederi UE neaplicabile		
(3) ENISA sprijină consolidarea capacităților și procesul de pregătire în întreaga Uniune, furnizând asistență instituțiilor, organelor, oficiilor și agențiilor 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.	(3) ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.			Prevederi UE neaplicabile		

(4) ENISA promovează cooperarea, inclusiv schimbul de informații și coordonarea la nivelul Uniunii între statele membre, instituțiile, organele, oficiile și agențiile Uniunii și părțile interesate relevante din sectorul public și privat cu privire la chestiuni legate de securitatea cibernetică.	(4) ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.			Prevederi UE neaplicabile		
(5) ENISA contribuie la sporirea capacităților de securitate cibernetică la nivelul Uniunii pentru a sprijini acțiunile statelor membre în materie de prevenire a amenințărilor cibernetice și de răspuns la acestea, în special în cazul incidentelor transfrontaliere.	(5) ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.			Prevederi UE neaplicabile		
(6) ENISA promovează recurgerea la certificarea europeană a securității cibernetice, cu scopul de a evita fragmentarea pieței interne. ENISA contribuie la instituirea și menținerea unui cadru de certificare europeană a securității cibernetice în conformitate cu titlul III din prezentul regulament, pentru a crește transparența securității cibernetice a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate, consolidând astfel încrederea în piața internă digitală și în competitivitatea acesteia.	(6) ENISA shall promote the use of European cybersecurity certification with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation with a view to increasing the transparency of the cybersecurity of ICT products, ICT services, ICT processes and managed security services, thereby strengthening trust in the digital internal market and its competitiveness.			Prevederi UE neaplicabile		
(7) ENISA promovează un nivel ridicat de sensibilizare în privința securității cibernetice, inclusiv a igienei cibernetice și alfabetizării cibernetice a cetățenilor, organizațiilor și întreprinderilor.	(7) ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.			Prevederi UE neaplicabile		
CAPITOLUL II **Atribuții**	**CHAPTER II** **Tasks**					

Articolul 5 **Elaborarea și punerea în aplicare a politicii și a dreptului Uniuni**	**Article 5** **Development and implementation of Union policy and law**					
ENISA contribuie la elaborarea și punerea în aplicare a politicii și a dreptului Uniunii: 1. acordând asistență și consiliere cu privire la elaborarea și revizuirea politicii și a dreptului Uniunii în domeniul securității cibernetice, precum și cu privire la inițiative politice și legislative sectoriale în cazul în care sunt implicate aspecte legate de securitatea cibernetică, în special prin furnizarea de avize independente și analize și prin desfășurarea de lucrări pregătitoare; 2. acordând asistență statelor membre pentru punerea în aplicare cu coerență a politicii și dreptului Uniunii privind securitatea cibernetică, mai ales în ceea ce privește Directiva (UE) 2016/1148, inclusiv prin intermediul emiterii 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. acordând asistență statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii la elaborarea și promovarea unor politici în materie de securitate cibernetică legate de susținerea disponibilității sau a integrității generale a	ENISA shall contribute to the development and implementation of Union policy and law, by: (1) assisting and advising on the development and review of Union policy and law in the field of cybersecurity and on sector-specific policy and law initiatives where matters related to cybersecurity are involved, in particular by providing its independent opinion and analysis as well as carrying out preparatory work; (2) assisting Member States to implement the Union policy and law regarding cybersecurity consistently, in particular in relation to Directive (EU) 2016/1148, including by means of issuing opinions, guidelines, providing advice and best practices on topics such as risk management, incident reporting and information sharing, as well as by facilitating the exchange of best practices between competent authorities in that regard; (3) assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies related to sustaining the general availability or integrity of the public core of the open internet; (4) contributing to the work of the Cooperation Group pursuant to Article 11 of			Prevederi UE neaplicabile		

nucleului public al internetului deschis; 4.contribuind la activitatea grupului de cooperare instituit în temeiul articolului 11 din Directiva (UE) 2016/1148, prin furnizarea de expertiză și de asistență; 5.sprijinind: (a)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 prin facilitarea schimbului de bune practici între autoritățile competente; (b)promovarea unui nivel sporit de securitate a comunicațiilor electronice, inclusiv prin furnizarea de consiliere și de expertiză, precum și prin facilitarea schimbului de bune practici între autoritățile competente; (c)statele membre în punerea în aplicare a aspectelor specifice legate de securitatea cibernetică cuprinse în politica și dreptul Uniunii referitoare la protecția datelor și a vieții private, inclusiv prin consilierea Comitetului european pentru protecția datelor, la cerea acestuia. 6.sprijinind revizuirea periodică a activităților legate de politica Uniunii prin elaborarea unui raport anual privind stadiul punerii în aplicare a cadrului juridic aplicabil în ceea ce privește: (a)informările privind notificările incidentelor	Directive (EU) 2016/1148, by providing its expertise and assistance; (5) supporting: (b) the promotion of an enhanced level of security of electronic communications, including by providing advice and expertise, as well as by facilitating the exchange of best practices between competent authorities; (c) Member States in the implementation of specific cybersecurity aspects of Union policy and law relating to data protection and privacy, including by providing advice to the European Data Protection Board upon request; (6) supporting the regular review of Union policy activities by preparing an annual report on the state of the implementation of the respective legal framework regarding: (d) information on Member States' incident notifications provided by the single points of contact to the Cooperation Group pursuant to Article 10(3) of Directive (EU) 2016/1148; (e) summaries of notifications of breach of security or loss of integrity received from trust service providers provided by the supervisory bodies to ENISA, pursuant to Article 19(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council (1); (f) notifications of security incidents transmitted by the providers of public electronic					

transmise de statele membre prin punctele unice de contact grupului de cooperare în temeiul articolului 10 alineatul (3) din Directiva (UE) 2016/1148; (b) rezumatul notificărilor privind încălcarea securității sau pierderea integrității primite de la prestatorii de servicii de încredere, transmise ENISA de organismele de supraveghere în temeiul articolului 19 alineatul (3) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([23]); (c) notificările privind incidentele de securitate transmise de furnizorii de rețele publice de comunicații electronice sau servicii de comunicații electronice destinate publicului, transmise ENISA de autoritățile competente în temeiul articolului 40 din Directiva (UE) 2018/1972.	communications networks or of publicly available electronic communications services, provided by the competent authorities to ENISA, pursuant to Article 40 of Directive (EU) 2018/1972.					
Articolul 6 **Consolidarea capacităților**	**Article 6** **Capacity-building**					
(1) ENISA acordă asistență: (a) statelor membre, în eforturile lor de a îmbunătăți prevenirea, detectarea și analizarea amenințărilor cibernetice și a incidentelor și capacitatea de răspuns la acestea, prin furnizarea cunoștințelor și a expertizei necesare; (b) statelor membre și instituțiilor, organelor, oficiilor și agențiilor Uniunii la elaborarea și punerea în	(1) ENISA shall assist: (a) Member States in their efforts to improve the prevention, detection and analysis of, and the capability to respond to cyber threats and incidents by providing them with knowledge and expertise; (b) Member States and Union institutions, bodies, offices and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis;			Prevederi UE neaplicabile		

aplicare a politicilor pentru divulgarea vulnerabilităților în mod voluntar; (c) instituțiilor, organelor, oficiilor și agențiilor Uniunii, în eforturile lor de a îmbunătăți prevenirea, detectarea și analiza amenințărilor cibernetice și a incidentelor și de a îmbunătăți capacitățile de răspuns la astfel de amenințări cibernetice și incidente, mai ales printr-un sprijin adecvat acordat CERT-UE; (d) statelor membre în ceea ce privește dezvoltarea echipelor CSIRT naționale, la solicitarea acestora, în temeiul articolului 9 alineatul (5) din Directiva (UE) 2016/1148; (e) statelor membre în ceea ce privește elaborarea strategiilor naționale privind securitatea rețelelor și a sistemelor informatice, la solicitarea acestora în temeiul articolului 7 alineatul (2) din Directiva (UE) 2016/1148 și promovează difuzarea acestor strategii în întreaga Uniune și constată progresele înregistrate în punerea lor în aplicare, pentru a promova bunele practici; (f) 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; (g) echipelor CSIRT naționale și ale Uniunii, în ceea ce privește creșterea nivelului	(c) Union institutions, bodies, offices and agencies in their efforts to improve the prevention, detection and analysis of cyber threats and incidents and to improve their capabilities to respond to such cyber threats and incidents, in particular through appropriate support for the CERT-EU; (d) Member States in developing national CSIRTs, where requested pursuant to Article 9(5) of Directive (EU) 2016/1148; (e) Member States in developing national strategies on the security of network and information systems, where requested pursuant to Article 7(2) of Directive (EU) 2016/1148, and promote the dissemination of those strategies and note the progress in their implementation across the Union in order to promote best practices; (f) Union institutions in developing and reviewing Union strategies regarding cybersecurity, promoting their dissemination and tracking the progress in their implementation; (g) national and Union CSIRTs in raising the level of their capabilities, including by promoting dialogue and exchanges of information, with a view to ensuring that, with regard to the state of the art, each CSIRT possesses a common set of minimum capabilities and operates according to best practices; (h) Member States by regularly organising the					

capacităților proprii, inclusiv prin promovarea dialogului și a schimbului de informații, pentru a garanta că, având în vedere stadiul actual al tehnologiei, fiecare echipă CSIRT dispune de un set comun de capacități minime și funcționează în conformitate cu cele mai bune practici; (h) statelor membre, prin organizarea în mod regulat a exercițiilor în materie de securitate cibernetică la nivelul Uniunii menționate la articolul 7 alineatul (5) cel puțin o dată la doi ani și prin formularea de recomandări de politici bazate pe procesul de evaluare a exercițiilor și pe învățămintele desprinse în urma acestora; (i) organismelor publice relevante, prin oferirea de cursuri de formare privind securitatea cibernetică, în cooperare cu părțile interesate acolo unde este cazul; (j) grupului de cooperare, în ceea ce privește schimbul de bune practici, în special în ceea ce privește identificarea de către statele membre a operatorilor de servicii esențiale, în temeiul articolului 11 alineatul (3) litera (l) din Directiva (UE) 2016/1148, inclusiv în legătură cu dependența transfrontalieră legată de riscuri și incidente.	cybersecurity exercises at Union level referred to in Article 7(5) on at least a biennial basis and by making policy recommendations based on the evaluation process of the exercises and lessons learned from them; (i) relevant public bodies by offering trainings regarding cybersecurity, where appropriate in cooperation with stakeholders; (j) the Cooperation Group, in the exchange of best practices, in particular with regard to the identification by Member States of operators of essential services, pursuant to point (l) of Article 11(3) of Directive (EU) 2016/1148, including in relation to cross-border dependencies, regarding risks and incidents.					
(2) ENISA sprijină schimbul de informații în cadrul sectoarelor și între acestea, mai ales în sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, prin furnizarea de bune practici și de orientări privind	(2) ENISA shall support information sharing in and between sectors, in particular in the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available			Prevederi UE neaplicabile		

instrumentele disponibile, proceduri, precum și privind modul de abordare a aspectelor de reglementare legate de schimbul de informații.	tools, procedures, as well as on how to address regulatory issues related to information-sharing.					
Articolul 7 **Cooperarea operațională la nivelul Uniunii**	**Article 7** **Operational cooperation at Union level**					
(1) ENISA sprijină cooperarea operațională între statele membre, instituțiile, organele, oficiile și agențiile Uniunii, precum și între părțile interesate.	(1) ENISA shall support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders.			Prevederi UE neaplicabile		
(2) ENISA cooperează la nivel operațional și stabilește sinergii cu instituțiile, organele, oficiile și agențiile Uniunii, inclusiv cu CERT-UE, cu serviciile care au atribuții de combatere a criminalității informatice și cu autoritățile de supraveghere care au atribuții de protecție a vieții private și a datelor cu caracter personal, în vederea abordării problemelor de interes comun, inclusiv prin: (a)schimbul de know-how și de bune practici; (b)furnizarea de consiliere și emiterea de orientări privind chestiunile relevante legate de securitatea cibernetică; (c)stabilirea modalităților practice pentru executarea unor atribuții specifice, după consultarea Comisiei.	(2) ENISA shall cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies, including the CERT-EU, with the services dealing with cybercrime and with supervisory authorities dealing with the protection of privacy and personal data, with a view to addressing issues of common concern, including by means of: (a) the exchange of know-how and best practices; (b) the provision of advice and issuing of guidelines on relevant matters related to cybersecurity; (c) the establishment of practical arrangements for the execution of specific tasks, after consulting the Commission.			Prevederi UE neaplicabile		
(3) ENISA asigură secretariatul rețelei CSIRT în temeiul articolului 12 alineatul (2) din Directiva (UE) 2016/1148 și, în această capacitate, sprijină activ schimbul de informații și cooperarea între membrii acesteia.	(3) ENISA shall provide the secretariat of the CSIRTs network pursuant to Article 12(2) of Directive (EU) 2016/1148, and in that capacity shall actively support the information sharing and			Prevederi UE neaplicabile		

	the cooperation among its members.					
(4) ENISA sprijină statele membre în cooperarea operațională cu rețeaua CSIRT: (a) acordându-le consiliere cu privire la modul în care își pot îmbunătăți capacitățile de a preveni, de a detecta incidentele și de a răspunde la acestea, precum și acordându-le consiliere, la cererea unuia sau mai multor state membre, în legătură cu o amenințare cibernetică specifică; (b) acordându-le asistență, la cererea unuia sau mai multor state membre, la evaluarea incidentelor cu un impact semnificativ sau substanțial prin furnizarea de expertiză și prin facilitarea administrării din punct de vedere tehnic a respectivelor incidente, mai ales susținând schimbul voluntar de informații relevante și de soluții tehnice între statele membre; (c) analizând vulnerabilitățile și incidentele pe baza informațiilor disponibile public sau a informațiilor furnizate în mod voluntar de statele membre în acest scop; și (d) la cererea unuia sau mai multor state membre, oferind sprijin în legătură cu anchetele tehnice *ex post* privind incidentele cu un impact semnificativ sau substanțial în înțelesul Directivei (UE) 2016/1148. În îndeplinirea acestor atribuții, ENISA și CERT-UE desfășoară o cooperare structurată pentru a beneficia de sinergii și pentru a evita dublarea activităților.	(4) ENISA shall support Member States with respect to operational cooperation within the CSIRTs network by: (a) advising on how to improve their capabilities to prevent, detect and respond to incidents and, at the request of one or more Member States, providing advice in relation to a specific cyber threat; (b) assisting, at the request of one or more Member States, in the assessment of incidents having a significant or substantial impact through the provision of expertise and facilitating the technical handling of such incidents including in particular by supporting the voluntary sharing of relevant information and technical solutions between Member States; (c) analysing vulnerabilities and incidents on the basis of publicly available information or information provided voluntarily by Member States for that purpose; and (d) at the request of one or more Member States, providing support in relation to ex-post technical inquiries regarding incidents having a significant or substantial impact within the meaning of Directive (EU) 2016/1148. In performing those tasks, ENISA and CERT-EU shall engage in structured cooperation to benefit from synergies and to avoid the duplication of activities.			Prevederi UE neaplicabile		

(5) ENISA organizează exerciții periodice de securitate cibernetică la nivelul Uniunii și sprijină statele membre și instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește organizarea de exerciții de securitate cibernetică, la cererea acestora. Aceste exerciții de securitate cibernetică la nivelul Uniunii pot include elemente tehnice, operaționale sau strategice. Din doi în doi ani, ENISA organizează un exercițiu cuprinzător la scară largă. După caz, ENISA contribuie, de asemenea, la exercițiile sectoriale de securitate cibernetică și sprijină organizarea acestora, împreună cu organizațiile relevante care participă, de asemenea, la exercițiile de securitate cibernetică desfășurate la nivelul Uniunii.	(5) ENISA shall regularly organise cybersecurity exercises at Union level, and shall support Member States and Union institutions, bodies, offices and agencies in organising cybersecurity exercises following their requests. Such cybersecurity exercises at Union level may include technical, operational or strategic elements. On a biennial basis, ENISA shall organise a large-scale comprehensive exercise. Where appropriate, ENISA shall also contribute to and help organise sectoral cybersecurity exercises together with relevant organisations that also participate in cybersecurity exercises at Union level.			Prevederi UE neaplicabile		
(6) În strânsă cooperare cu statele membre, ENISA întocmește periodic un raport aprofundat asupra situației tehnice în materie de securitate cibernetică la nivelul UE referitor la incidente și amenințări cibernetice, pe baza informațiilor disponibile public, a propriei sale analize și pe baza unor rapoarte transmise de echipele CSIRT ale statelor membre sau punctele unice de contact instituite prin Directiva (UE) 2016/1148, în ambele cazuri în mod voluntar, EC3 și CERT-UE, printre altele.	(6) ENISA, in close cooperation with the Member States, shall prepare a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats based on publicly available information, its own analysis, and reports shared by, among others, the Member States' CSIRTs or the single points of contact established by Directive (EU) 2016/1148, both on a voluntary basis, EC3 and CERT-EU.			Prevederi UE neaplicabile		
(7) ENISA 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	(7) ENISA shall contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or			Prevederi UE neaplicabile		

amploare legate de securitatea cibernetică, în principal prin: (a)agregarea și analizarea rapoartelor autorităților naționale care fac parte din domeniul public sau sunt 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)facilitarea, la cerere, a administrării din punct de vedere tehnic a acestor incidente sau crize, mai ales prin sprijinirea partajării voluntare a soluțiilor tehnice între statele membre; (d)sprijinirea instituțiilor, organelor, oficiilor și agențiilor Uniunii precum și, la cererea acestora, a statelor membre, în ceea ce privește comunicarea publică referitoare la astfel de incidente sau crize; (e)testarea planurilor de cooperare menite să răspundă la aceste incidente sau crize la nivelul Uniunii și, la cerere, sprijinirea statelor membre în ceea ce privește testarea respectivelor planuri la nivel național.	crises related to cybersecurity, mainly by: (a) aggregating and analysing reports from national sources that are in the public domain or shared on a voluntary basis with a view to contributing to the establishment of common situational awareness; (b) ensuring the efficient flow of information and the provision of escalation mechanisms between the CSIRTs network and the technical and political decision-makers at Union level; (c) upon request, facilitating the technical handling of such incidents or crises, including, in particular, by supporting the voluntary sharing of technical solutions between Member States; (d) supporting Union institutions, bodies, offices and agencies and, at their request, Member States, in the public communication relating to such incidents or crises; (e) testing the cooperation plans for responding to such incidents or crises at Union level and, at their request, supporting Member States in testing such plans at national level.					
Articolul 8 **Piața, certificarea securității cibernetice și standardizarea**	**Article 8** **Market, cybersecurity certification, and standardisation**					
(1) ENISA sprijină și promovează elaborarea și punerea în aplicare a politicii Uniunii privind certificarea securității cibernetice	(1) ENISA shall support and promote the development and implementation of Union policy on the cybersecurity certification of ICT products,			Prevederi UE neaplicabile		

a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate, astfel cum se prevede în titlul III din prezentul regulament, prin: (a)monitorizarea permanentă a evoluțiilor din domenii conexe standardizării și recomandarea unor specificații tehnice adecvate pentru a fi utilizate la dezvoltarea unor sisteme europene de certificare a securității cibernetice, în temeiul articolului 54 alineatul (1) litera (c), în cazurile în care standardele nu sunt disponibile; (b)pregătirea propunerilor de sisteme europene de certificare a securității cibernetice (denumite în continuare „propuneri de sisteme”) pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate, în conformitate cu articolul 49; (c)evaluarea sistemelor europene de certificare a securității cibernetice adoptate, în conformitate cu articolul 49 alineatul (8); (d)participarea la evaluările *inter pares* în temeiul articolului 59 alineatul (4); (e)oferirea de asistență Comisiei în ceea ce privește asigurarea secretariatului ECCG, în temeiul articolului 62 alineatul (5).	ICT services, ICT processes and managed security services, as established in Title III of this Regulation, by: (a) monitoring developments, on an ongoing basis, in related areas of standardisation and recommending appropriate technical specifications for use in the development of European cybersecurity certification schemes pursuant to point (c) of Article 54(1) where standards are not available; (b) preparing candidate European cybersecurity certification schemes (candidate schemes) for ICT products, ICT services, ICT processes and managed security services in accordance with Article 49; (c) evaluating adopted European cybersecurity certification schemes in accordance with Article 49(8); (d) participating in peer reviews pursuant to Article 59(4); (e) assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62(5).					
(2) ENISA asigură secretariatului Grupului părților interesate pentru certificarea securității cibernetice, în temeiul articolului 22 alineatul (4).	(2) ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4).			Prevederi UE neaplicabile		

(3) ENISA compilează și publică orientări și dezvoltă bune practici în ceea ce privește cerințele în materie de securitate cibernetică pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate, în cooperare cu autoritățile naționale de certificare de securitate și cu industria, în cadrul unui proces oficial, standardizat și transparent.	(3) ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements for ICT products, ICT services, ICT processes and managed security services, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way.			Prevederi UE neaplicabile		
(4) ENISA contribuie la consolidarea capacităților în legătură cu procesele de evaluare și certificare prin compilarea și emiterea unor orientări, precum și oferind sprijin statelor membre, la cererea lor.	(4) ENISA shall contribute to capacity-building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request.			Prevederi UE neaplicabile		
(5) ENISA facilitează elaborarea și adoptarea de standarde europene și internaționale pentru gestionarea riscurilor și pentru securitatea produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate.	(5) ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services, ICT processes and managed security services.			Prevederi UE neaplicabile		
(6) ENISA elaborează, în colaborare cu statele membre și industria, 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.	(6) ENISA shall draw up, in collaboration with Member States and industry, advice and guidelines regarding the technical areas related to the security requirements for operators of essential services and digital service providers, as well as regarding already existing standards, including Member States' national standards, pursuant to Article 19(2) of Directive (EU) 2016/1148.			Prevederi UE neaplicabile		
(7) ENISA efectuează și disemnează analize periodice privind principalele tendințe de pe piața securității cibernetice, atât din punctul de vedere al	(7) ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides,			Prevederi UE neaplicabile		

cererii, cât și al ofertei, în vederea stimulării pieței securității cibernetice în cadrul Uniunii.	with a view to fostering the cybersecurity market in the Union.					
Articolul 9 **Cunoștințe și informare**	**Article 9** **Knowledge and information**					
ENISA: (a) efectuează analize ale tehnologiilor emergente și furnizează evaluări tematice privind impactul preconizat din punct de vedere societal, juridic, economic și de reglementare al inovațiilor tehnologice în materie de securitate cibernetică; (b) efectuează analize strategice pe termen lung ale amenințărilor cibernetice și incidentelor, pentru a identifica tendințele emergente și a contribui la prevenirea incidentelor; (c) în cooperare cu experți ai autorităților statelor membre și cu părțile interesate relevante, furnizează 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) culege, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea cibernetică furnizate de instituțiile, organele, oficiile și agențiile Uniunii și informații privind securitatea cibernetică	ENISA shall: (a) perform analyses of emerging technologies and provide topic-specific assessments on the expected societal, legal, economic and regulatory impact of technological innovations on cybersecurity; (b) perform long-term strategic analyses of cyber threats and incidents in order to identify emerging trends and help prevent incidents; (c) in cooperation with experts from Member States authorities and relevant stakeholders, provide advice, guidance and best practices for the security of network and information systems, in particular for the security of the infrastructures supporting the sectors listed in Annex II to Directive (EU) 2016/1148 and those used by the providers of the digital services listed in Annex III to that Directive; (d) through a dedicated portal, pool, organise and make available to the public information on cybersecurity provided by the Union institutions, bodies, offices and agencies and information on cybersecurity provided on a voluntary basis by Member States and private and public stakeholders; (e) collect and analyse publicly available information regarding significant incidents			Prevederi UE neaplicabile		

furnizate, în mod voluntar, de statele membre și de părțile interesate private și publice; (e) culege și analizează informațiile disponibile public cu privire la incidentele semnificative și compilează rapoarte, cu scopul de a oferi orientări pentru cetățenii, organizațiile și întreprinderile din întreaga Uniune.	and compile reports with a view to providing guidance to citizens, organisations and businesses across the Union.					
Articolul 10 **Sensibilizare și educare**	**Article 10** **Awareness-raising and education**					
ENISA: (a) sensibilizează publicul în legătură cu riscurile pentru securitatea cibernetică și oferă orientări cu privire la bune practici pentru utilizatorii individuali, inclusiv cu privire la igiena cibernetică și alfabetizarea cibernetică, destinate cetățenilor, organizațiilor și întreprinderilor; (b) în cooperare cu statele membre și cu instituțiile, organele, oficiile și agențiile Uniunii, precum și cu industria, organizează campanii periodice de informare pentru sporirea securității cibernetice și a vizibilității acesteia în Uniune și stimulează o amplă dezbatere publică; (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) susține coordonarea mai strânsă și schimbul de bune practici între statele membre	ENISA shall: (a) raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy; (b) in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate; (c) assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education; (d) support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education.			Prevederi UE neaplicabile		

privind sensibilizarea și educarea în domeniul securității cibernetice.						
Articolul 11 **Cercetare și inovare**	**Article 11** **Research and innovation**					
În ceea ce privește cercetarea și inovarea, ENISA: (a) consiliază instituțiile, organele, oficiile și agențiile Uniunii 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 cibernetice 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 conferit competențele relevante, la etapa de punere în aplicare a programelor de finanțare a cercetării și inovării sau în calitate de beneficiar al acestora. (c) contribuie la agenda strategică în privința cercetării și inovării în domeniul securității cibernetice la nivelul Uniunii.	In relation to research and innovation, ENISA shall: (a) advise the Union institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of cybersecurity, with a view to enabling effective responses to current and emerging risks and cyber threats, including with respect to new and emerging information and communications technologies, and with a view to using risk-prevention technologies effectively; (b) where the Commission has conferred the relevant powers on it, participate in the implementation phase of research and innovation funding programmes or as a beneficiary; (c) contribute to the strategic research and innovation agenda at Union level in the field of cybersecurity.			Prevederi UE neaplicabile		
Articolul 12 **Cooperarea internațională**	**Article 12** **International cooperation**					
ENISA contribuie la eforturile Uniunii de cooperare cu țări terțe și cu organizații internaționale, precum și în cadrele internaționale de cooperare relevante, pentru a promova cooperarea internațională privind aspecte legate de securitatea cibernetică prin:	ENISA shall contribute to the Union's efforts to cooperate with third countries and international organisations as well as within relevant international cooperation frameworks to promote international cooperation on			Prevederi UE neaplicabile		

(a)participarea ca observator la organizarea de exerciții internaționale și realizarea de analize și de rapoarte destinate consiliului de administrație privind rezultatele acestor exerciții, după caz; (b)facilitarea, la solicitarea Comisiei, a schimbului de bune practici; (c)furnizarea de expertiză Comisiei, la cererea acesteia; (d)consilierea și sprijinirea Comisiei în legătură cu chestiuni privind acorduri cu țări terțe pentru recunoașterea reciprocă a certificatelor de securitate cibernetică, în colaborare cu ECCG instituit în temeiul articolului 62.	issues related to cybersecurity, by: (a) where appropriate, engaging as an observer in the organisation of international exercises, and analysing and reporting to the Management Board on the outcome of such exercises; (b) at the request of the Commission, facilitating the exchange of best practices; (c) at the request of the Commission, providing it with expertise; (d) providing advice and support to the Commission on matters concerning agreements for the mutual recognition of cybersecurity certificates with third countries, in collaboration with the ECCG established under Article 62.					
CAPITOLUL III **Organizarea agenției**	**CHAPTER III** **Organisation of ENISA**					
Articolul 13 **Structura ENISA**	**Article 13** **Structure of ENISA**					
Structura administrativă și de conducere a ENISA este compusă din următoarele: (a)un consiliu de administrație; (b) un comitet executiv; (c) un director executiv; (d)un grup consultativ al ENISA; (e)o rețea a ofițerilor naționali de legătură.	The administrative and management structure of ENISA shall be composed of the following: (a) a Management Board; (b) an Executive Board; (c) an Executive Director; (d) an ENISA Advisory Group; (e) a National Liaison Officers Network.			Prevederi UE neaplicabile		
Secțiunea 1 **Consiliul de administrație**	**Section 1** **Management Board**					
Articolul 14 **Componența consiliului de administrație**	**Article 14** **Composition of the Management Board**					
(1) Consiliul de administrație este compus din câte un membru numit de fiecare stat membru, și din doi membri numiți de	(1) The Management Board shall be composed of one member appointed by each Member State, and two			Prevederi UE neaplicabile		

Comisie. Toți membrii au drept de vot.	members appointed by the Commission. All members shall have the right to vote.					
(2) Fiecare membru al consiliului de administrație are un supleant. Supleantul reprezintă membrul în absența acestuia din urmă.	(2) Each member of the Management Board shall have an alternate. That alternate shall represent the member in the member's absence.			Prevederi UE neaplicabile		
(3) Membrii consiliului de administrație și supleanții acestora sunt numiți pe baza cunoștințelor 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 din perspectiva genului în consiliul de administrație.	(3) Members of the Management Board and their alternates shall be appointed on the basis of their knowledge in the field of cybersecurity, taking into account their relevant managerial, administrative and budgetary skills. The Commission and the Member States shall make efforts to limit the turnover of their representatives on the Management Board, in order to ensure continuity of the Management Board's work. The Commission and the Member States shall aim to achieve gender balance on the Management Board.			Prevederi UE neaplicabile		
(4) Durata mandatului membrilor consiliului de administrație și al membrilor supleanți este de patru ani. Acest mandat se poate reînnoi.	(4) The term of office of the members of the Management Board and their alternates shall be four years. That term shall be renewable.			Prevederi UE neaplicabile		
Articolul 15 **Funcțiile consiliului de administrație**	**Article 15** **Functions of the Management Board**					
(1) Consiliul de administrație: (a)stabilește direcția generală de funcționare a ENISA și se asigură că ENISA funcționează în conformitate cu normele și principiile stabilite în prezentul regulament; acesta asigură în același timp coerența activității ENISA cu activitățile desfășurate de	(1) The Management Board shall: (a) establish the general direction of the operation of ENISA and ensure that ENISA operates in accordance with the rules and principles laid down in this Regulation; it shall also ensure the consistency of ENISA's work with activities conducted by			Prevederi UE neaplicabile		

statele membre și cu cele de la nivelul Uniunii; (b) adoptă proiectul de document unic de programare al ENISA menționat la articolul 24, înainte de transmiterea acestuia Comisiei spre avizare; (c) adoptă documentul unic de programare al ENISA, ținând seama de avizul Comisiei; (d) supraveghează punerea în aplicare a programării multianuale și anuale cuprinse în documentul unic de programare; (e) adoptă bugetul anual al ENISA și exercită alte funcții privind bugetul ENISA în conformitate cu capitolul IV; (f) evaluează și adoptă raportul anual consolidat privind activitățile ENISA, care include conturile ENISA și descrierea modului în care aceasta și-a atins indicatorii de performanță, transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi, până la data de 1 iulie a anului următor, atât raportul anual, cât și evaluarea acestuia, și publică raportul anual; (g) adoptă normele financiare aplicabile ENISA în conformitate cu articolul 32; (h) adoptă o strategie de combatere a fraudei care să fie proporțională cu riscurile de fraudă, ținând seama de analiza cost-beneficiu a măsurilor care urmează să fie puse în aplicare; (i) adoptă norme de prevenire și gestionare a conflictelor de interese în cazul membrilor săi;	the Member States as well as at Union level; (b) adopt ENISA's draft single programming document referred to in Article 24, before its submission to the Commission for an opinion; (c) adopt ENISA's single programming document, taking into account the Commission opinion; (d) supervise the implementation of the multiannual and annual programming included in the single programming document; (e) adopt the annual budget of ENISA and exercise other functions in respect of ENISA's budget in accordance with Chapter IV; (f) assess and adopt the consolidated annual report on ENISA's activities, including the accounts and a description of how ENISA has met its performance indicators, submit both the annual report and the assessment thereof by 1 July of the following year, to the European Parliament, to the Council, to the Commission and to the Court of Auditors, and make the annual report public; (g) adopt the financial rules applicable to ENISA in accordance with Article 32; (h) adopt an anti-fraud strategy that is proportionate to the fraud risks, having regard to a cost-benefit analysis of the measures to be implemented; (i) adopt rules for the prevention and management					

(j)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; (k)adoptă regulamentul de procedură, inclusiv norme pentru decizii provizorii privind delegarea unor atribuții specifice în temeiul articolului 19 alineatul (7); (l)exercită, în ceea ce privește personalul ENISA, competențele conferite autorității împuternicite să facă numiri și autorității abilitate să încheie contracte de muncă (denumite în continuare „competențele de autoritate împuternicită să facă numiri”) prin Statutul funcționarilor Uniunii Europene (Statutul funcționarilor) și Regimul aplicabil celorlalți agenți ai Uniunii Europene (Regimul aplicabil celorlalți agenți), stabilite prin Regulamentul (CEE, Euratom, CECO) nr. 259/68 al Consiliului ([24]), în conformitate cu alineatul (2) din prezentul articol; (m)adoptă norme de aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți în conformitate cu procedura prevăzută la articolul 110 din Statutul funcționarilor; (n)numește directorul executiv și, după caz, îi prelungește mandatul sau îl demite din funcție, în conformitate cu articolul 36;	of conflicts of interest in respect of its members; (j) ensure adequate follow-up to the findings and recommendations resulting from investigations of the European Anti-Fraud Office (OLAF) and the various internal or external audit reports and evaluations; (k) adopt its rules of procedure, including rules for provisional decisions on the delegation of specific tasks, pursuant to Article 19(7); (l) with respect to the staff of ENISA, exercise the powers conferred by the Staff Regulations of Officials (the ‘Staff Regulations of Officials’) and the Conditions of Employment of Other Servants of the European Union (the ‘Conditions of Employment of Other Servants’), laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 (2) on the appointing authority and on the Authority Empowered to Conclude a Contract of Employment (‘appointing authority powers’) in accordance with paragraph 2 of this Article; (m) adopt rules implementing the Staff Regulations of Officials and the Conditions of Employment of Other Servants in accordance with the procedure provided for in Article 110 of the Staff Regulations of Officials; (n) appoint the Executive Director and where relevant extend his or her term of office or remove him or her from					

(o)numește un contabil, care poate fi contabilul Comisiei și care este pe deplin independent în îndeplinirea îndatoririlor sale; (p)ia toate deciziile privind instituirea structurilor interne ale ENISA și, dacă este necesar, privind modificarea acestora, luând în considerare nevoile activității agenției și având în vedere buna gestiune bugetară; (q)autorizează stabilirea acordurilor de lucru în ceea ce privește articolul 7; (r)autorizează stabilirea sau încheierea acordurilor de lucru în conformitate cu articolul 42.	office in accordance with Article 36; (o) appoint an accounting officer, who may be the Commission's accounting officer, who shall be wholly independent in the performance of his or her duties; (p) take all decisions concerning the establishment of ENISA's internal structures and, where necessary, the modification of those internal structures, taking into consideration ENISA's activity needs and having regard to sound budgetary management; (q) authorise the establishment of working arrangements with regard to Article 7; (r) authorise the establishment or conclusion of working arrangements in accordance with Article 42.					
(2) În conformitate cu articolul 110 din Statutul funcționarilor, consiliul de administrație adoptă 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 stabilite condițiile în care această delegare de competențe poate fi suspendată. Directorul executiv poate să subdelege aceste competențe.	(2) In accordance with Article 110 of the Staff Regulations of Officials, the Management Board shall adopt a decision based on Article 2(1) of the Staff Regulations of Officials and Article 6 of the Conditions of Employment of Other Servants, delegating the relevant appointing authority powers to the Executive Director and determining the conditions under which that delegation of powers can be suspended. The Executive Director may sub-delegate those powers.			Prevederi UE neaplicabile		
(3) În cazul în care apar împrejurări excepționale care impun acest lucru, consiliul de administrație poate adopta o decizie pentru a suspenda	(3) Where exceptional circumstances so require, the Management Board may adopt a decision to temporarily suspend the delegation of			Prevederi UE neaplicabile		

temporar delegarea competențelor de autoritate împuternicită să facă numiri către directorul executiv și delegarea competențelor subdelegate de către directorul executiv și să le exercite el însuși sau să le delege unuia dintre membrii săi ori unui alt membru al personalului decât directorul executiv.	appointing authority powers to the Executive Director and any appointing authority powers sub-delegated by the Executive Director and instead exercise them itself or delegate them to one of its members or to a staff member other than the Executive Director.					
Articolul 16 **Președintele Consiliului de administrație**	**Article 16** **Chairperson of the Management Board**					
Consiliul de administrație alege cu o majoritate de două treimi din membrii săi un președinte și un vicepreședinte dintre membrii săi. Mandatul acestora este de patru ani și poate fi reînnoit 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 pe președinte din oficiu în cazul în care acesta din urmă nu își poate exercita prerogativele.	The Management Board shall elect a Chairperson and a Deputy Chairperson from among its members, by a majority of two thirds of the members. Their terms of office shall be four years, which shall be renewable once. If, however, their membership of the Management Board ends at any time during their term of office, their term of office shall automatically expire on that date. The Deputy Chair shall replace the Chairperson ex officio if the Chairperson is unable to attend to his or her duties.			Prevederi UE neaplicabile		
Articolul 17 **Reuniunile consiliului de administrație**	**Article 17** **Meetings of the Management Board**					
(1) Reuniunile consiliului de administrație sunt convocate de președintele acestuia.	(1) Meetings of the Management Board shall be convened by its Chairperson.			Prevederi UE neaplicabile		
(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 acestuia, a Comisiei sau la cererea a cel puțin o treime din membrii săi.	(2) The Management Board shall hold at least two ordinary meetings a year. It shall also hold extraordinary meetings at the request of its Chairperson, at the request of the Commission, or at the request of at least one third of its members.			Prevederi UE neaplicabile		

(3) Directorul executiv ia parte la ședințele consiliului de administrație, dar nu are drept de vot.	(3) The Executive Director shall take part in the meetings of the Management Board but shall not have the right to vote.			Prevederi UE neaplicabile		
(4) Membrii Grupului consultativ al ENISA pot lua parte la reuniunile consiliului de administrație, la invitația președintelui, dar nu au drept de vot.	(4) Members of the ENISA Advisory Group may take part in the meetings of the Management Board at the invitation of the Chairperson, but shall not have the right to vote.			Prevederi UE neaplicabile		
(5) Membrii consiliului de administrație și supleanții lor pot să fie asistați în cursul reuniunilor consiliului de administrație de consilieri sau de experți, sub rezerva regulamentului de procedură al consiliului de administrație.	(5) The members of the Management Board and their alternates may be assisted at the meetings of the Management Board by advisers or experts, subject to the rules of procedure of the Management Board.			Prevederi UE neaplicabile		
(6) ENISA asigură secretariatul consiliului de administrație.	(6) ENISA shall provide the secretariat of the Management Board.			Prevederi UE neaplicabile		
Articolul 18 **Regulile de vot ale consiliului de administrație**	**Article 18** **Voting rules of the Management Board**					
(1) Consiliul de administrație își adoptă deciziile cu majoritatea membrilor săi.	(1) The Management Board shall take its decisions by a majority of its members.			Prevederi UE neaplicabile		
(2) Pentru adoptarea documentului unic de programare și a bugetului anual, precum și pentru numirea, prelungirea mandatului sau demiterea din funcție a directorului executiv, este necesară o majoritate de două treimi din membrii consiliului de administrație.	(2) A majority of two-thirds of the members of the Management Board shall be required for the adoption of the single programming document and of the annual budget and for the appointment, extension of the term of office or removal of the Executive Director.			Prevederi UE neaplicabile		
(3) Fiecare membru dispune de un vot. În absența unui membru, dreptul său de vot poate fi exercitat de supleantul său.	(3) Each member shall have one vote. In the absence of a member, their alternate shall be entitled to exercise the member's right to vote.			Prevederi UE neaplicabile		
(4) Președintele consiliului de administrație participă la vot.	(4) The Chairperson of the Management Board shall take part in the voting.			Prevederi UE neaplicabile		

(5) Directorul executiv nu participă la vot.	(5) The Executive Director shall not take part in the voting.			Prevederi UE neaplicabile		
(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.	(6) The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member.			Prevederi UE neaplicabile		
Secțiunea 2 **Comitetul executiv**	**Section 2** **Executive Board**					
Articolul 19 **Comitetul executiv**	**Article 19** **Executive Board**					
(1) Consiliul de administrație este asistat de un comitet executiv.	(1) The Management Board shall be assisted by an Executive Board.			Prevederi UE neaplicabile		
(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 20, 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 20.	(2) The Executive Board shall: (a) prepare decisions to be adopted by the Management Board; (b) together with the Management Board, ensure the adequate follow-up to the findings and recommendations stemming from investigations of OLAF and the various internal or external audit reports and evaluations; (c) without prejudice to the responsibilities of the Executive Director set out in Article 20, assist and advise the Executive Director in implementing the decisions of the Management Board on administrative and budgetary matters pursuant to Article 20.			Prevederi UE neaplicabile		
(3) Comitetul executiv este format din cinci membri. Membrii comitetului executivi sunt numiți dintre membrii consiliului de administrație. Dintre membri, unul este președintele Consiliului de	(3) The Executive Board shall be composed of five members. The members of the Executive Board shall be appointed from among the members of the Management Board. One of the members shall be the			Prevederi UE neaplicabile		

administrație, care poate prezida și comitetul executiv, și unul este unul dintre reprezentanții Comisiei. Numirile membrilor comitetului executiv urmăresc asigurarea unei reprezentări echilibrate din perspectiva genului în comitetul executiv. Directorul executiv ia parte la reuniunile comitetului executiv, dar nu are drept de vot.	Chairperson of the Management Board, who may also chair the Executive Board, and another shall be one of the representatives of the Commission. The appointments of the members of the Executive Board shall aim to ensure gender balance on the Executive Board. The Executive Director shall take part in the meetings of the Executive Board but shall not have the right to vote.					
(4) Durata mandatului membrilor comitetului executiv este de patru ani. Acest mandat se poate reînnoi.	(4) The term of office of the members of the Executive Board shall be four years. That term shall be renewable.			Prevederi UE neaplicabile		
(5) Comitetul executiv se întrunește cel puțin o dată la trei luni. Președintele comitetului executiv convoacă reuniuni suplimentare la cererea membrilor săi.	(5) The Executive Board shall meet at least once every three months. The Chairperson of the Executive Board shall convene additional meetings at the request of its members.			Prevederi UE neaplicabile		
(6) Consiliul de administrație stabilește regulamentul de procedură al comitetului executiv.	(6) The Management Board shall lay down the rules of procedure of the Executive Board.			Prevederi UE neaplicabile		
(7) Atunci când este necesar din motive de urgență, comitetul executiv poate lua anumite decizii provizorii în numele consiliului de administrație, îndeosebi cu privire la aspecte legate de gestionarea administrativă, inclusiv la suspendarea delegării competențelor de autoritate împuternicită să facă numiri, precum și cu privire la aspecte bugetare. Astfel de decizii provizorii se notifică consiliului de administrație fără întârzieri nejustificate. Consiliul de administrație decide dacă aprobă sau respinge decizia provizorie în termen de cel mult trei luni de la luarea deciziei. Comitetul	(7) When necessary because of urgency, the Executive Board may take certain provisional decisions on behalf of the Management Board, in particular on administrative management matters, including the suspension of the delegation of the appointing authority powers and budgetary matters. Any such provisional decisions shall be notified to the Management Board without undue delay. The Management Board shall then decide whether to approve or reject the provisional decision no later than three months after the decision was taken. The			Prevederi UE neaplicabile		

executiv nu ia decizii în numele consiliului de administrație care necesită pentru aprobare o majoritate de două treimi din membrii consiliului de administrație.	Executive Board shall not take decisions on behalf of the Management Board that require the approval of a majority of two-thirds of the members of the Management Board.					
Secțiunea 3 **Directorul executiv**	**Section 3** **Executive Director**					
Articolul 20 **Responsabilitățile directorului executiv**	**Article 20** **Duties of the Executive Director**					
(1) ENISA este condusă de un director executiv care este independent în îndeplinirea atribuțiilor sale. Directorul executiv răspunde în fața consiliului de administrație.	(1) ENISA shall be managed by its Executive Director, who shall be independent in the performance of his or her duties. The Executive Director shall be accountable to the Management Board.			Prevederi UE neaplicabile		
(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.	(2) The Executive Director shall report to the European Parliament on the performance of his or her duties when invited to do so. The Council may invite the Executive Director to report on the performance of his or her duties.			Prevederi UE neaplicabile		
(3) Directorul executiv răspunde de: (a)administrarea curentă a ENISA; (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;	(3) The Executive Director shall be responsible for: (a) the day-to-day administration of ENISA; (b) implementing the decisions adopted by the Management Board; (c) preparing the draft single programming document and submitting it to the Management Board for approval before its submission to the Commission; (d) implementing the single programming document and reporting to the Management Board thereon; (e) preparing the consolidated annual report on ENISA's activities, including the			Prevederi UE neaplicabile		

(e)pregătirea raportului anual consolidat privind activitățile ENISA, inclusiv punerea în aplicare a programului anual de activitate al ENISA, 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, din doi în doi ani, a unui raport privind progresele înregistrate; (g)elaborarea unui plan de acțiune pentru a da curs concluziilor rapoartelor de audit intern sau extern, precum și a investigațiilor desfășurate de 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 ENISA, astfel cum se menționează la articolul 32; (i)întocmirea proiectului de situație a estimărilor de venituri și cheltuieli ale ENISA 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	implementation of ENISA's annual work programme, and presenting it to the Management Board for assessment and adoption; (f) preparing an action plan that follows up on the conclusions of the retrospective evaluations, and reporting on progress every two years to the Commission; (g) preparing an action plan that follows up on the conclusions of internal or external audit reports, as well as on investigations by OLAF and reporting on progress biannually to the Commission and regularly to the Management Board; (h) preparing the draft financial rules applicable to ENISA as referred to in Article 32; (i) preparing ENISA's draft statement of estimates of revenue and expenditure and implementing its budget; (j) protecting the financial interests of the Union by the application of preventive measures against fraud, corruption and any other illegal activities, by effective checks and, if irregularities are detected, by the recovery of the amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties; (k) preparing an anti-fraud strategy for ENISA and presenting it to the Management Board for approval; (l) developing and maintaining contact with the business					

eficace, proporționale și disuasive; (k) pregătirea unei strategii antifraudă pentru ENISA și prezentarea acesteia consiliului de administrație, spre adoptare; (l) stabilirea și menținerea contactului cu comunitatea de afaceri și cu organizațiile consumatorilor, în vederea asigurării unui dialog periodic cu părțile interesate relevante; (m) desfășurarea de schimburi periodice de opinii și de informații cu instituțiile, organele, oficiile și agențiile Uniunii în ceea ce privește activitățile lor referitoare la securitatea cibernetică, pentru a asigura coerența în dezvoltarea și punerea în aplicare a politicii Uniunii; (n) îndeplinirea altor atribuții care îi sunt încredințate directorului executiv prin prezentul regulament.	community and consumers' organisations to ensure regular dialogue with relevant stakeholders; (m) exchanging views and information regularly with Union institutions, bodies, offices and agencies regarding their activities relating to cybersecurity to ensure coherence in the development and the implementation of Union policy; (n) carrying out other tasks assigned to the Executive Director by this Regulation.					
(4) După caz, în limitele obiectivelor și atribuțiilor ENISA, directorul executiv poate înființa grupuri de lucru ad-hoc compuse din experți, inclusiv experți din rândul autorităților competente ale statelor membre. Directorul executiv informează în prealabil Consiliul de administrație cu privire la acest aspect. 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 ENISA.	(4) Where necessary and within ENISA's objectives and tasks, the Executive Director may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities. The Executive Director shall inform the Management Board in advance thereof. The procedures regarding in particular the composition of the working groups, the appointment of the experts of the working groups by the Executive Director and the operation of the working groups shall be specified in			Prevederi UE neaplicabile		

	ENISA's internal rules of operation.					
(5) Dacă este necesar, în scopul îndeplinirii atribuțiilor ENISA în 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 cere opinia statului membru sau a statelor membre în cauză, inclusiv a statului membru în care este situat sediul ENISA, și obține 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. Numărul total al personalului din toate birourile locale este păstrat la minimum și nu depășește 40 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA. Numărul personalului din fiecare birou local nu depășește 10 % din numărul total al personalului ENISA care se află în statul membru în care este situat sediul ENISA. Decizia de înființare a unui birou local precizează domeniul de aplicare al activităților care urmează să fie efectuate în cadrul respectivului birou local, astfel încât să se evite costurile inutile și dublarea funcțiilor administrative ale ENISA.	(5) Where necessary, for the purpose of carrying out ENISA's tasks in an efficient and effective manner and based on an appropriate cost-benefit analysis, the Executive Director may decide to establish one or more local offices in one or more Member States. Before deciding to establish a local office, the Executive Director shall seek the opinion of the Member States concerned, including the Member State in which the seat of ENISA is located, and shall obtain the prior consent of the Commission and the Management Board. In cases of disagreement during the consultation process between the Executive Director and the Member States concerned, the issue shall be brought to the Council for discussion. The aggregate number of staff in all local offices shall be kept to a minimum and shall not exceed 40 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The number of the staff in each local office shall not exceed 10 % of the total number of ENISA's staff located in the Member State in which the seat of ENISA is located. The decision establishing a local office shall specify the scope of the activities to be carried out at the local office in a manner that avoids unnecessary costs and			Prevederi UE neaplicabile		

	duplication of administrative functions of ENISA.					
Secțiunea 4 **Grupul consultativ al ENISA, grupul părților interesate pentru certificarea securității cibernetice și rețeaua ofițerilor naționali de legătură**	**Section 4** **ENISA Advisory Group, the Stakeholder Cybersecurity Certification Group and the National Liaison Officers Network**					
Articolul 21 **Grupul consultativ al ENISA**	**Article 21** **ENISA Advisory Group**					
(1) La propunerea directorului executiv, consiliul de administrație stabilește, în mod transparent, grupul consultativ al ENISA, alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi industria TIC, furnizorii de rețele comunicații electronice sau de servicii de destinate publicului, IMM-urile, operatorii de servicii esențiale, grupurile de consumatori, experții din mediul academic în domeniul securității cibernetice și reprezentanți ai autorităților competente notificate în conformitate cu Directiva (UE) 2018/1972, organizațiile de standardizare europene, precum și autoritățile de aplicare a legii și cele de supraveghere a protecției datelor. Consiliul de administrație depune eforturi pentru a asigura un echilibru adecvat din punct de vedere geografic și al genului, precum și un echilibru între diversele grupuri de părți interesate.	(1) The Management Board, acting on a proposal from the Executive Director, shall establish in a transparent manner the ENISA Advisory Group composed of recognised experts representing the relevant stakeholders, such as the ICT industry, providers of electronic communications networks or services available to the public, SMEs, operators of essential services, consumer groups, academic experts in the field of cybersecurity, and representatives of competent authorities notified in accordance with Directive (EU) 2018/1972, of European standardisation organisations, as well as of law enforcement and data protection supervisory authorities. The Management Board shall aim to ensure an appropriate gender and geographical balance as well as a balance between the different stakeholder groups.			Prevederi UE neaplicabile		
(2) Procedurile privind Grupul consultativ al ENISA, în special cele referitoare la componența sa, la propunerea directorului executiv menționată la alineatul (1), la numărul și numirea membrilor săi și la funcționarea	(2) Procedures for the ENISA Advisory Group, in particular regarding its composition, the proposal by the Executive Director referred to in paragraph 1, the number and appointment of its members			Prevederi UE neaplicabile		

grupului consultativ al ENISA, se detaliază în normele interne de funcționare ale ENISA și se fac publice.	and the operation of the ENISA Advisory Group, shall be specified in ENISA's internal rules of operation and shall be made public.					
(3) Grupul consultativ al ENISA este prezidat de directorul executiv sau de orice persoană numită de acesta de la caz la caz.	(3) The ENISA Advisory Group shall be chaired by the Executive Director or by any person whom the Executive Director appoints on a case-by-case basis.			Prevederi UE neaplicabile		
(4) Mandatul membrilor grupului consultativ al ENISA este de doi ani și jumătate. Membrii consiliului de administrație nu pot fi membri ai grupului consultativ al ENISA. Experții Comisiei și ai statelor membre au dreptul de a participa la reuniunile grupului consultativ al ENISA și la activitățile acestuia. Reprezentanții altor organisme considerate relevante de către directorul executiv, care nu au calitatea de membri ai grupului consultativ al ENISA, pot fi invitați să participe la reuniunile grupului consultativ al ENISA și la activitățile acestuia.	(4) The term of office of the members of the ENISA Advisory Group shall be two-and-a-half years. Members of the Management Board shall not be members of the ENISA Advisory Group. Experts from the Commission and the Member States shall be entitled to be present at the meetings of the ENISA Advisory Group and to participate in its work. Representatives of other bodies deemed to be relevant by the Executive Director, who are not members of the ENISA Advisory Group, may be invited to attend the meetings of the ENISA Advisory Group and to participate in its work.			Prevederi UE neaplicabile		
(5) Grupul consultativ al ENISA acordă consiliere ENISA în exercitarea atribuțiilor sale, cu excepția aplicării dispozițiilor titlului III din prezentul regulament. Acesta acordă consiliere în special directorului executiv în ceea ce privește elaborarea unei propuneri de program anual de activitate al ENISA și asigurarea comunicării cu părțile interesate relevante referitor la aspecte legate de programul anual de activitate.	(5) The ENISA Advisory Group shall advise ENISA in respect of the performance of ENISA's tasks, except of the application of the provisions of Title III of this Regulation. It shall in particular advise the Executive Director on the drawing up of a proposal for ENISA's annual work programme, and on ensuring communication with the relevant stakeholders on issues related to the annual work programme.			Prevederi UE neaplicabile		

(6) Grupul consultativ al ENISA informează periodic consiliul de administrație despre activitățile sale.	(6) The ENISA Advisory Group shall inform the Management Board of its activities on a regular basis.			Prevederi UE neaplicabile		
Articolul 22 **Grupul părților interesate pentru certificarea securității cibernetice**	**Article 22** **Stakeholder Cybersecurity Certification Group**					
(1) Se instituie Grupul părților interesate pentru certificarea securității cibernetice.	(1) The Stakeholder Cybersecurity Certification Group shall be established.			Prevederi UE neaplicabile		
(2) Grupul părților interesate pentru certificarea securității cibernetice este alcătuit din membri selecționați din rândul experților recunoscuți care reprezintă părți interesate relevante. Comisia selecționează membrii Grupului părților interesate pentru certificarea securității cibernetice pe baza unei propuneri din partea ENISA, printr-o cerere deschisă și transparentă care asigură echilibrul între diferitele grupuri de părți interesate, precum și un echilibru adecvat din punct de vedere geografic și al genului.	(2) The Stakeholder Cybersecurity Certification Group shall be composed of members selected from among recognised experts representing the relevant stakeholders. The Commission, following a transparent and open call, shall select, on the basis of a proposal from ENISA, members of the Stakeholder Cybersecurity Certification Group ensuring a balance between the different stakeholder groups as well as an appropriate gender and geographical balance.			Prevederi UE neaplicabile		
(3) Grupul părților interesate pentru certificarea securității cibernetice are următoarele atribuții: (a)să acorde Comisiei consiliere în legătură cu aspecte strategice referitoare la cadrul european de certificare a securității cibernetice; (b)la cerere, să acorde consiliere ENISA în legătură cu chestiuni generale și strategice referitoare la atribuțiile ENISA în legătură cu piața, certificarea securității cibernetice și standardizarea; (c)să asiste Comisia la pregătirea programul de activitate	(3) The Stakeholder Cybersecurity Certification Group shall: (a) advise the Commission on strategic issues regarding the European cybersecurity certification framework; (b) upon request, advise ENISA on general and strategic matters concerning ENISA's tasks relating to market, cybersecurity certification, and standardisation; (c) assist the Commission in the preparation of the Union rolling work programme referred to in Article 47;			Prevederi UE neaplicabile		

etapizat la nivelul Uniunii menționat la articolul 47; (d)să emită un aviz referitor la programul de activitate etapizat la nivelul Uniunii în temeiul articolului 47 alineatul (4); și (e)în cazuri urgente, să acorde consiliere Comisiei și ECCG în legătură cu necesitatea unor sisteme de certificare suplimentare față de cele incluse în programul de activitate etapizat la nivelul Uniunii, astfel cum se menționează la articolele 47 și 48.	(d) issue an opinion on the Union rolling work programme pursuant to Article 47(4); and (e) in urgent cases, provide advice to the Commission and the ECCG on the need for additional certification schemes not included in the Union rolling work programme, as outlined in Articles 47 and 48.					
(4) Grupul părților interesate pentru certificarea securității cibernetice este coprezidat de reprezentanții Comisiei și ai ENISA, iar secretariatul acestuia este asigurat de ENISA.	(4) The Stakeholder Certification Group shall be co-chaired by the representatives of the Commission and of ENISA, and its secretariat shall be provided by ENISA.			Prevederi UE neaplicabile		
Articolul 23 **Rețeaua ofițerilor naționali de legătură**	**Article 23** **National Liaison Officers Network**					
(1) Consiliul de administrație, acționând la propunerea directorului executiv, instituie o rețea a ofițerilor naționali de legătură, formată din reprezentanți ai tuturor statelor membre (ofițeri naționali de legătură). Fiecare stat membru numește un reprezentant în rețeaua ofițerilor naționali de legătură. Reuniunile rețelei ofițerilor naționali de legătură pot fi ținute în diverse configurații ale experților dintr-un anumit domeniu.	(1) The Management Board, acting on a proposal from the Executive Director, shall set up a National Liaison Officers Network composed of representatives of all Member States (National Liaison Officers). Each Member State shall appoint one representative to the National Liaison Officers Network. The meetings of the National Liaison Officers Network may be held in different expert formations.			Prevederi UE neaplicabile		
(2) Rețeaua ofițerilor naționali de legătură facilitează în special schimbul de informații între ENISA și statele membre și sprijină ENISA la diseminarea	(2) The National Liaison Officers Network shall in particular facilitate the exchange of information between ENISA and the			Prevederi UE neaplicabile		

activităților, constatărilor și recomandărilor sale părților interesate relevante din întreaga Uniune.	Member States, and shall support ENISA in disseminating its activities, findings and recommendations to the relevant stakeholders across the Union.					
(3) Ofițerii naționali de legătură acționează drept punct de contact la nivel național pentru a facilita cooperarea între ENISA și experții naționali în contextul punerii în aplicare a programului anual de activitate al ENISA.	(3) National Liaison Officers shall act as a point of contact at national level to facilitate cooperation between ENISA and national experts in the context of the implementation of ENISA's annual work programme.			Prevederi UE neaplicabile		
(4) Deși ofițerii naționali de legătură cooperează strâns cu reprezentanții statelor membre respective în cadrul consiliului de administrație, rețeaua ofițerilor naționali de legătură înșiși nu dublează activitatea consiliului de administrație, și nici a altor foruri ale Uniunii.	(4) While National Liaison Officers shall cooperate closely with the Management Board representatives of their respective Member States, the National Liaisons Officers Network itself shall not duplicate the work of the Management Board or of other Union forums.			Prevederi UE neaplicabile		
(5) Funcțiile și procedurile pentru rețeaua ofițerilor naționali de legătură sunt specificate în normele interne de funcționare ale ENISA și se fac publice.	(5) The functions and procedures of the National Liaisons Officers Network shall be specified in ENISA's internal rules of operation and shall be made public.			Prevederi UE neaplicabile		
Secțiunea 5 Funcționare	**Section 5 Operation**					
Articolul 24 Documentul unic de programare	**Article 24 Single programming document**					
(1) ENISA 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.	(1) ENISA shall operate in accordance with a single programming document containing its annual and multiannual programming, which shall include all of its planned activities.			Prevederi UE neaplicabile		
(2) În fiecare an, directorul executiv elaborează un proiect de document unic de programare care conține programarea anuală și multianuală cu planificarea	(2) Each year, the Executive Director shall draw up a draft single programming document containing its annual and multiannual programming			Prevederi UE neaplicabile		

corespunzătoare a resurselor financiare și umane în conformitate cu articolul 32 din Regulamentul delegat (UE) nr. 1271/2013 al Comisiei (25) și luând în considerare orientările stabilite de Comisie.	with the corresponding financial and human resources planning in accordance with Article 32 of Commission Delegated Regulation (EU) No 1271/2013 (1) and taking into account the guidelines set by the Commission.					
(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 până la data de 31 ianuarie a anului următor, împreună cu orice altă versiune ulterioară actualizată a documentului respectiv.	(3) By 30 November each year, the Management Board shall adopt the single programming document referred to in paragraph 1 and shall transmit it to the European Parliament, to the Council and to the Commission by 31 January of the following year, as well as any subsequently updated versions of that document.			Prevederi UE neaplicabile		
(4) Documentul unic de programare se definitivează după adoptarea definitivă a bugetului general al Uniunii și, dacă este necesar, se ajustează în mod corespunzător.	(4) The single programming document shall become final after the definitive adoption of the general budget of the Union and shall be adjusted as necessary.			Prevederi UE neaplicabile		
(5) Programul anual de activitate cuprinde obiectivele detaliate și rezultatele preconizate, inclusiv indicatorii de performanță. Acesta include și 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 atribuțiile care au fost adăugate, modificate sau eliminate față de exercițiul financiar precedent.	(5) The annual work programme shall comprise detailed objectives and expected results including performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be coherent with the multiannual work programme referred to in paragraph 7. It shall clearly indicate tasks that have been added, changed or deleted in comparison with the previous financial year.			Prevederi UE neaplicabile		

(6) Consiliul de administrație modifică programul anual de activitate adoptat atunci când o nouă atribuție este încredințată ENISA. 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 îi delege directorului executiv competența de a aduce modificări nesubstanțiale programului anual de activitate.	(6) The Management Board shall amend the adopted annual work programme when a new task is assigned to ENISA. Any substantial amendments to the annual work programme shall be adopted by the same procedure as for the initial annual work programme. The Management Board may delegate the power to make non-substantial amendments to the annual work programme to the Executive Director.			Prevederi UE neaplicabile		
(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.	(7) The multiannual work programme shall set out the overall strategic programming including objectives, expected results and performance indicators. It shall also set out the resource programming including multiannual budget and staff.			Prevederi UE neaplicabile		
(8) Programarea resurselor se actualizează anual. Programarea strategică se actualizează după caz, în special pentru a ține seama de rezultatul evaluării menționate la articolul 67.	(8) The resource programming shall be updated annually. The strategic programming shall be updated where appropriate and in particular where necessary to address the outcome of the evaluation referred to in Article 67.			Prevederi UE neaplicabile		
Articolul 25 **Declarația de interese**	**Article 25** **Declaration of interests**					
(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 menționează 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	(1) Members of the Management Board, the Executive Director, and officials seconded by Member States on a temporary basis, shall each make a declaration of commitments and a declaration indicating the absence or presence of any direct or indirect interest which might be considered to be prejudicial to their independence. The declarations shall be accurate			Prevederi UE neaplicabile		

se actualizează ori de câte ori este nevoie.	and complete, shall be made annually in writing, and shall be updated whenever necessary.					
(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.	(2) Members of the Management Board, the Executive Director, and external experts participating in ad hoc working groups, shall each accurately and completely declare, at the latest at the start of each meeting, any interest which might be considered to be prejudicial to their independence in relation to the items on the agenda, and shall abstain from participating in the discussion of and voting on such items.			Prevederi UE neaplicabile		
(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice pentru normele referitoare la declarațiile de interese menționate la alineatele (1) și (2).	(3) ENISA shall lay down, in its internal rules of operation, the practical arrangements for the rules on declarations of interest referred to in paragraphs 1 and 2.			Prevederi UE neaplicabile		
Articolul 26 **Transparență**	**Article 26** **Transparency**					
(1) ENISA își desfășoară activitățile cu un nivel ridicat de transparență și în conformitate cu articolul 28.	(1) ENISA shall carry out its activities with a high level of transparency and in accordance with Article 28.			Prevederi UE neaplicabile		
(2) ENISA 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 25.	(2) ENISA shall ensure that the public and any interested parties are provided with appropriate, objective, reliable and easily accessible information, in particular with regard to the results of its work. It shall also make public the declarations of interest made in accordance with Article 25.			Prevederi UE neaplicabile		
(3) Consiliul de administrație, pe baza unei propuneri din partea directorului executiv, poate autoriza părțile interesate să	(3) The Management Board, acting on a proposal from the Executive Director, may authorise interested parties to			Prevederi UE neaplicabile		

participe ca observatori la unele dintre activitățile ENISA.	observe the proceedings of some of ENISA's activities.					
(4) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor privind transparența menționate la alineatele (1) și (2).	(4) ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the transparency rules referred to in paragraphs 1 and 2.			Prevederi UE neaplicabile		
Articolul 27 Confidențialitate	**Article 27 Confidentiality**					
(1) Fără a aduce atingere articolului 28, ENISA 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.	(1) Without prejudice to Article 28, ENISA shall not divulge to third parties information that it processes or receives in relation to which a reasoned request for confidential treatment has been made.			Prevederi UE neaplicabile		
(2) Membrii consiliului de administrație, directorul executiv, membrii Grupului consultativ al ENISA, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului ENISA, inclusiv funcționarii detașați temporar de statele membre, respectă cerințele de confidențialitate prevăzute la articolul 339 din TFUE, chiar și după încetarea atribuțiilor lor.	(2) Members of the Management Board, the Executive Director, the members of the ENISA Advisory Group, external experts participating in ad hoc working groups, and members of the staff of ENISA, including officials seconded by Member States on a temporary basis, shall comply with the confidentiality requirements of Article 339 TFEU, even after their duties have ceased.			Prevederi UE neaplicabile		
(3) ENISA stabilește, în regulamentul său intern de funcționare, modalitățile practice de punere în aplicare a normelor de confidențialitate menționate la alineatele (1) și (2).	(3) ENISA shall lay down, in its internal rules of operation, the practical arrangements for implementing the confidentiality rules referred to in paragraphs 1 and 2.			Prevederi UE neaplicabile		
(4) Dacă este necesar pentru realizarea atribuțiilor ENISA, consiliul de administrație decide să acorde ENISA permisiunea de a gestiona informații clasificate. În acest caz, ENISA, cu acordul serviciilor Comisiei, adoptă	(4) If required for the performance of ENISA's tasks, the Management Board shall decide to allow ENISA to handle classified information. In that case ENISA, in agreement with the			Prevederi UE neaplicabile		

norme de securitate care să aplice principiile de securitate cuprinse în Deciziile (UE, Euratom) 2015/443 (26) și 2015/444 (27) ale Comisiei. Respectivele norme de securitate includ dispoziții privind schimbul, prelucrarea și stocarea informațiilor clasificate.	Commission services, shall adopt security rules applying the security principles set out in Commission Decisions (EU, Euratom) 2015/443 (1) and 2015/444 (2). Those security rules shall include provisions for the exchange, processing and storage of classified information.					
Articolul 28 **Accesul la documente**	**Article 28** **Access to documents**					
(1) Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de ENISA.	(1) Regulation (EC) No 1049/2001 shall apply to documents held by ENISA.			Prevederi UE neaplicabile		
(2) Consiliul de administrație adoptă modalitățile de punere în aplicare a Regulamentului (CE) nr. 1049/2001 până la 28 decembrie 2019.	(2) The Management Board shall adopt arrangements for implementing Regulation (EC) No 1049/2001 by 28 December 2019.			Prevederi UE neaplicabile		
(3) Deciziile adoptate de ENISA în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului European în temeiul articolului 228 din TFUE sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene în temeiul articolului 263 din TFUE.	(3) Decisions taken by ENISA pursuant to Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman under Article 228 TFEU or of an action before the Court of Justice of the European Union under Article 263 TFEU.			Prevederi UE neaplicabile		
CAPITOLUL IV **Întocmirea și structura bugetului ENISA**	**CHAPTER IV** **Establishment and structure of ENISA's budget**					
Articolul 29 **Întocmirea bugetului ENISA**	**Article 29** **Establishment of ENISA's budget**					
(1) În fiecare an, directorul executiv întocmește un proiect de situație a estimărilor de venituri și cheltuieli ale ENISA pentru următorul exercițiu financiar și îl transmite consiliului de administrație, împreună cu un proiect de schemă de personal. Se asigură	(1) Each year, the Executive Director shall draw up a draft statement of estimates of ENISA's revenue and expenditure for the following financial year, and shall transmit it to the Management Board, together with a draft establishment plan. Revenue			Prevederi UE neaplicabile		

un echilibru între venituri și cheltuieli.	and expenditure shall be in balance.					
(2) În fiecare an, pe baza proiectului de situație a estimărilor, consiliul de administrație adoptă situația estimărilor de venituri și cheltuieli ale ENISA pentru următorul exercițiu financiar.	(2) Each year the Management Board, on the basis of the draft statement of estimates, shall produce a statement of estimates of ENISA's revenue and expenditure for the following financial year.			Prevederi UE neaplicabile		
(3) În fiecare an, până la data de 31 ianuarie, consiliul de administrație transmite situația estimărilor, care face parte din documentul unic de programare, Comisiei și țărilor terțe cu care Uniunea a încheiat acorduri astfel cum se menționează la articolul 42 alineatul (2).	(3) The Management Board, by 31 January each year, shall send the statement of estimates, which shall be part of the draft single programming document, to the Commission and the third countries with which the Union has concluded agreements as referred to in Article 42(2).			Prevederi UE neaplicabile		
(4) Pe baza situației estimărilor, Comisia înscrie în proiectul de buget general al Uniunii estimările pe care le consideră necesare pentru schema de personal și valoarea contribuției care urmează să fie suportată din bugetul general al Uniunii, pe care le prezintă Parlamentului European și Consiliului în conformitate cu articolul 314 din TFUE.	(4) On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates it deems to be necessary for the establishment plan and the amount of the contribution to be charged to the general budget of the Union, which it shall submit to the European Parliament and to the Council in accordance with Article 314 TFEU.			Prevederi UE neaplicabile		
(5) Parlamentul European și Consiliul autorizează creditele reprezentând contribuția Uniunii alocată ENISA.	(5) The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to ENISA.			Prevederi UE neaplicabile		
(6) Parlamentul European și Consiliul adoptă schema de personal a ENISA.	(6) The European Parliament and the Council shall adopt ENISA's establishment plan.			Prevederi UE neaplicabile		
(7) Consiliul de administrație adoptă bugetul ENISA odată cu documentul unic de programare. Bugetul ENISA se definitivează după adoptarea definitivă a bugetului general al Uniunii.	(7) The Management Board shall adopt ENISA's budget together with the single programming document. ENISA's budget shall become final following the definitive			Prevederi UE neaplicabile		

Dacă este necesar, consiliul de administrație ajustează bugetul ENISA și documentul unic de programare în conformitate cu bugetul general al Uniunii.	adoption of the general budget of the Union. Where necessary, the Management Board shall adjust ENISA's budget and single programming document in accordance with the general budget of the Union.					
Articolul 30 **Structura bugetului ENISA**	**Article 30** **Structure of ENISA's budget**					
(1) Fără a aduce atingere altor resurse, veniturile ENISA sunt alcătuite astfel: (a)dintr-o contribuție de la bugetul general al Uniunii; (b)din venituri alocate unor cheltuieli specifice în conformitate cu normele sale financiare menționate la articolul 32; (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 32 și cu dispozițiile instrumentelor relevante care sprijină politicile Uniunii; (d)din eventuale contribuții din partea țărilor terțe care participă la lucrările ENISA, astfel cum se menționează la articolul 42; (e)din orice contribuție voluntară din partea statelor membre, în bani sau în natură. Statele membre care oferă contribuții voluntare în temeiul primului paragraf litera (e) nu pot solicita niciun drept sau serviciu specific ca rezultat al acelor contribuții.	(1) Without prejudice to other resources, ENISA's revenue shall be composed of: (a) a contribution from the general budget of the Union; (b) revenue assigned to specific items of expenditure in accordance with its financial rules referred to in Article 32; (c) Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 32 and with the provisions of the relevant instruments supporting the policies of the Union; (d) contributions from third countries participating in the work of ENISA as referred to in Article 42; (e) any voluntary contributions from Member States in money or in kind. Member States that provide voluntary contributions under point (e) of the first subparagraph shall not claim any specific right or service as a result thereof.			Prevederi UE neaplicabile		
(2) Cheltuielile ENISA cuprind cheltuieli cu personalul, cheltuieli administrative și de suport tehnic, cheltuieli cu infrastructura și operaționale,	(2) The expenditure of ENISA shall include staff, administrative and technical support, infrastructure and operational expenses, and			Prevederi UE neaplicabile		

precum și cheltuieli rezultate din contracte cu părți terțe.	expenses resulting from contracts with third parties.					
Articolul 31 **Execuția bugetară a ENISA**	**Article 31** **Implementation of ENISA's budget**					
(1) Directorul executiv răspunde de execuția bugetului ENISA.	(1) The Executive Director shall be responsible for the implementation of ENISA's budget.			Prevederi UE neaplicabile		
(2) Auditorul intern al Comisiei exercită asupra ENISA aceleași prerogative ca și asupra serviciilor Comisiei.	(2) The Commission's internal auditor shall exercise the same powers over ENISA as over Commission departments.			Prevederi UE neaplicabile		
(3) Contabilul ENISA trimite conturile provizorii contabilului Comisiei și Curții de Conturi pentru exercițiul financiar (exercițiul N) până la data de 1 martie a următorului exercițiu financiar (exercițiul N + 1).	(3) ENISA's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).			Prevederi UE neaplicabile		
(4) După primirea observațiilor formulate de Curtea de Conturi privind conturile provizorii ale ENISA în temeiul articolului 246 din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului [(28)], contabilul ENISA întocmește conturile finale ale ENISA pe răspunderea sa și le prezintă consiliului de administrație în vederea avizării.	(4) Upon the receipt of the Court of Auditors' observations on ENISA's provisional accounts pursuant to Article 246 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (1), ENISA's accounting officer shall draw up ENISA's final accounts under his or her responsibility and shall submit them to the Management Board for an opinion.			Prevederi UE neaplicabile		
(5) Consiliul de administrație emite un aviz cu privire la conturile finale ale ENISA.	(5) The Management Board shall deliver an opinion on ENISA's final accounts.			Prevederi UE neaplicabile		
(6) Până la data de 31 martie a exercițiului N + 1, directorul executiv transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi raportul privind gestiunea bugetară și financiară.	(6) By 31 March of year N + 1, the Executive Director shall transmit the report on the budgetary and financial management to the European Parliament, to the Council, to the Commission and to the Court of Auditors.			Prevederi UE neaplicabile		

(7) Până la data de 1 iulie a exercițiului N + 1, contabilul ENISA transmite Parlamentului European, Consiliului, contabilului Comisiei și Curții de Conturi conturile finale ale ENISA, împreună cu avizul consiliului de administrație.	(7) By 1 July of year N + 1, ENISA's accounting officer shall transmit ENISA's final accounts to the European Parliament, to the Council, to the Commission's accounting officer and to the Court of Auditors, together with the Management Board's opinion.			Prevederi UE neaplicabile		
(8) La aceeași dată la care transmite conturile finale ale ENISA, contabilul ENISA transmite, de asemenea, Curții de Conturi și, în copie, contabilului Comisiei, o scrisoare cuprinzând declarațiile conducerii cu privire la conturile finale respective.	(8) At the same date as the transmission of ENISA's final accounts, ENISA's accounting officer shall also send to the Court of Auditors a representation letter covering those final accounts, with a copy to the Commission's accounting officer.			Prevederi UE neaplicabile		
(9) Până la data de 15 noiembrie a exercițiului N + 1, directorul executiv publică conturile finale ale ENISA în Jurnalul Oficial al Uniunii Europene.	(9) By 15 November of year N + 1, the Executive Director shall publish ENISA's final accounts in the Official Journal of the European Union.			Prevederi UE neaplicabile		
(10) Până la data de 30 septembrie a exercițiului N + 1, directorul executiv transmite Curții de Conturi un răspuns la observațiile acesteia și transmite, de asemenea, o copie a răspunsului respectiv consiliului de administrație și Comisiei.	(10) By 30 September of year N + 1, the Executive Director shall send the Court of Auditors a reply to its observations and shall also send a copy of that reply to the Management Board and to the Commission.			Prevederi UE neaplicabile		
(11) Directorul executiv prezintă Parlamentului European, la cererea acestuia, orice informații necesare pentru buna desfășurare a procedurii de descărcare de gestiune pentru exercițiul financiar în cauză în conformitate cu articolului 261 alineatul (3) din Regulamentul (UE, Euratom) 2018/1046.	(11) The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for the financial year concerned in accordance with Article 261(3) of Regulation (EU, Euratom) 2018/1046.			Prevederi UE neaplicabile		
(12) La recomandarea Consiliului, Parlamentul European acordă, înaintea datei de 15 mai a exercițiului N + 2,	(12) On a recommendation from the Council, the European Parliament shall, before 15 May of year N + 2,			Prevederi UE neaplicabile		

descărcarea de gestiune directorului executiv în ceea ce privește execuția bugetului pentru exercițiul N.	give a discharge to the Executive Director in respect of the implementation of the budget for the year N.					
Articolul 32 **Reglementări financiare**	**Article 32** **Financial rules**					
Normele financiare aplicabile ENISA se adoptă de către consiliul de administrație după consultarea Comisiei. Acestea nu derogă de la Regulamentul delegat (UE) nr. 1271/2013, cu excepția cazului o astfel de derogare se impune în mod special pentru funcționarea ENISA, iar Comisia și-a dat acordul prealabil.	The financial rules applicable to ENISA shall be adopted by the Management Board after consulting the Commission. They shall not depart from Delegated Regulation (EU) No 1271/2013 unless such a departure is specifically required for the operation of ENISA and the Commission has given its prior consent.			Prevederi UE neaplicabile		
Articolul 33 **Combaterea fraudei**	**Article 33** **Combating fraud**					
(1) Pentru a facilita combaterea fraudei, a corupției și a altor activități ilegale, în temeiul Regulamentului (UE, Euratom) nr. 883/2013 al Parlamentului European și al Consiliului ([29]), până la 10 decembrie 2019, ENISA aderă la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene și Comisia Comunităților Europene privind investigațiile interne desfășurate de Oficiul European de Luptă Antifraudă (OLAF) ([30]). ENISA adoptă dispozițiile corespunzătoare care se aplică tuturor angajaților ENISA, folosind modelul prevăzut în anexa la respectivul acord.	(1) 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF) (2). ENISA shall adopt appropriate provisions applicable to all employees of ENISA, using the template set out in the Annex to that Agreement.			Prevederi UE neaplicabile		
(2) Curtea de Conturi are competența de a-i audita, pe baza documentelor și a inspecțiilor la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții care au primit fonduri ale Uniunii din partea ENISA.	(2) The Court of Auditors shall have the power of audit, on the basis of documents and of on-the-spot inspections, over all grant beneficiaries, contractors and subcontractors who have received Union funds from ENISA.			Prevederi UE neaplicabile		

(3) OLAF poate efectua investigații, inclusiv controale și inspecții la fața locului, în conformitate cu dispozițiile și procedurile prevăzute în Regulamentul nr. 883/2013 și în Regulamentul (Euratom, CE) nr. 2185/96 al Consiliului ([31]), pentru 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 ENISA.	(3) OLAF may carry out investigations, including on-the-spot checks and inspections, in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and Council Regulation (Euratom, EC) No 2185/96 (3), with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract funded by ENISA.			Prevederi UE neaplicabile		
(4) Fără a aduce atingere alineatelor (1), (2) și (3), acordurile de cooperare cu țările terțe sau cu organizațiile internaționale, contractele, acordurile de grant și deciziile de acordare a unui grant ale ENISA conțin dispoziții care împuternicesc în mod expres Curtea de Conturi și OLAF să efectueze astfel de audituri și investigații, în conformitate cu competențele care le revin.	(4) Without prejudice to paragraphs 1, 2 and 3, cooperation agreements with third countries or international organisations, contracts, grant agreements and grant decisions of ENISA shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct such audits and investigations, according to their respective competences.			Prevederi UE neaplicabile		
CAPITOLUL V **Personalul**	**CHAPTER V** **Staff**					
Articolul 34 **Dispoziții generale**	**Article 34** **General provisions**					
Personalului ENISA i se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți, precum și normele adoptate de comun acord de instituțiile Uniunii pentru punerea în aplicare a Statutului funcționarilor și a Regimului aplicabil celorlalți agenți.	The Staff Regulations of Officials and the Conditions of Employment of Other Servants, as well as the rules adopted by agreement between the Union institutions for giving effect to the Staff Regulations of Officials and the Conditions of Employment of Other Servants shall apply to the staff of ENISA.			Prevederi UE neaplicabile		
Articolul 35 **Privilegii și imunități**	**Article 35** **Privileges and immunity**					

Protocolul nr. 7 privind privilegiile și imunitățile Uniunii Europene, anexat la TUE și la TFUE, se aplică ENISA și personalului acesteia.	Protocol No 7 on the privileges and immunities of the European Union, annexed to the TEU and to the TFEU, shall apply to ENISA and its staff.			Prevederi UE neaplicabile		
Articolul 36 **Directorul executiv**	**Article 36** **Executive Director**					
(1) Directorul executiv este angajat ca agent temporar al ENISA în temeiul articolului 2 litera (a) din Regimul aplicabil celorlalți agenți.	(1) The Executive Director shall be engaged as a temporary agent of ENISA under point (a) of Article 2 of the Conditions of Employment of Other Servants.			Prevederi UE neaplicabile		
(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.	(2) The Executive Director shall be appointed by the Management Board from a list of candidates proposed by the Commission, following an open and transparent selection procedure.			Prevederi UE neaplicabile		
(3) În scopul încheierii contractului de muncă al directorului executiv, ENISA este reprezentată de președintele Consiliului de administrație.	(3) For the purpose of concluding the employment contract with the Executive Director, ENISA shall be represented by the Chairperson of the Management Board.			Prevederi UE neaplicabile		
(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 adresate de membrii acesteia.	(4) Before appointment, the candidate selected by the Management Board shall be invited to make a statement before the relevant committee of the European Parliament and to answer Members' questions.			Prevederi UE neaplicabile		
(5) Durata mandatului directorului executiv este de cinci ani. Până la sfârșitul perioadei respective, Comisia realizează o evaluare a rezultatelor obținute de directorul executiv și viitoarele atribuții și provocări ale ENISA.	(5) The term of office of the Executive Director shall be five years. By the end of that period, the Commission shall carry out an assessment of the performance of the Executive Director and ENISA's future tasks and challenges.			Prevederi UE neaplicabile		
(6) Consiliul de administrație adoptă deciziile privind numirea, prelungirea mandatului sau demiterea din funcție a	(6) The Management Board shall reach decisions on appointment, extension of the term of office or removal from			Prevederi UE neaplicabile		

directorului executiv în conformitate cu articolul 18 alineatul (2).	office of the Executive Director in accordance with Article 18(2).					
(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 o perioadă de cinci ani.	(7) The Management Board, acting on a proposal from the Commission which takes into account the assessment referred to in paragraph 5, may extend the term of office of the Executive Director once by five years.			Prevederi UE neaplicabile		
(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 precedă prelungirea mandatului său, directorul executiv, dacă este invitat, face o declarație în fața comisiei relevante a Parlamentului European și răspunde întrebărilor deputaților.	(8) The Management Board shall inform the European Parliament about its intention to extend the Executive Director's term of office. Within three months before any such extension, the Executive Director, if invited, shall make a statement before the relevant committee of the European Parliament and answer Members' questions.			Prevederi UE neaplicabile		
(9) Un director executiv al cărui mandat a fost prelungit nu poate să participe la o nouă procedură de selecție pentru același post.	(9) An Executive Director whose term of office has been extended shall not participate in another selection procedure for the same post.			Prevederi UE neaplicabile		
(10) Directorul executiv poate fi demis din funcție numai printr-o decizie a consiliului de administrație care acționează la propunerea Comisiei.	(10) The Executive Director may be removed from office only by decision of the Management Board acting on a proposal from the Commission.			Prevederi UE neaplicabile		
Articolul 37 **Experții naționali detașați și alte categorii de personal**	**Article 37** **Seconded national experts and other staff**					
(1) ENISA poate face apel la experți naționali detașați sau alte categorii de personal care nu sunt angajați ai ENISA. Acestor categorii de personal nu li se aplică Statutul funcționarilor și Regimul aplicabil celorlalți agenți.	(1) ENISA may make use of seconded national experts or other staff not employed by ENISA. The Staff Regulations of Officials and the Conditions of Employment of Other Servants shall not apply to such staff.			Prevederi UE neaplicabile		
(2) Consiliul de administrație adoptă o decizie de stabilire a	(2) The Management Board shall adopt a decision laying			Prevederi UE neaplicabile		

normelor aplicabile detașării experților naționali la ENISA.	down rules on the secondment of national experts to ENISA.					
CAPITOLUL VI **Dispoziții generale privind ENISA**	**CHAPTER VI** **General provisions concerning ENISA**					
Articolul 38 **Statutul juridic al ENISA**	**Article 38** **Legal status of ENISA**					
(1) ENISA este un organ al Uniunii și are personalitate juridică.	(1) ENISA shall be a body of the Union and shall have legal personality.			Prevederi UE neaplicabile		
(2) În fiecare stat membru, ENISA dispune de cea mai extinsă capacitate juridică acordată persoanelor juridice în temeiul dreptului intern. Aceasta poate, în special, să dobândească sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare.	(2) In each Member State ENISA shall enjoy the most extensive legal capacity accorded to legal persons under national law. It may, in particular, acquire or dispose of movable and immovable property and be a party to legal proceedings.			Prevederi UE neaplicabile		
(3) ENISA este reprezentată de directorul său executiv.	(3) ENISA shall be represented by the Executive Director.			Prevederi UE neaplicabile		
Articolul 39 **Răspunderea ENISA**	**Article 39** **Liability of ENISA**					
(1) Răspunderea contractuală a ENISA este reglementată de legea aplicabilă contractului în cauză.	(1) The contractual liability of ENISA shall be governed by the law applicable to the contract in question.			Prevederi UE neaplicabile		
(2) Curtea de Justiție a Uniunii Europene este competentă să se pronunțe în temeiul oricărei clauze compromisorii cuprinse într-un contract încheiat de ENISA.	(2) The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause contained in a contract concluded by ENISA.			Prevederi UE neaplicabile		
(3) În materie de răspundere necontractuală, ENISA repară orice prejudiciu cauzat de personalul său în cursul exercitării atribuțiilor acestuia, în conformitate cu principiile generale comune legislațiilor statelor membre.	(3) In the case of non-contractual liability, ENISA shall make good any damage caused by it or its staff in the performance of their duties, in accordance with the general principles common to the laws of the Member States.			Prevederi UE neaplicabile		
(4) Curtea de Justiție a Uniunii Europene este competentă în ceea ce privește orice litigiu privind repararea prejudiciilor astfel cum se menționează la alineatul (3).	(4) The Court of Justice of the European Union shall have jurisdiction in any dispute over compensation for damage as referred to in paragraph 3.			Prevederi UE neaplicabile		

(5) Răspunderea personală a personalului ENISA față de ENISA este reglementată de condițiile relevante care se aplică personalului ENISA.	(5) The personal liability of ENISA's staff towards ENISA shall be governed by the relevant conditions applying to ENISA's staff.			Prevederi UE neaplicabile		
Articolul 40 **Regimul lingvistic**	**Article 40** **Language arrangements**					
(1) Regulamentul nr. 1 al Consiliului (32) se aplică ENISA. Statele membre și celelalte organisme desemnate de către statele membre se pot adresa ENISA și pot primi răspunsuri în una dintre limbile oficiale ale instituțiilor Uniunii, la alegerea acestora.	(1) Council Regulation No 1 (1) shall apply to ENISA. The Member States and the other bodies appointed by the Member States may address ENISA and receive a reply in the official language of the institutions of the Union that they choose.			Prevederi UE neaplicabile		
(2) Serviciile de traducere necesare funcționării ENISA sunt asigurate de către Centrul de Traduceri pentru Organismele Uniunii Europene.	(2) The translation services required for the functioning of ENISA shall be provided by the Translation Centre for the Bodies of the European Union.			Prevederi UE neaplicabile		
Articolul 41 **Protecția datelor cu caracter personal**	**Article 41** **Protection of personal data**					
(1) Prelucrarea datelor cu caracter personal de către ENISA face obiectul Regulamentului (UE) 2018/1725.	(1) The processing of personal data by ENISA shall be subject to Regulation (EU) 2018/1725.			Prevederi UE neaplicabile		
(2) Consiliul de administrație adoptă normele de punere în aplicare astfel cum se menționează la articolul 45 alineatul (3) din Regulamentul (UE) 2018/1725. Consiliul de administrație poate adopta dispozițiile suplimentare necesare pentru aplicarea de către ENISA a Regulamentului (UE) 2018/1725.	(2) The Management Board shall adopt implementing rules as referred to in Article 45(3) of Regulation (EU) 2018/1725. The Management Board may adopt additional measures necessary for the application of Regulation (EU) 2018/1725 by ENISA.			Prevederi UE neaplicabile		
Articolul 42 **Cooperarea cu țările terțe și cu organizațiile internaționale**	**Article 42** **Cooperation with third countries and international organisations**					
(1) În măsura în care este necesar pentru atingerea obiectivelor stabilite în prezentul regulament, ENISA	(1) To the extent necessary in order to achieve the objectives set out in this Regulation, ENISA may cooperate with			Prevederi UE neaplicabile		

poate coopera cu autoritățile competente din țările terțe sau cu organizațiile internaționale sau cu ambele. În acest scop, ENISA poate stabili acorduri de lucru cu autoritățile din țări terțe și cu organizații internaționale, sub rezerva aprobării prealabile a Comisiei. Respectivele acorduri de lucru nu creează obligații legale pentru Uniune și nici pentru statele sale membre.	the competent authorities of third countries or with international organisations or both. To that end, ENISA may establish working arrangements with the authorities of third countries and international organisations, subject to the prior approval of the Commission. Those working arrangements shall not create legal obligations incumbent on the Union and its Member States.					
(2) ENISA este deschisă participării țărilor terțe care au încheiat acorduri cu Uniunea în acest sens. În baza dispozițiilor relevante ale acestor acorduri, se stabilesc acorduri de lucru care specifică, în special, caracterul, amploarea și modalitatea participării acestor țări terțe la activitatea ENISA, inclusiv dispoziții referitoare la participarea la inițiativele puse în practică de ENISA, la contribuțiile financiare și la personal. În ceea ce privește chestiunile legate de personal, aceste acorduri de lucru respectă, în orice caz, Statutul funcționarilor și Regimul aplicabil celorlalți agenți.	(2) ENISA shall be open to the participation of third countries that have concluded agreements with the Union to that effect. Under the relevant provisions of such agreements, working arrangements shall be established specifying in particular the nature, extent and manner in which those third countries are to participate in ENISA's work, and shall include provisions relating to participation in the initiatives undertaken by ENISA, to financial contributions and to staff. As regards staff matters, those working arrangements shall comply with the Staff Regulations of Officials and Conditions of Employment of Other Servants in any event.			Prevederi UE neaplicabile		
(3) Consiliul de administrație adoptă o strategie pentru relațiile cu țări terțe și cu organizații internaționale, în ceea ce privește aspectele pentru care ENISA este competentă. Comisia se asigură că ENISA își desfășoară activitatea în limitele mandatului său și în cadrul	(3) The Management Board shall adopt a strategy for relations with third countries and international organisations concerning matters for which ENISA is competent. The Commission shall ensure that ENISA operates within its mandate and the existing			Prevederi UE neaplicabile		

instituțional existent prin încheierea de acorduri de lucru adecvate cu directorul agenției.	institutional framework by concluding appropriate working arrangements with the Executive Director.					
Articolul 43 **Norme de securitate privind protecția informațiilor sensibile neclasificate și a informațiilor clasificate**	**Article 43** **Security rules on the protection of sensitive non-classified information and classified information**					
După consultarea Comisiei, ENISA adoptă norme de securitate care pun în aplicare principiile de securitate cuprinse în normele de securitate ale Comisiei pentru protecția informațiilor sensibile neclasificate și a IUEC, astfel cum sunt prevăzute în Deciziile (UE, Euratom) 2015/443 și (UE, Euratom) 2015/444. Normele de securitate ale ENISA includ dispoziții privind schimbul, prelucrarea și stocarea unor astfel de informații.	After consulting the Commission, ENISA shall adopt security rules applying the security principles contained in the Commission's security rules for protecting sensitive non-classified information and EUCI, as set out in Decisions (EU, Euratom) 2015/443 and 2015/444. ENISA's security rules shall include provisions for the exchange, processing and storage of such information.			Prevederi UE neaplicabile		
Articolul 44 **Acordul privind sediul și condițiile de funcționare**	**Article 44** **Headquarters Agreement and operating conditions**					
(1) Prevederile necesare referitoare la sediul care urmează să fie pus la dispoziția ENISA în statul membru gazdă și la facilitățile care urmează să fie oferite de statul membru respectiv, precum și normele specifice aplicabile în statul membru gazdă directorului executiv, membrilor consiliului de administrație, personalului ENISA și membrilor familiilor acestora se stabilesc într-un acord privind sediul, încheiat între ENISA și statul membru gazdă după obținerea aprobării consiliului de administrație.	(1) The necessary arrangements concerning the accommodation to be provided for ENISA in the host Member State and the facilities to be made available by that Member State together with the specific rules applicable in the host Member State to the Executive Director, members of the Management Board, ENISA's staff and members of their families shall be laid down in a headquarters agreement between ENISA and the host Member State, concluded after obtaining the approval of the Management Board.			Prevederi UE neaplicabile		
(2) Statul membru care găzduiește ENISA pune la	(2) ENISA's host Member State shall provide the best			Prevederi UE neaplicabile		

dispoziție cele mai bune condiții posibile pentru a asigura buna funcționare a ENISA, ținând cont de 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 sau soțiile personalului.	possible conditions for ensuring the proper functioning of ENISA, taking into account the accessibility of the location, the existence of adequate education facilities for the children of staff members, appropriate access to the labour market, social security and medical care for both children and spouses of staff members.					
Articolul 45 **Controlul administrativ**	**Article 45** **Administrative control**					
Activitățile ENISA fac obiectul supravegherii de către Ombudsmanul European, în conformitate cu articolul 228 din TFUE.	The operations of ENISA shall be supervised by the European Ombudsman in accordance with Article 228 TFEU.			Prevederi UE neaplicabile		
TITLUL III **CADRUL DE CERTIFICARE A SECURITĂȚII CIBERNETICE**	**TITLE III** **CYBERSECURITY CERTIFICATION FRAMEWORK**					
Articolul 46 **Cadrul european de certificare a securității cibernetice**	**Article 46** **European cybersecurity certification framework**				Prevederile art. 46–50 reglementează instituirea cadrului european de certificare a securității cibernetice și activitatea Comisiei Europene, a ENISA și a ECCG privind elaborarea, adoptarea, revizuirea și publicitatea sistemelor europene de certificare și, prin obiectul lor, nu necesită măsuri naționale de punere în aplicare.	
(1) Se instituie cadrul european de certificare a securității cibernetice pentru a îmbunătăți condițiile de funcționare a pieței interne prin creșterea nivelului de securitate cibernetică în Uniune și prin permiterea unei abordări armonizate la nivelul Uniunii în privința sistemelor europene de certificare a	(1) The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within the Union and enabling a harmonised approach at Union			Prevederi UE neaplicabile		

securității cibernetice, în scopul creării unei piețe unice digitale pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate.	level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services, ICT processes and managed security services.					
(2) Cadrul european de certificare a securității cibernetice prevede un mecanism pentru instituirea unor sisteme europene de certificare a securității cibernetice, și de atestare că produsele TIC, serviciile TIC și procesele TIC care au fost evaluate în conformitate cu sistemele 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 respectivele produse, servicii și procese sau accesibile prin intermediul acestora pe întregul lor ciclu de viață. În plus, acesta atestă că serviciile de securitate gestionate care au fost evaluate în conformitate cu astfel de sisteme respectă cerințele de securitate specificate în scopul protejării disponibilității, autenticității, integrității și confidențialității datelor care sunt accesate, prelucrate, stocate sau transmise în legătură cu furnizarea serviciilor respective și că serviciile respective sunt furnizate în mod continuu de personal care are competența, expertiza și experiența necesare, cu un nivel suficient și adecvat	(2) The European cybersecurity certification framework shall provide for a mechanism to establish European cybersecurity certification schemes and to attest that the ICT products, ICT services and ICT processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle. In addition, it shall attest that managed security services that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity and confidentiality of data which are accessed, processed, stored or transmitted in relation to the provision of those services, and that those services are provided continuously with the requisite competence, expertise and experience by staff with a sufficient and appropriate level of relevant			Prevederi UE neaplicabile		

de cunoștințe tehnice relevante și de integritate profesională.	technical knowledge and professional integrity.					
Articolul 47 **Programul de activitate etapizat la nivelul Uniunii pentru certificarea europeană a securității cibernetice**	**Article 47** **The Union rolling work programme for European cybersecurity certification**					
(1) Comisia publică un program de activitate etapizat la nivelul Uniunii pentru certificarea europeană a securității cibernetice (denumit în continuare „programul de activitate etapizat la nivelul Uniunii") în care se identifică prioritățile strategice pentru viitoarele sisteme europene de certificare a securității cibernetice.	(1) The Commission shall publish a Union rolling work programme for European cybersecurity certification (the 'Union rolling work programme') that shall identify strategic priorities for future European cybersecurity certification schemes.			Prevederi UE neaplicabile		
(2) Programul de activitate etapizat la nivelul Uniunii include îndeosebi o listă a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate, sau a categoriilor acestora, care pot beneficia de includerea în sfera de aplicare a unui sistem european de certificare a securității cibernetice.	(2) The Union rolling work programme shall in particular include a list of ICT products, ICT services, ICT processes and managed security services, or categories thereof, that are capable of benefiting from being included in the scope of a European cybersecurity certification scheme.			Prevederi UE neaplicabile		
(3) Includerea în programul de activitate etapizat la nivelul Uniunii a unui anumit produs TIC, serviciu TIC, proces TIC ori a unor servicii de securitate gestionate, sau a unor categorii a acestora, se justifică în baza unuia sau a mai multora dintre considerentele următoare: (a)disponibilitatea și dezvoltarea sistemelor naționale de certificare a securității cibernetice care se aplică oricărei categorii specifice de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, cu	(3) Inclusion in the Union rolling work programme of specific ICT products, ICT services, ICT processes, or managed security services, or categories thereof, shall be justified on the basis of one or more of the following grounds: (a) the availability and the development of national cybersecurity certification schemes covering a specific category of ICT products, ICT services, ICT processes or managed security services			Prevederi UE neaplicabile		

precădere în ceea ce privește riscul de fragmentare; (b)politica sau dreptul relevant al Uniunii sau al statelor membre; (c)cererea de pe piață; (ca) evoluțiile tehnologice și disponibilitatea și dezvoltarea sistemelor internaționale de certificare a securității cibernetice, a standardelor internaționale și a standardelor aplicate în industrie; (d)dezvoltările din aria amenințărilor cibernetice; (e)solicitarea de pregătire a unei propuneri de sistem specifice de către ECCG.	and, in particular, as regards the risk of fragmentation; (b) relevant Union or Member State law or policy; (c) market demand; (ca) technological developments and the availability and development of international cybersecurity certification schemes and international standards and standards used by the industry; (d) developments in the cyber threat landscape; (e) request for the preparation of a specific candidate scheme by the ECCG.					
(4) Comisia ține seama în mod corespunzător de avizele emise în privința proiectului de program de activitate etapizat la nivelul Uniunii de către ECCG și de către Grupul părților interesate pentru certificare.	(4) The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme.			Prevederi UE neaplicabile		
(5) Primul program de activitate etapizat la nivelul Uniunii se publică până la 28 iunie 2020. Programul de activitate etapizat la nivelul Uniunii se actualizează cel puțin o dată la trei ani sau mai des, dacă este necesar.	(5) The first Union rolling work programme shall be published by 28 June 2020. The Union rolling work programme shall be updated at least once every three years and more often if necessary.			Prevederi UE neaplicabile		
Articolul 48 **Solicitarea unui sistem european de certificare a securității cibernetice**	**Article 48** **Request for a European cybersecurity certification scheme**					
(1) Comisia îi poate solicita ENISA să pregătească o propunere de sistem sau să revizuiască un sistem european de certificare a securității cibernetice existent, pe baza programului de activitate etapizat la nivelul Uniunii.	(1) The Commission may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme on the basis of the Union rolling work programme.			Prevederi UE neaplicabile		

(2) În cazuri justificate în mod corespunzător, Comisia sau ECCG îi poate solicita ENISA să pregătească o propunere de sau să revizuiască un sistem european de certificare a securității cibernetice existent, fără ca acestea să fie incluse în programul de activitate etapizat la nivelul Uniunii. Programul de activitate etapizat la nivelul Uniunii se actualizează în consecință.	(2) In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. The Union rolling work programme shall be updated accordingly.			Prevederi UE neaplicabile		
Articolul 49 **Pregătirea, adoptarea și revizuirea unui sistem european de certificare a securității cibernetice**	**Article 49** **Preparation, adoption and review of a European cybersecurity certification scheme**					
(1) În urma unei solicitări din partea Comisiei în temeiul articolului 48, ENISA pregătește o propunere de sistem care îndeplinește cerințele aplicabile prevăzute la articolele 51, 51a, 52 și 54.	(1) Following a request from the Commission pursuant to Article 48, ENISA shall prepare a candidate scheme that meets the applicable requirements set out in Articles 51, 51a, 52 and 54.			Prevederi UE neaplicabile		
(2) În urma unei solicitări din partea ECCG în temeiul articolului 48 alineatul (2), ENISA poate pregăti o propunere de sistem care îndeplinește cerințele aplicabile prevăzute la articolele 51, 51a, 52 și 54. În cazul în care refuză o astfel de solicitare, ENISA prezintă motivele de refuz. Orice decizie de refuz al unei astfel de solicitări se ia de către consiliul de administrație.	(2) Following a request from the ECCG pursuant to Article 48(2), ENISA may prepare a candidate scheme that meets the applicable requirements set out in Articles 51, 51a, 52 and 54. If ENISA refuses such a request, it shall give reasons for its refusal. Any decision to refuse such a request shall be taken by the Management Board.			Prevederi UE neaplicabile		
(3) Atunci când pregătește o propunere de sistem, ENISA consultă toate părțile interesate relevante în timp util, printr-un proces de consultare formal, deschis, transparent și cuprinzător. Atunci când transmite Comisiei propunerea de sistem în temeiul alineatului (6), ENISA furnizează	(3) When preparing a candidate scheme, ENISA shall consult all relevant stakeholders in a timely manner by means of a formal, open, transparent and inclusive consultation process. When transmitting the candidate scheme to the Commission pursuant to			Prevederi UE neaplicabile		

informații cu privire la modul în care a respectat prezentul alineat.	paragraph 6, ENISA shall provide information on the manner in which it has complied with this paragraph.					
(4) Pentru fiecare propunere de sistem, ENISA instituie un grup de lucru ad-hoc în conformitate cu articolul 20 alineatul (4) cu scopul de a-i oferi ENISA consiliere și expertiză specifice. Respectivele grupuri de lucru ad-hoc includ, după caz și fără a aduce atingere procedurilor și marjei de apreciere prevăzute în articolul 20 alineatul (4), experți din administrațiile publice ale statelor membre, din instituțiile, organele, oficiile și agențiile Uniunii și din sectorul privat.	(4) For each candidate scheme, ENISA shall establish an ad hoc working group in accordance with Article 20(4) for the purpose of providing ENISA with specific advice and expertise. Those ad hoc working groups shall, as appropriate and without prejudice to the procedures and discretion provided for in Article 20(4), include experts from the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector.			Prevederi UE neaplicabile		
(5) ENISA cooperează strâns cu ECCG. ECCG furnizează ENISA asistență și consiliere de specialitate în legătură cu pregătirea propunerii de sistem și adoptă un aviz privind propunerea de sistem.	(5) ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme and shall adopt an opinion on the candidate scheme.			Prevederi UE neaplicabile		
(6) ENISA ține seama în cea mai mare măsură posibilă de avizul ECCG înainte de a transmite Comisiei propunerea de sistem pregătită în conformitate cu alineatele (3), (4) și (5). Avizul ECCG nu este obligatoriu pentru ENISA, iar lipsa unui astfel de aviz nu împiedică ENISA să transmită Comisiei propunerea de sistem.	(6) ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme prepared in accordance with paragraphs 3, 4 and 5 to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission.			Prevederi UE neaplicabile		
(7) Pe baza propunerii de sistem pregătite de ENISA, Comisia poate adopta acte de punere în aplicare care să prevadă un sistem european de certificare a securității cibernetice pentru	(7) The Commission may, on the basis of the candidate scheme prepared by ENISA, adopt implementing acts providing for a European cybersecurity certification			Prevederi UE neaplicabile		

produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care îndeplinesc cerințele relevante prevăzute la articolele 51, 51a, 52 și 54. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 66 alineatul (2).	scheme for ICT products, ICT services, ICT processes and managed security services which meets the relevant requirements set out in Articles 51, 51a, 52 and 54. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).					
(8) ENISA evaluează cel puțin o dată la cinci ani fiecare sistem european de certificare a securității cibernetice adoptat, ținând seama de observațiile primite de la părțile interesate. Dacă este necesar, Comisia sau ECCG îi pot solicita ENISA să demareze procesul de elaborare a unei propuneri revizuite de sistem în conformitate cu articolul 48 și cu prezentul articol.	(8) At least every five years, ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. If necessary, the Commission or the ECCG may request ENISA to start the process of developing a revised candidate scheme in accordance with Article 48 and this Article.			Prevederi UE neaplicabile		
Articolul 49a **Informarea și consultarea privind sistemele europene de certificare a securității cibernetice**	**Article 49a** **Information and consultation on the European cybersecurity certification schemes**					
(1) Comisia pune la dispoziția publicului informațiile aferente cererii sale către ENISA de a pregăti o propunere de sistem sau de a revizui un sistem european de certificare a securității cibernetice existent, astfel cum se menționează la articolul 48.	(1) The Commission shall make the information on its request to ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme as referred to in Article 48 publicly available.			Prevederi UE neaplicabile		
(2) În cursul pregătirii de către ENISA a unei propuneri de sistem în temeiul articolului 49, Parlamentul European, Consiliul sau ambele instituții pot solicita Comisiei, în calitatea sa de președinte al ECCG, și ENISA să prezinte trimestrial informații relevante cu privire la proiectul unei propuneri de sistem. La cererea Parlamentului European	(2) During the preparation of a candidate scheme by ENISA pursuant to Article 49, the European Parliament, the Council or both may request the Commission, in its capacity as chair of the ECCG, and ENISA to present relevant information on a draft candidate scheme on a quarterly basis. Upon the			Prevederi UE neaplicabile		

sau a Consiliului, ENISA, de comun acord cu Comisia și fără a aduce atingere articolului 27, poate pune la dispoziția Parlamentului European și a Consiliului părțile relevante ale proiectului unei propuneri de sistem, într-un mod adecvat nivelului de confidențialitate necesar și, după caz, în mod restrâns.	request of the European Parliament or the Council, ENISA, in agreement with the Commission and without prejudice to Article 27, may make available to the European Parliament and to the Council relevant parts of a draft candidate scheme in a manner appropriate to the confidentiality level required, and where appropriate in a restricted manner.					
(3) Pentru a consolida dialogul dintre instituțiile Uniunii și pentru a contribui la un proces de consultare formal, deschis, transparent și cuprinzător, Parlamentul European, Consiliul sau ambele instituții pot invita Comisia și ENISA să discute aspecte legate de funcționarea sistemelor europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate.	(3) In order to enhance the dialogue between the Union institutions and to contribute to a formal, open, transparent and inclusive consultation process, the European Parliament, the Council or both may invite the Commission and ENISA to discuss matters concerning the functioning of European cybersecurity certification schemes for ICT products, ICT services, ICT processes or managed security services.			Prevederi UE neaplicabile		
(4) Comisia ține seama, după caz, de elementele care decurg din opiniile exprimate de Parlamentul European și de Consiliu cu privire la aspectele menționate la alineatul (3) de la prezentul articol atunci când evaluează prezentul regulament în temeiul articolului 67.	(4) The Commission shall take into account, where appropriate, elements arising from the views expressed by the European Parliament and by the Council on the matters referred to in paragraph 3 of this Article when evaluating this Regulation pursuant to Article 67.			Prevederi UE neaplicabile		
Articolul 50 **Site-ul referitor la sistemele europene de certificare a securității cibernetice**	**Article 50** **Website on European cybersecurity certification schemes**					
(1) ENISA întreține un site dedicat care oferă informații despre sistemele europene de certificare a securității cibernetice, certificatele europene de securitate	(1) ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European			Prevederi UE neaplicabile		

cibernetică și declarațiile de conformitate UE, și le asigură publicitatea, inclusiv informații în ceea ce privește sistemele europene de certificare a securității cibernetice care nu mai sunt valabile, certificatele europene de securitate cibernetică și declarațiile de conformitate UE retrase sau expirate și registrul conținând legături către informații despre securitatea cibernetică furnizate în conformitate cu articolul 55.	cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55.					
(2) După caz, site-ul menționat la alineatul (1) indică și sistemele naționale de certificare a securității cibernetice care au fost înlocuite de un sistem european de certificare a securității cibernetice.	(2) Where applicable, the website referred to in paragraph 1 shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.			Prevederi UE neaplicabile		
Articolul 51 **Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC și procesele TIC**	**Article 51** **Security objectives of European cybersecurity certification schemes for ICT products, ICT services and ICT processes**	**Articolul 10. Obiectivele de securitate ale sistemelor naționale de certificare pentru produsele TIC, serviciile TIC și procesele TIC**				
Un sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC sau procesele TIC este conceput pentru a îndeplini, 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 produsului TIC, serviciului TIC sau procesului TIC; (b) să protejeze datele stocate, transmise sau prelucrate într-un	A European cybersecurity certification scheme for ICT products, ICT services or ICT processes shall be designed to achieve, as applicable, at least the following security objectives: (a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process; (b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised	Un sistem național de certificare a securității cibernetice pentru produsele TIC, serviciile TIC sau procesele TIC este conceput pentru a îndeplini, 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 produsului TIC, serviciului TIC sau procesului TIC; b) să protejeze datele stocate, transmise sau prelucrate într-un alt mod împotriva		Compatibil		

alt mod împotriva distrugerii, pierderii sau modificării accidentale sau neautorizate ori lipsei de disponibilitate pe întregul ciclu de viață al produsului TIC, serviciului TIC sau procesului TIC; (c) să asigure faptul că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces; (d) să identifice și să documenteze dependențele și vulnerabilitățile cunoscute; (e) să înregistreze 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 facă 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; (g) să verifice că produsele TIC, serviciile TIC și procesele TIC nu conțin vulnerabilități cunoscute; (h) să restabilească disponibilitatea datelor, serviciilor și funcțiilor și accesul la acestea în timp util în cazul unui incident fizic sau tehnic; (i) să asigure că produsele TIC, serviciile TIC și procesele TIC sunt securizate implicit și începând cu momentul conceperii; (j) să asigure că produsele TIC, serviciile TIC și procesele TC sunt furnizate cu software și hardware actualizate care nu conțin vulnerabilități cunoscute public și că sunt prevăzute cu	destruction, loss or alteration or lack of availability during the entire life cycle of the ICT product, ICT service or ICT process; (c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer; (d) to identify and document known dependencies and vulnerabilities; (e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; (f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom; (g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities; (h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident; (i) that ICT products, ICT services and ICT processes are secure by default and by design; (j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	distrugerii, pierderii sau modificării accidentale sau neautorizate ori lipsei de disponibilitate pe întregul ciclu de viață al produsului TIC, serviciului TIC sau procesului TIC; c) să asigure faptul că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces; d) să identifice și să documenteze dependențele și vulnerabilitățile cunoscute; e) să înregistreze 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 facă 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; g) să verifice că produsele TIC, serviciile TIC și procesele TIC nu conțin vulnerabilități cunoscute; h) să restabilească disponibilitatea datelor, serviciilor și funcțiilor și accesul la acestea în timp util în cazul unui incident fizic sau tehnic; i) să asigure că produsele TIC, serviciile TIC și procesele TIC sunt securizate implicit și începând cu momentul conceperii; j) să asigure că produsele TIC, serviciile TIC și procesele TC sunt furnizate cu software și hardware actualizate care nu conțin vulnerabilități cunoscute public și că sunt prevăzute cu				

mecanisme pentru actualizări securizate.		mecanisme pentru actualizări securizate.				
Articolul 51a **Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice pentru serviciile de securitate gestionate**	**Article 51a** **Security objectives of European cybersecurity certification schemes for managed security services**	**Articolul 11. Obiectivele de securitate ale sistemelor naționale de certificare pentru serviciile de securitate gestionate**				
Un sistem european de certificare a securității cibernetice pentru serviciile de securitate gestionate este conceput pentru a îndeplini, după caz, cel puțin următoarele obiective de securitate: (a) că serviciile de securitate gestionate sunt furnizate de personal care are competența, expertiza și experiența necesare, inclusiv un nivel suficient și adecvat de cunoștințe tehnice și competențe în domeniul specific, experiență suficientă și adecvată și cel mai înalt grad de integritate profesională; (b) că furnizorul dispune de proceduri interne adecvate pentru a se asigura că serviciile de securitate gestionate sunt furnizate la un nivel suficient și adecvat de calitate în orice moment; (c) că datele accesate, stocate, transmise sau prelucrate în alt mod în legătură cu furnizarea de servicii de securitate gestionate sunt protejate împotriva accesului accidental sau neautorizat, a stocării, a divulgării, a distrugerii, a altor prelucrări, a pierderii, a modificării sau a lipsei disponibilității; (d) că disponibilitatea datelor, a serviciilor și a funcțiilor și accesul la acestea sunt restabilite	A European cybersecurity certification scheme for managed security services shall be designed to achieve, as applicable, at least the following security objectives: (a) that the managed security services are provided with the requisite competence, expertise and experience, including that the staff tasked with providing those services have a sufficient and appropriate level of technical knowledge and competence in the specific field, sufficient and appropriate experience, and the highest degree of professional integrity; (b) that the provider has appropriate internal procedures in place to ensure that the managed security services are provided at a sufficient and appropriate level of quality at all times; (c) that data accessed, stored, transmitted or otherwise processed in relation to the provision of managed security services are protected against accidental or unauthorised access, storage, disclosure, destruction, other processing, or loss or alteration or lack of availability; (d) that the availability of, and access to, data, services and	Un sistem național de certificare a securității cibernetice pentru serviciile de securitate gestionate este conceput pentru a îndeplini, după caz, cel puțin următoarele obiective de securitate: a) că serviciile de securitate gestionate sunt furnizate de personal care are competența, expertiza și experiența necesare, inclusiv un nivel suficient și adecvat de cunoștințe tehnice și competențe în domeniul specific, experiență suficientă și adecvată și cel mai înalt grad de integritate profesională; b) că furnizorul dispune de proceduri interne adecvate pentru a se asigura că serviciile de securitate gestionate sunt furnizate la un nivel suficient și adecvat de calitate în orice moment; c) că datele accesate, stocate, transmise sau prelucrate în alt mod în legătură cu furnizarea de servicii de securitate gestionate sunt protejate împotriva accesului accidental sau neautorizat, a stocării, a divulgării, a distrugerii, a altor prelucrări, a pierderii, a modificării sau a lipsei disponibilității; d) că disponibilitatea datelor, a serviciilor și a funcțiilor și accesul la acestea sunt		Compatibil		

în timp util în cazul unui incident fizic sau tehnic; (e) că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces; (f) că se ține o evidență care este disponibilă pentru a se stabili care sunt datele, serviciile sau funcțiile care au fost accesate, utilizate sau procesate în alt mod, precum și în ce moment și de către cine au fost accesate, utilizate sau procesate acestea; (g) că produsele TIC, serviciile TIC și procesele TIC utilizate pentru furnizarea serviciilor de securitate gestionate sunt securizate începând cu momentul conceperii și în mod implicit și, după caz, includ cele mai recente actualizări de securitate și nu conțin vulnerabilități cunoscute public.	functions is restored in a timely manner in the event of a physical or technical incident; (e) that authorised persons, programs or machines are able to access only the data, services or functions to which their access rights refer; (f) that a record is kept and is available for assessment, of the data, services or functions that have been accessed, used or otherwise processed, at what times and by whom; (g) that the ICT products, ICT services and ICT processes deployed in the provision of the managed security services are secure by design and by default and, where applicable, include the latest security updates and do not contain publicly known vulnerabilities.	restabilite în timp util în cazul unui incident fizic sau tehnic; e) că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces; f) că se ține o evidență care este disponibilă pentru a se stabili care sunt datele, serviciile sau funcțiile care au fost accesate, utilizate sau procesate în alt mod, precum și în ce moment și de către cine au fost accesate, utilizate sau procesate acestea; g) că produsele TIC, serviciile TIC și procesele TIC utilizate pentru furnizarea serviciilor de securitate gestionate sunt securizate începând cu momentul conceperii și în mod implicit și, după caz, includ cele mai recente actualizări de securitate și nu conțin vulnerabilități cunoscute public.				
Articolul 52 **Niveluri de asigurare ale sistemelor europene de certificare a securității cibernetice**	**Article 52** **Assurance levels of European cybersecurity certification schemes**	**Articolul 13. Nivelurile de asigurare**				
(1) Un sistem european de certificare a securității cibernetice poate stabili unul sau mai multe dintre următoarele niveluri de asigurare pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate: „de bază”, „substanțial” sau „ridicat”. Nivelul de asigurare este corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat, înțeles ca	(1) A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services, ICT processes and managed security services: ‘basic’, ‘substantial’ or ‘high’. The assurance level shall be commensurate with the level of the risk associated with the intended use of the ICT product, ICT service, ICT process or managed security service, in terms of the	(1) Un sistem național de certificare a securității cibernetice poate stabili unul sau mai multe dintre următoarele niveluri de asigurare pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate: „de bază”, „substanțial” sau „ridicat”. Nivelul de asigurare este corespunzător nivelului riscului asociat cu utilizarea preconizată a unui produs TIC, serviciu TIC, proces TIC sau serviciu de securitate gestionat, înțeles ca		Compatibil		

probabilitate și impact al unui incident.	probability and impact of an incident.	probabilitate și impact al unui incident cibernetic.				
(2) Certificatele europene de securitate cibernetică și declarațiile de conformitate UE fac trimitere la orice nivel de asigurare prevăzut în sistemul european de certificare a securității cibernetice în temeiul căruia a fost emis certificatul european de securitate cibernetică sau declarația de conformitate UE.	(2) European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity certification scheme under which the European cybersecurity certificate or EU statement of conformity is issued.	(2) Certificatele naționale de securitate cibernetică și declarațiile de conformitate fac trimitere la orice nivel de asigurare prevăzut în sistemul național de certificare a securității cibernetice în temeiul căruia a fost emis certificatul național de securitate cibernetică sau declarația de conformitate.		Compatibil		
(3) Cerințele de securitate corespunzătoare fiecărui nivel de asigurare sunt prevăzute de sistemul european de certificare a securității cibernetice relevant, inclusiv funcțiile de securitate corespunzătoare și rigoarea și profunzimea corespunzătoare ale evaluării la care a fost supus produsul TIC, serviciul TIC, procesul TIC sau serviciul de securitate gestionat.	(3) The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme, including the corresponding security functionalities and the corresponding rigour and depth of the evaluation that the ICT product, ICT service, ICT process or managed security service is to undergo.	(3) Cerințele de securitate corespunzătoare fiecărui nivel de asigurare sunt prevăzute de sistemul național de certificare a securității cibernetice relevant, inclusiv funcțiile de securitate corespunzătoare și rigoarea și profunzimea corespunzătoare ale evaluării asupra produsului TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat.		Compatibil		
(4) Certificatul sau declarația de conformitate UE face trimitere 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 preîntâmpina.	(4) The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of, or to prevent cybersecurity incidents.	(4) Certificatul sau declarația de conformitate face trimitere la specificații tehnice, standarde și proceduri conexe acestora, inclusiv controale tehnice, al căror scop este de a diminua riscul de incidente cibernetice sau de a le preîntâmpina.		Compatibil		
(5) 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 produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv sau declarația de conformitate UE respectivă	(5) A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT products, ICT services, ICT processes or managed security services for which that certificate or that EU statement of conformity is issued meet the corresponding security requirements,	(5) Un certificat național de securitate cibernetică sau o declarație de conformitate care face trimitere la nivelul de asigurare „de bază” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv sau declarația de conformitate respectivă		Compatibil		

îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și de atacuri cibernetice. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin o examinare a documentației tehnice. În cazurile în care o astfel de examinare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.	including security functionalities, and that they have been evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. Where such a review is not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.	îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor de bază cunoscute de incidente și de atacuri cibernetice. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin o examinare a documentației tehnice. În cazurile în care o astfel de examinare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.				
(6) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „substanțial” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor pentru securitatea cibernetică cunoscute și a riscului de incidente și de atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare. În cazurile în care oricare dintre	(6) A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services, ICT processes or managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities. Where any such evaluation activities are	(6) Un certificat național de securitate cibernetică care face trimitere la nivelul de asigurare „substanțial” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscurilor pentru securitatea cibernetică cunoscute și a riscului de incidente și de atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare. În cazurile în care oricare dintre aceste activități de evaluare nu		Compatibil		

aceste activități de evaluare nu este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.	not appropriate, substitute evaluation activities with equivalent effect shall be undertaken.	este adecvată, se desfășoară activități de evaluare înlocuitoare cu efect echivalent.				
(7) Un certificat european de securitate cibernetică care face trimitere la nivelul de asigurare „ridicat” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public; testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare, la nivel de ultimă generație; și o evaluare a rezistenței acestora la atacatori competenți prin teste de rezistență la intruziuni. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități înlocuitoare cu efect echivalent.	(7) A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services, ICT processes or managed security services for which that certificate is issued meet the corresponding security requirements, including security functionalities, and that they have been evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that the ICT products, ICT services, ICT processes or managed security services correctly implement the necessary security functionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation activities are not appropriate, substitute activities with equivalent effect shall be undertaken.	(7) Un certificat național de securitate cibernetică care face trimitere la nivelul de asigurare „ridicat” oferă asigurare cu privire la faptul că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pentru care se eliberează certificatul respectiv îndeplinesc cerințele de securitate corespunzătoare, inclusiv funcțiile de securitate, și că acestea au fost evaluate la un nivel care urmărește minimizarea riscului de atacuri cibernetice de ultimă generație desfășurate de actori cu competențe și resurse substanțiale. Activitățile de evaluare care trebuie să fie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public; testarea pentru a demonstra că produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate implementează corect funcțiile de securitate necesare, la nivel de ultimă generație; și o evaluare a rezistenței acestora la atacatori competenți prin teste de rezistență la intruziuni. În cazurile în care oricare dintre aceste activități de evaluare nu este adecvată, se desfășoară activități înlocuitoare cu efect echivalent.		Compatibil		
(8) Un sistem european de certificare a securității cibernetice poate specifica mai multe niveluri de evaluare în funcție de rigoarea și	(8) A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation	(8) Un sistem național de certificare a securității cibernetice poate specifica mai multe niveluri de evaluare în funcție de rigoarea și		Compatibil		

profunzimea metodologiei de evaluare utilizate. Fiecare dintre nivelurile de evaluare corespunde unuia dintre nivelurile de asigurare și este definit printr-o combinație corespunzătoare de componente ale asigurării.	methodology used. Each of the evaluation levels shall correspond to one of the assurance levels and shall be defined by an appropriate combination of assurance components.	profunzimea metodologiei de evaluare utilizate. Fiecare dintre nivelurile de evaluare corespunde unuia dintre nivelurile de asigurare și este definit printr-o combinație corespunzătoare de componente ale asigurării.				
Articolul 53 **Autoevaluarea conformității**	**Article 53** **Conformity self-assessment**	**Articolul 18. Autoevaluarea conformității și declarația de conformitate**				
(1) Un sistem european de certificare a securității cibernetice poate permite efectuarea unei autoevaluări a conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate. O astfel de autoevaluare a conformității este permisă numai în cazul produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care prezintă un risc redus corespunzând nivelului de asigurare „de bază”.	(1) A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services. Conformity self-assessment shall be permitted only in relation to ICT products, ICT services, ICT processes or managed security services that present a low risk corresponding to assurance level ‘basic’.	(1) Un sistem național de certificare a securității cibernetice poate permite efectuarea unei autoevaluări a conformității pe răspunderea exclusivă a producătorului sau a furnizorului de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate. O astfel de autoevaluare a conformității este permisă numai în cazul produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care prezintă un risc redus corespunzând nivelului de asigurare „de bază”.		Compatibil		
(2) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate poate elibera o declarație de conformitate UE care menționează că s-a demonstrat îndeplinirea cerințelor prevăzute în sistem. Prin eliberarea unei astfel de declarații, producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat cu cerințele stabilite în sistemul respectiv.	(2) The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services may issue an EU statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated. By issuing such a statement, the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall assume responsibility for the compliance of the ICT product, ICT service, ICT process or managed security service with the requirements set out in that scheme.	(2) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate poate elibera o declarație de conformitate care menționează că s-a demonstrat îndeplinirea cerințelor prevăzute în sistem. Prin eliberarea unei astfel de declarații, producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate își asumă responsabilitatea pentru conformitatea produsului TIC, a serviciului TIC, a procesului TIC sau a serviciului de securitate gestionat cu cerințele stabilite în sistemul respectiv.		Compatibil		

(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate pune la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 58, pe durata stabilită în sistemul european de certificare a securității cibernetice corespunzător, declarația de conformitate UE, documentația tehnică și toate celelalte informații relevante legate de conformitatea cu sistemul a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate. O copie a declarației de conformitate UE se transmite către autoritatea națională de certificare a securității cibernetice și către ENISA.	(3) The manufacturer or provider of ICT products, ICT services, ICT processes or managed security services shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity of the ICT products, ICT services, ICT processes or managed security services with the scheme available to the national cybersecurity certification authority designated pursuant to Article 58 for the period provided for in the corresponding European cybersecurity certification scheme. A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.	(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate pune la dispoziția Agenției, pe durata stabilită în sistemul național de certificare a securității cibernetice corespunzător, declarația de conformitate, documentația tehnică și toate celelalte informații relevante legate de conformitatea cu sistemul a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate.		Compatibil		
(4) Eliberarea unei declarații de conformitate UE este voluntară, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau dreptul statelor membre.	(4) The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.	(4) Emiterea declarației de conformitate este voluntară, cu excepția cazului în care prin lege se prevede altfel.		Compatibil		
(5) Declarația de conformitate UE este recunoscută în toate statele membre.	(5) EU statements of conformity shall be recognised in all Member States.			Prevederi UE direct aplicabile la aderare	Prevederea va deveni direct aplicabilă de la data aderării. Până la această dată, recunoașterea în Republica Moldova a declarațiilor de conformitate UE se realizează în condițiile art. 24 din proiect.	
Articolul 54 **Elemente ale sistemelor europene de certificare a securității cibernetice**	**Article 54** **Elements of European cybersecurity certification schemes**	**Articolul 12. Elemente ale sistemelor naționale de certificare a securității cibernetice**				
(1) Un sistem european de certificare a securității cibernetice include cel puțin următoarele elemente:	(1) A European cybersecurity certification scheme shall include at least the following elements:	(1) Un sistem național de certificare a securității cibernetice include cel puțin următoarele elemente:		Compatibil		

(a)obiectul și sfera de aplicare a sistemului de certificare, inclusiv tipul sau categoriile de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate acoperite; (b)o descriere clară a scopului sistemului și a modului în care standardele selectate, metodele de evaluare și nivelurile de asigurare corespund nevoilor utilizatorilor preconizați ai sistemului; (c)trimiteri la standardele internaționale, europene sau naționale aplicate în cadrul evaluării sau, în cazul în care astfel de standarde nu sunt disponibile sau nu sunt adecvate, la specificațiile tehnice care îndeplinesc cerințele prevăzute în anexa II la Regulamentul (UE) nr. 1025/2012 sau, dacă astfel de specificații nu sunt disponibile, la specificații tehnice sau la alte cerințe de securitate cibernetică definite în sistemul european de certificare a securității cibernetice; (d)după caz, unul sau mai multe niveluri de asigurare; (e)o precizare care indică dacă autoevaluarea conformității este permisă în cadrul sistemului; (f)după caz, cerințe specifice sau suplimentare cărora se supun organismele de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică; (g)criteriile și metodele specifice de evaluare,	(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services, ICT processes or managed security services covered; (b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme; (c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or appropriate, to technical specifications that meet the requirements set out in Annex II to Regulation (EU) No 1025/2012 or, if such specifications are not available, to technical specifications or other cybersecurity requirements defined in the European cybersecurity certification scheme; (d) where applicable, one or more assurance levels; (e) an indication of whether conformity self-assessment is permitted under the scheme; (f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical competence to evaluate the cybersecurity requirements; (g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the	a) obiectul și sfera de aplicare a sistemului de certificare, inclusiv tipul sau categoriile de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate acoperite; b) o descriere clară a scopului sistemului și a modului în care standardele selectate, metodele de evaluare și nivelurile de asigurare corespund nevoilor utilizatorilor preconizați ai sistemului; c) trimiteri la standardele internaționale, europene sau naționale aplicate în cadrul evaluării sau, în cazul în care astfel de standarde nu sunt disponibile sau nu sunt adecvate, la specificații tehnice sau la alte cerințe de securitate cibernetică definite în sistemul european de certificare a securității cibernetice; d) după caz, unul sau mai multe niveluri de asigurare; e) o precizare care indică dacă autoevaluarea conformității este permisă în cadrul sistemului; f) după caz, cerințe specifice sau suplimentare cărora se supun organismele de evaluare a conformității pentru a garanta competența tehnică a acestora de a evalua cerințele de securitate cibernetică; g) criteriile și metodele specifice de evaluare, inclusiv tipurile de evaluări, utilizate pentru a demonstra că sunt îndeplinite obiectivele de securitate aplicabile menționate la art. 10 și 11; h) după caz, informațiile necesare pentru certificare care trebuie furnizate sau puse în alt mod la dispoziția organismelor				

inclusiv tipurile de evaluări, utilizate pentru a demonstra că sunt îndeplinite obiectivele de securitate aplicabile menționate la articolele 51 și 51a; (h) după caz, informațiile necesare pentru certificare care trebuie furnizate sau puse în alt mod la dispoziția organismelor de evaluare a conformității de către solicitant; (i) în cazul în care sistemul prevede mărci sau etichete, condițiile în care pot fi utilizate aceste mărci sau etichete; (j) normele pentru monitorizarea conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate cu cerințele certificatelor europene de securitate cibernetică sau ale declarațiilor de conformitate UE, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate; (k) după caz, condițiile de eliberare, de menținere, de continuare și de reînnoire a certificatelor europene de securitate cibernetică, precum și condițiile de extindere sau de restrângere a domeniului de aplicare a certificării; (l) normele privind consecințele neconformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care au fost certificate sau pentru care a fost eliberată o	applicable security objectives referred to in Articles 51 and 51a are achieved; (h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the conformity assessment bodies by an applicant; (i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used; (j) rules for monitoring the compliance of ICT products, ICT services, ICT processes or managed security services with the requirements of the European cybersecurity certificates or the EU statements of conformity, including mechanisms to demonstrate continued compliance with the specified cybersecurity requirements; (k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the conditions for extending or reducing the scope of certification; (l) rules concerning the consequences for ICT products, ICT services, ICT processes or managed security services that have been certified or for which an EU statement of conformity has been issued, but which do not comply with the requirements of the scheme; (m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services	de evaluare a conformității de către solicitant; i) în cazul în care sistemul prevede mărci sau etichete, condițiile în care pot fi utilizate aceste mărci sau etichete; j) normele pentru monitorizarea conformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate cu cerințele certificatelor naționale de securitate cibernetică sau ale declarațiilor de conformitate, inclusiv mecanisme care să demonstreze conformitatea neîntreruptă cu cerințele de securitate cibernetică specificate; k) după caz, condițiile de eliberare, de menținere, de continuare și de reînnoire a certificatelor europene de securitate cibernetică, precum și condițiile de extindere sau de restrângere a domeniului de aplicare a certificării; l) normele privind consecințele neconformității produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care au fost certificate sau pentru care a fost eliberată o declarație de conformitate, dar care nu sunt conforme cu cerințele sistemului; m) normele privind modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale produselor TIC, serviciilor TIC și proceselor TIC; n) după caz, normele privind păstrarea evidențelor de către organismele de evaluare a conformității;				

declarație de conformitate UE, dar care nu sunt conforme cu cerințele sistemului; (m) normele privind modalitățile de raportare și soluționare a vulnerabilităților în materie de securitate cibernetică nedetectate anterior ale produselor TIC, serviciilor TIC și proceselor TIC; (n) după caz, normele privind păstrarea evidențelor de către organismele de evaluare a conformității; (o) identificarea sistemelor naționale sau internaționale de certificare a securității cibernetice care se referă la aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare; (p) conținutul și formatul certificatelor europene de securitate cibernetică și ale declarațiilor de conformitate UE care urmează să fie eliberate; (q) perioada de valabilitate a declarației de conformitate UE, documentația tehnică și toate celelalte informații relevante care sunt puse la dispoziție de producătorul sau de furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate; (r) perioada maximă de valabilitate a certificatelor europene de securitate cibernetică eliberate în temeiul sistemului;	and ICT processes are to be reported and dealt with; (n) where applicable, rules concerning the retention of records by conformity assessment bodies; (o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT services, ICT processes or managed security services, security requirements, evaluation criteria and methods, and assurance levels; (p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued; (q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made available by the manufacturer or provider of ICT products, ICT services, ICT processes or managed security services; (r) maximum period of validity of European cybersecurity certificates issued under the scheme; (s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme; (t) conditions for the mutual recognition of certification schemes with third countries; (u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies	o) identificarea sistemelor naționale sau internaționale de certificare a securității cibernetice care se referă la aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare; p) conținutul și formatul certificatelor europene de securitate cibernetică și ale declarațiilor de conformitate care urmează să fie eliberate; q) perioada de valabilitate a declarației de conformitate, documentația tehnică și toate celelalte informații relevante care sunt puse la dispoziție de producătorul sau de furnizorul de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate; r) perioada maximă de valabilitate a certificatelor naționale de securitate cibernetică eliberate în temeiul sistemului; s) politica de divulgare pentru certificatele naționale de securitate cibernetică eliberate modificate sau retrase în temeiul sistemului; t) condițiile pentru recunoașterea reciprocă a sistemelor de certificare cu țări terțe; u) formatul și procedurile care trebuie urmate de producători sau de furnizori de produse TIC, de servicii TIC sau de procese TIC atunci când furnizează și actualizează informațiile suplimentare privind securitatea cibernetică.				

(s)politica de divulgare pentru certificatele europene de securitate cibernetică eliberate modificate sau retrase în temeiul sistemului; (t)condițiile pentru recunoașterea reciprocă a sistemelor de certificare cu țări terțe; (u)după caz, normele privind orice mecanism de evaluare *inter pares* instituit în cadrul sistemului pentru autoritățile sau organismele care eliberează certificate europene de securitate cibernetică pentru nivelul de asigurare „ridicat” în temeiul articolului 56 alineatul (6). Un astfel de mecanism nu aduce atingere evaluării *inter pares* prevăzute la articolul 59; (v)formatul și procedurile care trebuie urmate de producători sau de furnizori de produse TIC, de servicii TIC sau de procese TIC atunci când furnizează și actualizează informațiile suplimentare privind securitatea cibernetică în conformitate cu articolul 55.	issuing European cybersecurity certificates for assurance level 'high' pursuant to Article 56(6). Such mechanism shall be without prejudice to the peer review provided for in Article 59; (v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updating the supplementary cybersecurity information in accordance with Article 55.					
(2) Cerințele specifice ale sistemului european de certificare a securității cibernetice sunt în concordanță cu cerințele legale aplicabile, în special cu cerințele care decurg din dreptul armonizat al Uniunii.	(2) The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in particular requirements emanating from harmonised Union law.	(2) Cerințele specifice ale sistemului național de certificare sunt în concordanță cu cerințele legale aplicabile.		Compatibil		
(3) În cazul în care un act juridic specific al Uniunii prevede astfel, un certificat sau o	(3) Where a specific Union legal act so provides, a certificate or an EU statement			Prevederi UE direct aplicabile la aderare	Prevederea va deveni direct aplicabilă de la data aderării.	

declarație de conformitate UE eliberată în cadrul unui sistem european de certificare a securității cibernetice poate fi utilizată pentru a demonstra prezumția de conformitate cu cerințele din acel act juridic.	of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.					
(4) În absența unui drept armonizat al Uniunii, dreptul unui stat membru poate prevedea, de asemenea, că se poate folosi un sistem european de certificare a securității cibernetice pentru a stabili prezumția de conformitate cu cerințele legale.	(4) In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.			Prevederi UE direct aplicabile la aderare	Prevederea va deveni direct aplicabilă de la data aderării.	
Articolul 55 **Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate**	**Article 55** **Supplementary cybersecurity information for certified ICT products, ICT services and ICT processes**	**Articolul 19. Informații suplimentare privind securitatea cibernetică pentru produsele TIC, serviciile TIC și procesele TIC certificate**				
(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC certificate sau de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate UE pune la dispoziția publicului următoarele informații suplimentare privind securitatea cibernetică: (a)orientări și recomandări care să le servească utilizatorilor finali la configurarea, instalarea, derularea, funcționarea și întreținerea securizate a produselor TIC sau serviciilor TIC; (b)perioada în timpul căreia se oferă asistență în materie de securitate utilizatorilor finali, mai ales în ceea ce privește disponibilitatea actualizărilor legate de securitatea cibernetică;	(1) The manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes for which an EU statement of conformity has been issued shall make publicly available the following supplementary cybersecurity information: (a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services; (b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates; (c) contact information of the manufacturer or provider and	(1) Producătorul sau furnizorul de produse TIC, servicii TIC sau procese TIC certificate sau de produse TIC, servicii TIC sau procese TIC pentru care a fost eliberată o declarație de conformitate pune la dispoziția publicului următoarele informații suplimentare privind securitatea cibernetică: a) orientări și recomandări care să le servească utilizatorilor finali la configurarea, instalarea, derularea, funcționarea și întreținerea securizate a produselor TIC sau serviciilor TIC; b) perioada în timpul căreia se oferă asistență în materie de securitate utilizatorilor finali, mai ales în ceea ce privește disponibilitatea actualizărilor legate de securitatea cibernetică;		Compatibil		

(c)informații de contact ale producătorului sau furnizorului și metode acceptate pentru primirea informațiilor despre vulnerabilitate de la utilizatorii finali și de la cercetători din domeniul securității; (d)o trimitere la registrele online care conțin vulnerabilitățile divulgate public legate de produsul TIC, de serviciul TIC sau de procesul TIC și orice avertismente relevante în materie de securitate cibernetică.	accepted methods for receiving vulnerability information from end users and security researchers; (d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.	c) informații de contact ale producătorului sau furnizorului și metode acceptate pentru primirea informațiilor despre vulnerabilitate de la utilizatorii finali și de la cercetători din domeniul securității; d) o trimitere la registrele online care conțin vulnerabilitățile divulgate public legate de produsul TIC, de serviciul TIC sau de procesul TIC și orice avertismente relevante în materie de securitate cibernetică.				
(2) Informațiile menționate la alineatul (1) se pun la dispoziție în format electronic și rămân disponibile și se actualizează după cum este necesar cel puțin până la expirarea certificatului european de securitate cibernetică sau a declarației de conformitate UE aferente.	(2) The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at least until the expiry of the corresponding European cybersecurity certificate or EU statement of conformity.	Informațiile menționate la alin. (1) se pun la dispoziție în format electronic și rămân disponibile și se actualizează după cum este necesar cel puțin până la expirarea certificatului național de securitate cibernetică sau a declarației de conformitate aferente.		Compatibil		
Articolul 56 Certificarea securității cibernetice	**Article 56 Cybersecurity certification**	**Articolul 15. Certificarea securității cibernetice**				
(1) Produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care au fost certificate în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 sunt considerate a fi conforme cu cerințele acestui sistem.	(1) ICT products, ICT services, ICT processes and managed security services that have been certified under a European cybersecurity certification scheme adopted pursuant to Article 49 shall be presumed to comply with the requirements of such scheme.	(1) Produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care au fost certificate în cadrul unui sistem național de certificare a securității cibernetice sunt considerate a fi conforme cu cerințele acestui sistem.		Compatibil		
(2) Certificarea securității cibernetice este voluntară, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul unui stat membru.	(2) The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.	(2) Certificarea securității cibernetice este voluntară, cu excepția cazurilor în care legislația Republicii Moldova prevede altfel.		Compatibil		
(3) Comisia evaluează periodic eficiența și utilizarea sistemelor europene de certificare a securității cibernetice adoptate și analizează dacă un anumit	(3) The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and	(3) Agenția evaluează periodic eficiența și utilizarea sistemelor naționale de certificare a securității cibernetice aprobate și analizează		Compatibil		

sistem european de certificare a securității cibernetice trebuie să devină obligatoriu prin dreptul relevant al Uniunii, pentru a se asigura un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și, de la 4 februarie 2025, a serviciilor de securitate gestionate în Uniune și pentru a se îmbunătăți funcționarea pieței interne. Prima astfel de evaluare se efectuează până la 31 decembrie 2023, iar evaluările ulterioare se efectuează cel puțin din doi în doi ani după această dată. Pe baza rezultatelor evaluărilor respective, Comisia identifică produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care fac obiectul unui sistem de certificare existent și care trebuie să fie incluse într-un sistem de certificare obligatoriu. Comisia se concentrează cu prioritate pe sectoarele enumerate în anexa II la Directiva (UE) 2016/1148, pe care le evaluează cel târziu la doi ani de la adoptarea primului sistem european de certificare a securității cibernetice. Atunci când pregătește evaluarea, Comisia: (a) ia în considerare impactul măsurilor asupra producătorilor sau furnizorilor de astfel de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, precum și asupra utilizatorilor în ceea ce privește costul măsurilor respective, avantajele societale sau economice care decurg din nivelul sporit de securitate	whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law to ensure an adequate level of cybersecurity of ICT products, ICT services, ICT processes and, from 4 February 2025, managed security services in the Union and improve the functioning of the internal market. The first such assessment shall be carried out by 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services, ICT processes and managed security services covered by an existing certification scheme which are to be covered by a mandatory certification scheme. As a priority, the Commission shall focus on the sectors listed in Annex II to Directive (EU) 2016/1148, which shall be assessed at the latest two years after the adoption of the first European cybersecurity certification scheme. When preparing the assessment the Commission shall: (a) take into account the impact of the measures on the manufacturers or providers of such ICT products, ICT services, ICT processes or managed security services and on the users in terms of the cost of those measures and the societal or economic benefits	dacă un anumit sistem național de certificare a securității cibernetice trebuie să devină obligatoriu, pentru a se asigura un nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate în Republica Moldova și pentru a se îmbunătăți funcționarea pieței interne. (4) Atunci când pregătește evaluarea, Agenția: a) ia în considerare impactul măsurilor asupra producătorilor sau furnizorilor de astfel de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, precum și asupra utilizatorilor în ceea ce privește costul măsurilor respective, avantajele societale sau economice care decurg din nivelul sporit de securitate preconizat pentru produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate vizate; b) ține seama de existența și de punerea în aplicare a sistemelor europene de certificare a securității cibernetice; c) desfășoară un proces de consultare deschis, transparent și cuprinzător cu toate părțile interesate relevante; d) ia în considerare termenele de punere în aplicare, precum și măsurile și perioadele de tranziție, în special în ceea ce privește impactul posibil al măsurilor asupra producătorilor sau a furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, inclusiv asupra intereselor și				

preconizat pentru produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate vizate; (b) ține seama de existența și de punerea în aplicare a dreptului relevant al statelor membre și al țărilor terțe; (c) desfășoară un proces de consultare deschis, transparent și cuprinzător cu toate părțile interesate relevante și cu statele membre; (d) ia în considerare termenele de punere în aplicare, precum și măsurile și perioadele de tranziție, în special în ceea ce privește impactul posibil al măsurilor asupra producătorilor sau a furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, inclusiv asupra intereselor și nevoilor specifice ale IMM-urilor, inclusiv ale microîntreprinderilor; (e) propune cea mai rapidă și mai eficace modalitate de punere în aplicare a tranziției de la un sistem de certificare voluntar la unul obligatoriu.	stemming from the anticipated enhanced level of security for the targeted ICT products, ICT services, ICT processes or managed security services; (b) take into account the existence and implementation of relevant Member State and third country law; (c) carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States; (d) take into account any implementation deadlines, transitional measures and periods, in particular with regard to the possible impact of the measure on the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services, including the specific interests and needs of SMEs, including microenterprises; (e) propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented.	nevoilor specifice ale IMM-urilor, inclusiv ale microîntreprinderilor; e) propune cea mai rapidă și mai eficace modalitate de punere în aplicare a tranziției de la un sistem de certificare voluntar la unul obligatoriu.				
(4) Organismele de evaluare a conformității menționate la articolul 60 eliberează certificate europene de securitate cibernetică în temeiul prezentului articol, care fac trimitere la nivelul de asigurare „de bază” sau „substanțial” pe baza criteriilor incluse în sistemul european de certificare a securității cibernetice adoptat de Comisie în temeiul articolului 49.	(4) The conformity assessment bodies referred to in Article 60 shall issue European cybersecurity certificates pursuant to this Article referring to assurance level ‘basic’ or ‘substantial’ on the basis of criteria included in the European cybersecurity certification scheme adopted by the Commission pursuant to Article 49.	Articolul 16. Emiterea certificatelor de securitate cibernetică (1) Certificatele de securitate cibernetică care fac trimitere la nivelul de asigurare „de bază” sau „substanțial” se emit de organismele de evaluare a conformității acreditate și, după caz, autorizate în condițiile prezentei legi, pe baza criteriilor incluse în sistemul național de certificare.		Compatibil		
(5) Prin derogare de la alineatul (4), în cazuri justificate în mod corespunzător, un sistem	(5) By way of derogation from paragraph 4, in duly justified cases a European	Articolul 16. Emiterea certificatelor de securitate cibernetică		Compatibil		

european de certificare a securității cibernetice poate prevedea că certificatele europene de securitate cibernetică ce rezultă din acel sistem pot fi emise numai de un organism public. Acest organism este una din următoarele entități: (a)o autoritate națională de certificare a securității cibernetice astfel cum este menționată la articolul 58 alineatul (1); sau (b)un organism public care este acreditat ca organism de evaluare a conformității în temeiul articolului 60 alineatul (1).	cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by a public body. Such body shall be one of the following: (a) a national cybersecurity certification authority as referred to in Article 58(1); or (b) a public body that is accredited as a conformity assessment body pursuant to Article 60(1).	(2) Certificatele de securitate cibernetică care fac trimitere la nivelul de asigurare „ridicat” se emit de Agenție sau, în cazurile prevăzute de sistemul național de certificare, de un organism de evaluare a conformității, cu condiția aprobării prealabile a fiecărui certificat de către Agenție ori a delegării generale prealabile a acestei atribuții de către Agenție organismului de evaluare a conformității respectiv.				
(6) În cazurile în care un sistem european de certificare a securității cibernetice adoptat în temeiul articolului 49 impune un nivel de asigurare „ridicat”, certificatul european de securitate cibernetică în temeiul sistemului respectiv se eliberează numai de o autoritate națională de certificare a securității cibernetice sau, în următoarele cazuri, de un organism de evaluare a conformității: (a)cu aprobarea prealabilă a autorității de certificare a securității cibernetice pentru fiecare certificat european de securitate cibernetică individual eliberat de un organism de evaluare a conformității; sau (b)pe baza unei delegări generale a atribuției de eliberare a acestor certificate europene de securitate cibernetică către organismul de evaluare a conformității de către autoritatea națională de	(6) Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level ‘high’, the European cybersecurity certificate under that scheme is to be issued only by a national cybersecurity certification authority or, in the following cases, by a conformity assessment body: (a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conformity assessment body; or (b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the national cybersecurity certification authority.	Articolul 16. Emiterea certificatelor de securitate cibernetică (3) În cazul în care Agenția emite certificate de securitate cibernetică în condițiile alin. (2), subdiviziunea de certificare a Agenției se acreditează ca organism de evaluare a conformității în condițiile art. 20.		Compatibil		

certificare a securității cibernetice.						
(7) Persoana fizică sau juridică care își supune certificării produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pune la dispoziția autorității naționale de certificare a securității cibernetice desemnate în temeiul articolului 58, în cazul în care această autoritate este organismul care eliberează certificatul european de securitate cibernetică, sau la dispoziția organismului de evaluare a conformității menționat la articolul 60 toate informațiile necesare pentru desfășurarea certificării.	(7) The natural or legal person who submits ICT products, ICT services, ICT processes or managed security services for certification shall make available to the national cybersecurity certification authority designated pursuant to Article 58, where that authority is the body issuing the European cybersecurity certificate, or to the conformity assessment body referred to in Article 60 all information necessary to conduct the certification.	Articolul 15. Certificarea securității cibernetice (5) Persoana fizică sau juridică care își supune certificării produsele TIC, serviciile TIC, procesele TIC sau serviciile de securitate gestionate pune la dispoziția Agenției, în cazul în care aceasta este organismul care eliberează certificatul național de securitate cibernetică, sau la dispoziția organismului de evaluare a conformității toate informațiile necesare pentru desfășurarea certificării.		Compatibil		
(8) Deținătorul unui certificat european de securitate cibernetică informează autoritatea sau organismul menționat la alineatul (7) despre orice vulnerabilități sau nereguli detectate ulterior, legate de securitatea produsului TIC, a serviciului TIC, a procesului TIC certificat sau a serviciului de securitate gestionat certificat, care pot avea un impact asupra conformității cu cerințele legate de certificare. Autoritatea sau organismul respectiv transmite aceste informații fără întârzieri nejustificate autorității naționale de certificare a securității cibernetice în cauză.	(8) The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, ICT service, ICT process or managed security service that may have an impact on its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned.	Articolul 17. Menținerea, suspendarea și retragerea certificatelor (1) Titularul certificatului de securitate cibernetică informează organismul emitent sau, după caz, Agenția cu privire la toate vulnerabilitățile sau neregulile detectate ulterior emiterii certificatului, care privesc securitatea produsului TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat certificat, precum și cu privire la orice modificare care poate afecta conformitatea cu cerințele de certificare.		Compatibil		
(9) Certificatele europene de securitate cibernetică se eliberează pentru durata prevăzută de sistemul european de certificare a securității cibernetice și pot fi reînnoite numai dacă sunt îndeplinite în continuare cerințele relevante.	(9) A European cybersecurity certificate shall be issued for the period provided for in the European cybersecurity certification scheme and may be renewed, provided that the relevant requirements continue to be met.	Articolul 16. Emiterea certificatelor de securitate cibernetică (4) Certificatul de securitate cibernetică se emite în baza criteriilor și a procedurilor stabilite de sistemul național de certificare și a raportului de evaluare a conformității, pentru		Compatibil		

		perioada de valabilitate prevăzută de sistem, cu posibilitatea reînnoirii în condițiile acesteia.				
(10) Un certificat european de securitate cibernetică eliberat în temeiul prezentului articol este recunoscut în toate statele membre.	(10) A European cybersecurity certificate issued pursuant to this Article shall be recognised in all Member States.			Prevederi UE direct aplicabile la aderare	Prevederea va deveni direct aplicabilă de la data aderării. Până la această dată, recunoașterea în Republica Moldova a certificatelor europene de securitate cibernetică se realizează în condițiile art. 24 din proiect.	
Articolul 57 **Sistemele și certificatele naționale de certificare de a securității cibernetice**	**Article 57** **National cybersecurity certification schemes and certificates**					
(1) Fără a aduce atingere alineatului (3) din prezentul articol, sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care fac obiectul unui sistem european de certificare a securității cibernetice încetează să mai producă efecte de la data stabilită în actul de punere în aplicare adoptat în temeiul articolului 49 alineatul (7). Sistemele naționale de certificare a securității cibernetice și procedurile aferente pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care nu fac obiectul unui sistem european de certificare a securității cibernetice continuă să existe.	(1) Without prejudice to paragraph 3 of this Article, national cybersecurity certification schemes, and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). National cybersecurity certification schemes and the related procedures for the ICT products, ICT services, ICT processes and managed security services that are not covered by a European cybersecurity certification scheme shall continue to exist.	Articolul 14. Corelarea sistemelor naționale cu sistemele europene de certificare (2) Fiecare sistem național de certificare include clauze de tranziție aplicabile în cazul recunoașterii în Republica Moldova a unui sistem european de certificare care acoperă aceleași tipuri sau categorii de produse TIC, servicii TIC, procese TIC ori servicii de securitate gestionate, inclusiv privind încetarea, în tot sau în parte, a efectelor sistemului național.		Parțial compatibil	Prevederea este preluată cu adaptarea necesară perioadei anterioare aderării: încetarea efectelor sistemului național este raportată la recunoașterea în Republica Moldova, în condițiile art. 24 din proiect, a sistemului european de certificare care acoperă aceleași tipuri sau categorii de produse, servicii sau procese. De la data aderării, art. 57 din Regulament va deveni direct aplicabil.	
(2) Statele membre nu introduc noi sisteme naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele	(2) Member States shall not introduce new national cybersecurity certification schemes for ICT products, ICT services, ICT processes and	(1) Nu se elaborează și nu se aprobă sisteme naționale de certificare pentru tipurile sau categoriile de produse TIC, servicii TIC, procese TIC ori		Parțial compatibil	Interdicția este raportată la sistemele europene de certificare ale căror certificate sunt recunoscute în	

TIC și serviciile de securitate gestionate care fac deja obiectul unui sistem european de certificare a securității cibernetice în vigoare.	managed security services already covered by a European cybersecurity certification scheme that is in force.	servicii de securitate gestionate acoperite de o un sistem european de certificare a securității cibernetice ale cărei certificate sunt recunoscute în Republica Moldova în condițiile art. 24, cu excepția cazurilor justificate de motive de interes public.			Republica Moldova în condițiile art. 24 din proiect. Excepția privind motivele de interes public nu este prevăzută în Regulament; de la data aderării, se va aplica direct art. 57 alin. (2) din Regulament.	
(3) Certificatele existente care au fost eliberate în temeiul sistemelor naționale de certificare a securității cibernetice și care fac obiectul unui sistem european de certificare a securității cibernetice rămân valabile până la data expirării lor.	(3) Existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.	(3) În cazul încetării efectelor unui sistem național de certificare în condițiile alin. (2), certificatele de securitate cibernetică emise anterior în cadrul acesteia rămân valabile până la data expirării lor, fără posibilitatea reînnoirii pentru domeniile acoperite de sistemul european recunoscut.		Compatibil		
(4) Pentru a se evita fragmentarea pieței interne, statele membre informează Comisia și ECCG cu privire la orice intenție de a elabora noi sisteme naționale de certificare a securității cibernetice.	(4) With a view to avoiding the fragmentation of the internal market, Member States shall inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes.			Prevederi UE direct aplicabile la aderare	Obligația de informare a Comisiei Europene și a ECCG va deveni aplicabilă de la data aderării.	
Articolul 58 **Autoritățile naționale de certificare a securității cibernetice**	**Article 58** **National cybersecurity certification authorities**	**Articolul 4. Autoritatea națională de certificare a securității cibernetice**				
(1) Fiecare stat membru desemnează pe teritoriul său una sau mai multe autorități naționale de certificare a securității cibernetice sau, cu acordul unui alt stat membru, desemnează una sau mai multe autorități naționale de certificare a securității cibernetice stabilite în celălalt stat membru pentru a fi responsabile de atribuțiile de supraveghere în statul membru care face desemnarea.	(1) Each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State.	Agenția pentru Securitate Cibernetică (în continuare – Agenția) este desemnată în calitate de autoritate națională de certificare a securității cibernetice.		Compatibil		
(2) Fiecare stat membru informează Comisia cu privire la identitatea autorităților naționale de certificare de securitate	(2) Each Member State shall inform the Commission of the identity of the designated national cybersecurity			Prevederi UE direct aplicabile la aderare	Obligația de informare a Comisiei Europene va deveni aplicabilă de la data aderării.	

cibernetică desemnate. În cazul în care un stat membru desemnează mai multe autorități, acesta informează Comisia și cu privire la sarcinile atribuite fiecăreia dintre respectivele autorități.	certification authorities. Where a Member State designates more than one authority, it shall also inform the Commission about the tasks assigned to each of those authorities.					
(3) Fără a aduce atingere articolului 56 alineatul (5) litera (a) și articolului 56 alineatul (6), fiecare autoritate națională de certificare a securității cibernetice este independentă în ceea ce privește organizarea, deciziile de finanțare, structura juridică și luarea deciziilor, de entitățile pe care le supraveghează.	(3) Without prejudice to point (a) of Article 56(5) and Article 56(6), each national cybersecurity certification authority shall be independent of the entities it supervises in its organisation, funding decisions, legal structure and decision-making.	(2) În exercitarea atribuțiilor prevăzute de prezenta lege, Agenția este independentă, în ceea ce privește organizarea, luarea deciziilor și structura juridică, de entitățile pe care le supraveghează.		Compatibil		
(4) Statele membre se asigură că activitățile autorităților naționale de certificare a securității cibernetice, care se referă la eliberarea de certificate europene de securitate cibernetică menționate la articolul 56 alineatul (5) litera (a) și la articolul 56 alineatul (6) sunt strict separate de activitățile de supraveghere prevăzute în prezentul articol și că activitățile respective sunt desfășurate independent una de cealaltă.	(4) Member States shall ensure that the activities of the national cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in this Article and that those activities are carried out independently from each other.	(3) Activitățile Agenției aferente emiterii certificatelor de securitate cibernetică, exercitate în condițiile art. 16 alin. (2), sunt strict separate, din punct de vedere organizatoric și funcțional, de activitățile de supraveghere prevăzute de prezenta lege și se desfășoară independent unele de celelalte.		Compatibil		
(5) Statele membre se asigură că autoritățile naționale de certificare a securității cibernetice dispun de resursele adecvate pentru a-și exercita competențele și pentru a-și îndeplini cu eficacitate și în mod eficient sarcinile.	(5) Member States shall ensure that national cybersecurity certification authorities have adequate resources to exercise their powers and to carry out their tasks in an effective and efficient manner.			Prevederi UE neacoperite de măsuri naționale	Prevederea nu necesită reglementare la nivel de lege. Asigurarea resurselor adecvate ale Agenției se va realiza prin măsuri organizatorice și bugetare: suplimentarea efectivului-limită al Agenției cu 4 unități de personal, cu ajustarea corespunzătoare a Hotărârii Guvernului nr. 1028/2023, și alocarea mijloacelor financiare	

					aferente, conform estimărilor din compartimentul 4.2 al notei de fundamentare.	
(6) Pentru punerea efectivă în aplicare a prezentului regulament, este oportun ca autoritățile naționale de certificare a securității cibernetice să participe la ECCG în mod activ, eficace, eficient și sigur.	(6) For the effective implementation of this Regulation, it is appropriate that national cybersecurity certification authorities participate in the ECCG in an active, effective, efficient and secure manner.			Prevederi UE direct aplicabile la aderare	Participarea Agenției la activitatea ECCG va deveni posibilă de la data aderării.	
(7) Autoritățile naționale de certificare a securității cibernetice: (a) supraveghează și asigură respectarea normelor incluse în sistemele europene de certificare a securității cibernetice în temeiul articolului 54 alineatul (1) litera (j) pentru monitorizarea conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate cu cerințele certificatelor europene de securitate cibernetică care au fost eliberate pe teritoriile lor respective, în cooperare cu alte autorități relevante de supraveghere a pieței; (b) monitorizează și asigură respectarea obligațiilor producătorilor sau furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate care sunt stabiliți pe teritoriile lor respective și care desfășoară autoevaluări ale conformității și, în special, monitorizează și asigură respectarea obligațiilor unor astfel de producători sau furnizori prevăzute la articolul 53 alineatele (2) și (3) și în sistemele europene de certificare a securității cibernetice corespunzătoare;	(7) National cybersecurity certification authorities shall: (a) supervise and enforce rules included in European cybersecurity certification schemes pursuant to Article 54(1), point (j), for the monitoring of the compliance of ICT products, ICT services, ICT processes and managed security services with the requirements of the European cybersecurity certificates that have been issued in their respective territories, in cooperation with other relevant market surveillance authorities; (b) monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services, ICT processes or managed security services that are established in their respective territories and that carry out conformity self-assessment, and shall, in particular, monitor compliance with and enforce the obligations of such manufacturers or providers set out in Article 53(2) and (3) and in the corresponding European cybersecurity certification scheme;	Articolul 5. Atribuțiile autorității naționale de certificare a securității cibernetice (1) Agenția, în calitate de autoritate națională de certificare a securității cibernetice, exercită următoarele atribuții: a) supraveghează și asigură respectarea normelor incluse în sistemele naționale de certificare a securității cibernetice, inclusiv a normelor de monitorizare a conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate cu cerințele certificatelor de securitate cibernetică emise pe teritoriul Republicii Moldova, în cooperare cu alte autorități competente de supraveghere a pieței; b) monitorizează și asigură respectarea obligațiilor producătorilor și furnizorilor de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate stabiliți pe teritoriul Republicii Moldova care efectuează autoevaluarea conformității, inclusiv a obligațiilor prevăzute la art. 18; c) asistă și sprijină organismul național de acreditare la monitorizarea și supravegherea activităților organismelor de		Compatibil		

(c) fără a aduce atingere articolului 60 alineatul (3), asistă și sprijină activ organismele naționale de acreditare la monitorizarea și supravegherea activităților organismelor de evaluare a conformității în sensul prezentului regulament; (d) monitorizează și supraveghează activitățile organismelor publice menționate la articolul 56 alineatul (5); (e) după caz, autorizează organismele de evaluare a conformității în conformitate cu articolul 60 alineatul (3) și restricționează, suspendă sau retrag autorizația existentă atunci când organismele de evaluare a conformității încalcă cerințele prezentului regulament; (f) tratează plângerile persoanelor fizice sau juridice în legătură cu certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cu cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 56 alineatul (6), sau în legătură cu declarațiile de conformitate UE eliberate în temeiul articolului 53, și investighează, în măsura în care este oportun, subiectul plângerii și informează reclamantul despre stadiul și rezultatul investigației, într-un termen rezonabil; (g) prezintă ENISA și ECCG un raport anual de sinteză privind măsurile întreprinse	(c) without prejudice to Article 60(3), actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of conformity assessment bodies, for the purposes of this Regulation; (d) monitor and supervise the activities of the public bodies referred to in Article 56(5); (e) where applicable, authorise conformity assessment bodies in accordance with Article 60(3) and restrict, suspend or withdraw existing authorisation where conformity assessment bodies infringe the requirements of this Regulation; (f) handle complaints by natural or legal persons in relation to European cybersecurity certificates issued by national cybersecurity certification authorities or to European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6) or in relation to EU statements of conformity issued under Article 53, and shall investigate the subject matter of such complaints to the extent appropriate, and shall inform the complainant of the progress and the outcome of the investigation within a reasonable period; (g) provide an annual summary report on the activities conducted under points (b), (c) and (d) of this paragraph or under paragraph 8 to ENISA and the ECCG;	evaluare a conformității în sensul prezentei legi, fără a aduce atingere competențelor acestuia stabilite prin Legea nr. 235/2011; d) autorizează organismele de evaluare a conformității în condițiile art. 21 și restricționează, suspendă sau retrage autorizația în cazul în care organismele de evaluare a conformității încalcă cerințele prezentei legi sau ale sistemelor naționale de certificare; e) examinează plângerile persoanelor fizice sau juridice în condițiile art. 29 și informează reclamantul despre stadiul și rezultatul examinării; f) elaborează, cu consultarea părților interesate, proiectele sistemelor naționale de certificare a securității cibernetice și le propune spre aprobare în condițiile art. 9; g) ține evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate și asigură caracterul public al acestuia în condițiile art. 26; h) cooperează cu autoritățile de certificare a securității cibernetice din alte state, cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și cu alte structuri europene și internaționale relevante, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate cu cerințele aplicabile; i) monitorizează evoluțiile relevante din domeniul certificării securității cibernetice, inclusiv evoluția sistemului				

în temeiul literelor (b), (c) și (d) din prezentul alineat sau în temeiul alineatului (8); (h) cooperează cu alte autorități naționale de certificare a securității cibernetice sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor TIC, a serviciilor TIC, a proceselor TIC sau a serviciilor de securitate gestionate cu cerințele prezentului regulament sau cu cerințele sistemelor europene de certificare a securității cibernetice specifice; și (i) monitorizează evoluțiile relevante din domeniul certificării securității cibernetice.	(h) cooperate with other national cybersecurity certification authorities or other public authorities, including by sharing information on the possible non-compliance of ICT products, ICT services, ICT processes or managed security services with the requirements of this Regulation or with the requirements of specific European cybersecurity certification schemes; and (i) monitor relevant developments in the field of cybersecurity certification.	european de certificare a securității cibernetice; j) elaborează și publică anual pe pagina sa web oficială un raport de sinteză privind activitatea de certificare a securității cibernetice și măsurile întreprinse în temeiul prezentei legi; k) promovează certificarea securității cibernetice și informează opinia publică, producătorii, furnizorii și utilizatorii cu privire la beneficiile și condițiile acesteia. (2) Atribuțiile prevăzute la alin. (1) se exercită în conformitate cu procedurile stabilite de prezenta lege, de sistemele naționale de certificare și de actele normative aprobate în vederea executării prezentei legi.				
(8) Fiecare autoritate națională de certificare a securității cibernetice 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 declarații de conformitate UE să furnizeze toate informațiile care îi sunt necesare pentru îndeplinirea atribuțiilor 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 declarații de conformitate UE pentru a verifica conformitatea acestora cu prezentul titlu;	(8) Each national cybersecurity certification authority shall have at least the following powers: (a) to request conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires for the performance of its tasks; (b) to carry out investigations, in the form of audits, of conformity assessment bodies, European cybersecurity certificates' holders and issuers of EU statements of conformity, for the purpose of verifying their compliance with this Title; (c) to take appropriate measures, in accordance with national law, to ensure that conformity assessment bodies,	Articolul 6. Competențele autorității naționale de certificare a securității cibernetice (1) În vederea exercitării atribuțiilor prevăzute la art. 5, Agenția dispune de următoarele competențe: a) să solicite organismelor de evaluare a conformității, titularilor de certificate de securitate cibernetică și entităților care emit declarații de conformitate să furnizeze toate informațiile necesare pentru îndeplinirea atribuțiilor sale; b) să efectueze investigații, sub formă de audituri sau controale, asupra organismelor de evaluare a conformității, a titularilor de certificate de securitate cibernetică și a entităților care emit declarații de conformitate, pentru a verifica respectarea prevederilor prezentei legi și ale		Compatibil		

(c)competența de a lua măsuri adecvate, în conformitate cu dreptul intern, pentru a se asigura că organismele de evaluare a conformității, titularii de certificate europene de securitate cibernetică și entitățile care eliberează declarații de conformitate UE respectă prezentul regulament sau un sistem european de certificare a securității cibernetice; (d)competența de a obține acces la sediile oricărui organism de evaluare a conformității sau al titularilor de certificate europene de securitate cibernetică cu scopul de a desfășura investigații în conformitate cu dreptul procedural al Uniunii sau al statului membru; (e)competența de a retrage, în conformitate cu dreptul intern, certificatele europene de securitate cibernetică eliberate de autoritățile naționale de certificare a securității cibernetice sau cele eliberate de organismele de evaluare a conformității în conformitate cu articolul 56 alineatul (6), atunci când astfel de certificate nu sunt conforme cu prezentul regulament sau cu un sistem european de certificare a securității cibernetice; (f)competența de a impune sancțiuni, în conformitate cu dreptul intern, astfel cum se prevede la articolul 65, și de a cere încetarea imediată a încălcărilor obligațiilor prevăzute de prezentul regulament.	European cybersecurity certificates' holders and issuers of EU statements of conformity comply with this Regulation or with a European cybersecurity certification scheme; (d) to obtain access to the premises of any conformity assessment bodies or holders of European cybersecurity certificates, for the purpose of carrying out investigations in accordance with Union or Member State procedural law; (e) to withdraw, in accordance with national law, European cybersecurity certificates issued by the national cybersecurity certification authorities or European cybersecurity certificates issued by conformity assessment bodies in accordance with Article 56(6), where such certificates do not comply with this Regulation or with a European cybersecurity certification scheme; (f) to impose penalties in accordance with national law, as provided for in Article 65, and to require the immediate cessation of infringements of the obligations set out in this Regulation.	sistemelor naționale de certificare; c) să dispună măsuri adecvate, în conformitate cu legislația, pentru a asigura că organismele de evaluare a conformității, titularii de certificate de securitate cibernetică și entitățile care emit declarații de conformitate respectă prezenta lege și sistemele naționale de certificare; d) să obțină acces, în condițiile legii, la sediile organismelor de evaluare a conformității și ale titularilor de certificate de securitate cibernetică, în scopul desfășurării investigațiilor prevăzute la lit. b); e) să retragă, în condițiile prezentei legi și ale sistemelor naționale de certificare, certificatele de securitate cibernetică emise de Agenție sau de organismele de evaluare a conformității, atunci când acestea nu sunt conforme cu prezenta lege sau cu sistemul național de certificare; f) să aplice sancțiuni în condițiile art. 38 și să ceară încetarea imediată a încălcărilor obligațiilor prevăzute de prezenta lege. (2) Controalele asupra activității de întreprinzător se planifică, se efectuează și se înregistrează în condițiile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător.				

(9) Autoritățile naționale de certificare a securității cibernetice cooperează între ele și cu Comisia, în special prin schimb de informații, de experiență și de bune practici în ceea ce privește certificarea securității cibernetice și aspectele tehnice privind securitatea cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate.	(9) National cybersecurity certification authorities shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning the cybersecurity of ICT products, ICT services, ICT processes and managed security services.			Prevederi UE direct aplicabile la aderare	Cooperarea Agenției cu autoritățile de certificare a securității cibernetice din alte state și cu ENISA, inclusiv prin schimbul de informații, de experiență și de bune practici, este prevăzută la art. 5 alin. (1) lit. h) și la art. 8 alin. (4) din proiect. Cooperarea cu autoritățile naționale de certificare ale statelor membre și cu Comisia Europeană va deveni aplicabilă de la data aderării.	
Articolul 59 **Evaluarea inter pares**	**Article 59** **Peer review**				Alin. (1)–(4) vor deveni aplicabile Agenției, în calitate de autoritate națională de certificare a securității cibernetice, de la data aderării. Alin. (5) și (6) se referă la activitatea Comisiei Europene și a ECCG.	
(1) Pentru a se ajunge la standarde echivalente pe întreg teritoriul Uniunii cu privire la certificatele europene de securitate cibernetică și la declarațiile de conformitate UE, autoritățile naționale de certificare a securității cibernetice fac obiectul unei evaluări inter pares.	(1) With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, national cybersecurity certification authorities shall be subject to peer review.			Prevederi UE direct aplicabile la aderare		
(2) Evaluarea inter pares se efectuează pe baza unor criterii și proceduri de evaluare clare și transparente, în special în privința cerințelor structurale, de resurse umane și de proces, a confidențialității și a plângerilor.	(2) Peer review shall be carried out on the basis of sound and transparent evaluation criteria and procedures, in particular concerning structural, human resource and process requirements, confidentiality and complaints.			Prevederi UE direct aplicabile la aderare		
(3) Evaluarea *inter pares* examinează următoarele aspecte:	(3) Peer review shall assess: (a) where applicable, whether the activities of the national			Prevederi UE direct aplicabile la aderare		

(a)după caz, dacă activitățile autorităților naționale de certificare a securității cibernetice legate de eliberarea certificatelor europene de securitate cibernetică menționate la articolul 56 alineatul (5) litera (a) și la articolul 56 alineatul (6) sunt strict separate de activitățile de supraveghere prevăzute la articolul 58 și dacă activitățile respective sunt desfășurate independent una de cealaltă; (b)procedurile de supraveghere și de asigurare a respectării normelor de monitorizare a conformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate cu certificatele europene de securitate cibernetică în temeiul articolului 58 alineatul (7) litera (a); (c)procedurile de monitorizare și de asigurare a respectării obligațiilor producătorilor și ale furnizorilor de produse TIC, de servicii TIC, de procese TIC sau de servicii de securitate gestionate în conformitate cu articolul 58 alineatul (7) litera (b); (d)procedurile de monitorizare, de autorizare și de supraveghere a activităților desfășurate de organismele de evaluare a conformității; (e)după caz, dacă personalul autorităților sau organismelor care eliberează certificate pentru nivelul de asigurare „ridicat” în temeiul articolului 56 alineatul (6) deține expertiza corespunzătoare.	cybersecurity certification authorities that relate to the issuance of European cybersecurity certificates referred to in point (a) of Article 56(5) and in Article 56(6) are strictly separated from their supervisory activities set out in Article 58 and whether those activities are carried out independently from each other; (b) the procedures for supervising and enforcing the rules for monitoring the compliance of ICT products, ICT services, ICT processes and managed security services with European cybersecurity certificates pursuant to Article 58(7), point (a); (c) the procedures for monitoring and enforcing the obligations of manufacturers or providers of ICT products, ICT services, ICT processes or managed security services pursuant to Article 58(7), point (b); (d) the procedures for monitoring, authorising and supervising the activities of the conformity assessment bodies; (e) where applicable, whether the staff of authorities or bodies that issue certificates for assurance level ‘high’ pursuant to Article 56(6) have the appropriate expertise.					

(4) Evaluarea *inter pares* se desfășoară cel puțin o dată la cinci ani de către cel puțin două autorități naționale de certificare a securității cibernetice din alte state membre și de către Comisie. ENISA poate participa la evaluarea *inter pares*.	(4) Peer review shall be carried out by at least two national cybersecurity certification authorities of other Member States and the Commission and shall be carried out at least once every five years. ENISA may participate in the peer review.			Prevederi UE direct aplicabile la aderare		
(5) Comisia poate adopta acte de punere în aplicare prin care să stabilească un plan pentru evaluarea *inter pares*, care acoperă o perioadă de cel puțin cinci ani, și să definească criterii privind componența echipei de evaluare *inter pares*, metodologia utilizată pentru evaluarea *inter pares*, calendarul, frecvența și alte atribuții legate de aceasta. Atunci când adoptă respectivele acte de punere în aplicare, Comisia ține seama în mod corespunzător de observațiile formulate de ECCG. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 66 alineatul (2).	(5) The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. In adopting those implementing acts, the Commission shall take due account of the views of the ECCG. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).			Prevederi UE neaplicabile		
(6) Rezultatele evaluării *inter pares* sunt examinate de ECCG, care întocmește un rezumat ce poate fi făcut public, și care, atunci când este necesar, formulează orientări sau recomandări cu privire la acțiunile sau măsurile care trebuie întreprinse de entitățile în cauză.	(6) The outcomes of peer reviews shall be examined by the ECCG, which shall draw up summaries that may be made publicly available and which shall, where necessary, issue guidelines or recommendations on actions or measures to be taken by the entities concerned.			Prevederi UE neaplicabile		
Articolul 60 **Organisme de evaluare a conformității**	**Article 60** **Conformity assessment bodies**	**Capitolul V** **ORGANISMELE DE EVALUARE A CONFORMITĂȚII**				
(1) Organismele de evaluare a conformității sunt acreditate de organismele naționale de	(1) The conformity assessment bodies shall be accredited by national accreditation bodies	Articolul 20. Acreditarea organismelor de evaluare a conformității		Compatibil		

acreditare desemnate în temeiul Regulamentului (CE) nr. 765/2008. Acreditarea respectivă se eliberează numai dacă organismul național de acreditare îndeplinește cerințele stabilite în anexa la prezentul regulament.	appointed pursuant to Regulation (EC) No 765/2008. Such accreditation shall be issued only where the conformity assessment body meets the requirements set out in the Annex to this Regulation.	(1) Organismele de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare a securității cibernetice se acreditează de organismul național de acreditare în conformitate cu Legea nr. 235/2011. Acreditarea se acordă numai organismelor de evaluare a conformității care îndeplinesc cerințele prevăzute la art. 22.				
(2) În cazurile în care un certificat european de securitate cibernetică este eliberat de o autoritate națională de certificare a securității cibernetice în temeiul articolului 56 alineatul (5) litera (a) și al articolului 56 alineatul (6), organismul de certificare al autorității naționale de certificare a securității cibernetice este acreditat ca organism de evaluare a conformității în temeiul alineatului (1) din prezentul articol.	(2) Where a European cybersecurity certificate is issued by a national cybersecurity certification authority pursuant to point (a) of Article 56(5) and Article 56(6), the certification body of the national cybersecurity certification authority shall be accredited as a conformity assessment body pursuant to paragraph 1 of this Article.	Articolul 16. Emiterea certificatelor de securitate cibernetică (3) În cazul în care Agenția emite certificate de securitate cibernetică în condițiile alin. (2), subdiviziunea de certificare a Agenției se acreditează ca organism de evaluare a conformității în condițiile art. 20. Articolul 20. Acreditarea organismelor de evaluare a conformității (1) Organismele de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare a securității cibernetice se acreditează de organismul național de acreditare în conformitate cu Legea nr. 235/2011. Acreditarea se acordă numai organismelor de evaluare a conformității care îndeplinesc cerințele prevăzute la art. 22.		Compatibil		
(3) În cazul în care sistemele europene de certificare a securității cibernetice stabilesc cerințe specifice sau suplimentare în temeiul articolului 54 alineatul (1) litera (f), numai organismele de evaluare a conformității care îndeplinesc aceste cerințe sunt autorizate de autoritatea națională de certificare a	(3) Where European cybersecurity certification schemes set out specific or additional requirements pursuant to point (f) of Article 54(1), only conformity assessment bodies that meet those requirements shall be authorised by the national cybersecurity certification	Articolul 21. Autorizarea organismelor de evaluare a conformității (1) În cazul în care un sistem național de certificare stabilește cerințe specifice sau suplimentare în condițiile art. 12 alin. (1) lit. f), numai organismele de evaluare a conformității care îndeplinesc aceste cerințe sunt autorizate de Agenție pentru		Compatibil		

securității cibernetice pentru îndeplinirea atribuțiilor în temeiul sistemelor respective.	authority to carry out tasks under such schemes.	îndeplinirea atribuțiilor în temeiul sistemului respectiv. (2) Procedura de autorizare, documentele necesare, termenele de examinare, precum și temeiurile de restricționare, suspendare și retragere a autorizației se stabilesc prin regulament aprobat de Guvern, cu respectarea principiilor transparenței, imparțialității și proporționalității. (3) Agenția ține evidența organismelor de evaluare a conformității acreditate, autorizate și recunoscute și o publică pe pagina sa web oficială.				
(4) Acreditarea menționată la alineatul (1) se eliberează organismelor de evaluare a conformității pentru o perioadă de maximum cinci ani și poate fi reînnoită în aceleași condiții numai dacă organismul de evaluare a conformității îndeplinește în continuare cerințele prevăzute la prezentul articol. Organismele naționale 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 eliberată în temeiul alineatului (1) în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite sau în cazul în care organismul de evaluare a conformității încalcă prezentul regulament.	(4) The accreditation referred to in paragraph 1 shall be issued to the conformity assessment bodies for a maximum of five years and may be renewed on the same conditions, provided that the conformity assessment body still meets the requirements set out in this Article. National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a conformity assessment body issued pursuant to paragraph 1 where the conditions for the accreditation have not been met or are no longer met, or where the conformity assessment body infringes this Regulation.	Articolul 20. Acreditarea organismelor de evaluare a conformității (2) Acreditarea se acordă pentru o perioadă de 4 ani, cu efectuarea supravegherii periodice pe durata ciclului de acreditare, și poate fi reînnoită în condițiile prevăzute de Legea nr. 235/2011, dacă organismul de evaluare a conformității continuă să îndeplinească cerințele de acreditare. (3) Organismul național de acreditare ia toate măsurile corespunzătoare, pentru a restrânge, a suspenda sau a retrage acreditarea unui organism de evaluare a conformității în cazul în care condițiile de acreditare nu sunt sau nu mai sunt îndeplinite ori în cazul în care organismul de evaluare a conformității încalcă prezenta lege. (4) Organismul național de acreditare informează Agenția, în termen de 3 zile lucrătoare, cu privire la acordarea, restrângerea, suspendarea, retragerea sau		Compatibil		

		reînnoirea acreditării organismelor de evaluare a conformității în domeniul securității cibernetice.				
Articolul 61 **Notificare**	**Article 61** **Notification**				Alin. (1) și (4) vor deveni aplicabile Agenției de la data aderării. Alin. (2), (3) și (5) se referă la activitatea Comisiei Europene.	
(1) Pentru fiecare sistem european de certificare a securității cibernetice, autoritățile naționale de certificare a securității cibernetice îi notifică Comisiei organismele de evaluare a conformității care au fost acreditate și, după caz, autorizate în temeiul articolului 60 alineatul (3) să elibereze certificate europene de securitate cibernetică la nivelurile de asigurare specificate menționate la articolul 52. Autoritățile naționale de certificare a securității cibernetice îi notifică Comisiei, fără nicio întârziere nejustificată, orice modificare ulterioară referitoare la acestea.	(1) For each European cybersecurity certification scheme, the national cybersecurity certification authorities shall notify the Commission of the conformity assessment bodies that have been accredited and, where applicable, authorised pursuant to Article 60(3) to issue European cybersecurity certificates at specified assurance levels as referred to in Article 52. The national cybersecurity certification authorities shall notify the Commission of any subsequent changes thereto without undue delay.			Prevederi UE direct aplicabile la aderare		
(2) La un an de la intrarea în vigoare a unui sistem european de certificare a securității cibernetice, Comisia publică în *Jurnalul Oficial al Uniunii Europene* o listă a organismelor de evaluare a conformității notificate în temeiul sistemului respectiv.	(2) One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of the conformity assessment bodies notified under that scheme in the Official Journal of the European Union.			Prevederi UE neaplicabile		
(3) În cazul în care primește o notificare după expirarea perioadei menționate la alineatul (2), Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările listei a organismelor de evaluare a	(3) If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the			Prevederi UE neaplicabile		

conformității notificate, în termen de două luni de la data primirii notificării respective.	Official Journal of the European Union within two months of the date of receipt of that notification.					
(4) O autoritate națională de certificare a securității cibernetice poate înainta Comisiei o cerere de retragere a unui organism de evaluare a conformității notificat de autoritatea respectivă din lista menționată la alineatul (2). Comisia publică în *Jurnalul Oficial al Uniunii Europene* modificările corespunzătoare aduse listei respective, în termen de o lună de la data primirii cererii adresate de autoritatea națională de certificare a securității cibernetice.	(4) A national cybersecurity certification authority may submit to the Commission a request to remove a conformity assessment body notified by that authority from the list referred to in paragraph 2. The Commission shall publish the corresponding amendments to that list in the Official Journal of the European Union within one month of the date of receipt of the national cybersecurity certification authority's request.			Prevederi UE direct aplicabile la aderare		
(5) Comisia poate adopta acte de punere în aplicare prin care 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 66 alineatul (2).	(5) The Commission may adopt implementing acts to establish the circumstances, formats and procedures for notifications referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 66(2).			Prevederi UE neaplicabile		
Articolul 62 **Grupul european pentru certificarea securității cibernetice**	**Article 62** **European Cybersecurity Certification Group**				Prevederile se referă la ECCG, organ instituit la nivelul Uniunii Europene, și nu necesită măsuri naționale de punere în aplicare. Participarea Agenției la activitatea ECCG va deveni posibilă de la data aderării.	
(1) Se instituie Grupul european pentru certificarea securității cibernetice (ECCG).	(1) The European Cybersecurity Certification Group (the 'ECCG') shall be established.			Prevederi UE neaplicabile		
(2) ECCG este compus din reprezentanți ai autorităților	(2) The ECCG shall be composed of representatives			Prevederi UE neaplicabile		

naționale de certificare a securității cibernetice sau din reprezentanți ai altor autorități naționale relevante. Niciun membru ECCG nu poate reprezenta mai mult de două state membre.	of national cybersecurity certification authorities or representatives of other relevant national authorities. A member of the ECCG shall not represent more than two Member States.					
(3) Părțile interesate și părțile terțe relevante pot fi invitate să participe la reuniunile ECCG și la activitățile acestuia.	(3) Stakeholders and relevant third parties may be invited to attend meetings of the ECCG and to participate in its work.			Prevederi UE neaplicabile		
(4) ECCG are următoarele atribuții: (a)să acorde consiliere și asistență Comisiei în activitatea sa de asigurare a punerii în practică și a aplicării coerente a prezentului titlu, în special în ceea ce privește programul de activitate etapizat la nivelul Uniunii, chestiunile legate de politica în materie de certificare a securității cibernetice, coordonarea abordărilor privind politicile și pregătirea unor sisteme europene de certificare a securității cibernetice; (b)să acorde asistență și consiliere ENISA și să coopereze cu aceasta în legătură cu pregătirea unei propuneri de sistem în temeiul articolului 49; (c)să adopte un aviz cu privire la propunerea de sistem pregătită de ENISA în temeiul articolului 49; (d)să solicite ENISA să pregătească propuneri de sistem în temeiul articolului 48 alineatul (2); (e)să adopte avize adresate Comisiei cu privire la întreținerea și revizuirea sistemelor europene de	(4) The ECCG shall have the following tasks: (a) to advise and assist the Commission in its work to ensure the consistent implementation and application of this Title, in particular regarding the Union rolling work programme, cybersecurity certification policy issues, the coordination of policy approaches, and the preparation of European cybersecurity certification schemes; (b) to assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme pursuant to Article 49; (c) to adopt an opinion on candidate schemes prepared by ENISA pursuant to Article 49; (d) to request ENISA to prepare candidate schemes pursuant to Article 48(2); (e) to adopt opinions addressed to the Commission relating to the maintenance and review of existing European cybersecurity certifications schemes; (f) to examine relevant developments in the field of cybersecurity certification and to exchange information and			Prevederi UE neaplicabile		

certificare a securității cibernetice existente; (f)să examineze evoluțiile relevante din domeniul securității cibernetice și să facă schimb de informații și de bune practici privind sistemele de certificare a securității cibernetice; (g)să faciliteze cooperarea dintre autoritățile naționale de certificare a securității cibernetice 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 chestiunile privind certificarea securității cibernetice; (h)să sprijine punerea în aplicare a mecanismelor de evaluare *inter pares* în conformitate cu normele stabilite în cadrul unui sistem european de certificare a securității cibernetice în temeiul articolului 54 alineatul (1) litera (u); (i)să faciliteze alinierea sistemelor europene de certificare a securității cibernetice la standardele recunoscute pe plan internațional, inclusiv prin revizuirea actualelor sisteme europene de certificare a securității cibernetice și, după caz, recomandând ENISA să colaboreze cu organizațiile internaționale de standardizare relevante pentru a remedia insuficiențele sau lacunele care afectează standardele internaționale	good practices on cybersecurity certification schemes; (g) to facilitate the cooperation between national cybersecurity certification authorities under this Title through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to issues concerning cybersecurity certification; (h) to support the implementation of peer assessment mechanisms in accordance with the rules established in a European cybersecurity certification scheme pursuant to point (u) of Article 54(1); (i) to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity certification schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards.					

recunoscute care sunt în vigoare.						
(5) Comisia prezidează ECCG cu asistență din partea ENISA și asigură secretariatul acestuia în conformitate cu articolul 8 alineatul (1) litera (e).	(5) With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1).			Prevederi UE neaplicabile		
Articolul 63 **Dreptul de a depune o plângere**	**Article 63** **Right to lodge a complaint**	**Articolul 29. Dreptul de a depune plângere**				
(1) Persoanele fizice sau juridice au dreptul să depună o plângere la entitatea care a eliberat un certificat european de securitate cibernetică sau, dacă plângerea se referă la un certificat european de securitate cibernetică eliberat de un organism de evaluare a conformității în temeiul articolului 56 alineatul (6), la autoritatea națională relevantă de certificare a securității cibernetice.	(1) Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 56(6), with the relevant national cybersecurity certification authority.	(1) Persoanele fizice sau juridice au dreptul să depună o plângere la Agenție în legătură cu potențialele încălcări ale prezentei legi.		Compatibil		
(2) Autoritatea sau organismul la care s-a depus plângerea informează reclamantul despre evoluția procedurilor și despre decizia luată, și despre dreptul de a exercita o cale de atac eficientă în temeiul articolului 64.	(2) The authority or body with which the complaint has been lodged shall inform the complainant of the progress of the proceedings and of the decision taken, and shall inform the complainant of the right to an effective judicial remedy referred to in Article 64.	(5) Agenția informează autorul plângerii cu privire la evoluția și rezultatul plângerii, inclusiv cu privire la posibilitatea de a contesta actele acestuia în conformitate cu art. 30.		Compatibil		
Articolul 64 **Dreptul la o cale de atac eficientă**	**Article 64** **Right to an effective judicial remedy**	**Articolul 30. Dreptul de a contesta acțiunile sau inacțiunile**				
(1) În pofida oricăror căi de atac administrative sau a altor căi de atac fără caracter judiciar, persoanele fizice și juridice au dreptul să exercite o cale de atac eficientă cu privire la: (a)deciziile luate de autoritatea sau organismul menționat la articolul 63 alineatul (1),	(1) Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to: (a) decisions taken by the authority or body referred to in Article 63(1) including, where	(1) Acțiunile sau inacțiunile Agenției pot fi contestate direct în instanța de judecată, conform Codului administrativ, fără respectarea procedurii prealabile.		Compatibil		

inclusiv, după caz, în legătură cu emiterea necorespunzătoare, omisiunea de a emite sau recunoașterea unui certificat european de securitate cibernetică deținut de respectivele persoane fizice și juridice; (b)omisiunea de a da curs unei plângeri depuse la o autoritate sau un organism menționat la articolul 63 alineatul (1).	applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons; (b) a failure to act on a complaint lodged with the authority or body referred to in Article 63(1).					
(2) Acțiunile în temeiul prezentului articol se introduc în fața instanțelor din statul membru în care este situată autoritatea sau organismul împotriva căruia se exercită calea de atac.	(2) Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.	(2) În cazul în care Agenția nu examinează o plângere sau nu informează autorul acesteia în termen de 3 luni cu privire la progresele ori la soluționarea plângerii depuse conform art. 29, persoana afectată poate contesta inacțiunile Agenției direct în instanța de judecată, conform Codului administrativ, fără respectarea procedurii prealabile.		Compatibil		
Articolul 65 **Sancțiuni**	**Article 65** **Penalties**	**Articolul 37. Sancțiunile** **Articolul 38. Încălcările pasibile de amendă**				
Statele membre stabilesc normele privind sancțiunile care se aplică în cazul încălcării prezentului titlu și a încălcării sistemelor europene de certificare a securității cibernetice 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 fără întârziere cu privire la normele și măsurile respective și notifică acesteia orice modificare ulterioară care le afectează.	Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall without delay notify the Commission of those rules and of those measures and shall notify it of any subsequent amendment affecting them.	Articolul 37. Sancțiunile (1) Pentru încălcările prevăzute la art. 38, Agenția aplică amenzi. Amenzile aplicate sunt, în fiecare caz, eficace, proporționale și disuasive și se varsă la bugetul de stat. (2) La aplicarea amenzii și la determinarea cuantumului acesteia se iau în considerare, în fiecare caz, următoarele circumstanțe: a) natura, gravitatea și durata încălcării, inclusiv nivelul de asigurare aplicabil și impactul potențial asupra utilizatorilor; b) caracterul intenționat al încălcării sau comiterea acesteia din neglijență;		Compatibil		

		c) acțiunile întreprinse pentru a reduce prejudiciul și pentru a remedia încălcarea; d) eventualele încălcări anterioare relevante; e) gradul de cooperare cu Agenția pentru remedierea încălcării și atenuarea posibilelor efecte negative; f) beneficiile financiare dobândite sau pierderile evitate ca urmare a încălcării, în măsura în care acestea pot fi stabilite; g) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului. (3) În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi aplicată ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul amenzii. (4) Sancțiunile se aplică în termen de un an de la data constatării încălcării, dar nu mai târziu de 3 ani de la data comiterii acesteia. (5) Aplicarea sancțiunii nu exonerează persoana sancționată de obligația de a înceta încălcarea și de a executa măsurile corective dispuse. Articolul 38. Încălcările pasibile de amendă (1) Se aplică amenzi de până la 100 000 de lei pentru: a) utilizarea unui certificat de securitate cibernetică suspendat, retras ori expirat sau referirea falsă la deținerea unui certificat ori a unei declarații de conformitate; b) utilizarea mărcilor sau a etichetelor de certificare cu încălcarea condițiilor stabilite de sistemul național de certificare;			

		(2) Se aplică amenzi de până la 200 000 de lei pentru: a) desfășurarea, în cadrul unui sistem național de certificare a securității cibernetice, a activităților de evaluare a conformității sau emiterea certificatelor de securitate cibernetică de către un organism neacreditat ori, după caz, neautorizat sau nerecunoscut în condițiile prezentei legi; b) falsificarea rezultatelor evaluării conformității sau emiterea certificatelor în baza unor informații despre care organismul emitent cunoștea că sunt false; c) împiedicarea desfășurării investigațiilor, a auditurilor sau a controalelor efectuate în condițiile art. 6; d) neexecutarea măsurilor corective dispuse în condițiile art. 36. (3) Amenzile se aplică prin decizie a Agenției, care poate fi contestată în condițiile art. 30.				
TITLUL IV DISPOZIȚII FINALE	**TITLE IV FINAL PROVISIONS**				Prevederile titlului IV se referă la procedura comitetului, evaluarea și revizuirea regulamentului, abrogare și succesiune, intrarea în vigoare și aplicarea regulamentului și, prin natura lor, nu necesită măsuri naționale de punere în aplicare.	
Articolul 66 Procedura comitetului	**Article 66 Committee procedure**					
(1) Comisia este asistată de un comitet. Comitetul respectiv reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.	(1) The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.			Prevederi UE neaplicabile		

(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.	(2) Where reference is made to this paragraph, point (b) of Article 5(4) of Regulation (EU) No 182/2011 shall apply.			Prevederi UE neaplicabile		
Articolul 67 **Evaluare și revizuire**	**Article 67** **Evaluation and review**					
(1) Până la 28 iunie 2024 și la fiecare cinci ani după aceea, Comisia evaluează impactul, eficacitatea și eficiența activității ENISA și a practicilor sale de lucru, posibila necesitate de a modifica mandatul ENISA și implicațiile financiare ale unei astfel de modificări. Evaluarea ține seama de orice punct de vedere comunicat ENISA ca răspuns la activitățile sale. În cazul în care Comisia consideră că nu se mai justifică continuarea activității ENISA în raport cu obiectivele, mandatul și atribuțiile încredințate acesteia, Comisia poate propune modificarea prezentului regulament în ceea ce privește dispozițiile referitoare la ENISA.	(1) By 28 June 2024, and every five years thereafter, the Commission shall evaluate the impact, effectiveness and efficiency of ENISA and of its working practices, the possible need to modify ENISA's mandate and the financial implications of any such modification. The evaluation shall take into account any feedback provided to ENISA in response to its activities. Where the Commission considers that the continued operation of ENISA is no longer justified in light of the objectives, mandate and tasks assigned to it, the Commission may propose that this Regulation be amended with regard to the provisions related to ENISA.			Prevederi UE neaplicabile		
(2) Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor din titlul III din prezentul regulament, inclusiv procedurile care conduc la adoptarea sistemelor europene de certificare a securității cibernetice și bazele lor de dovezi, în ceea ce privește obiectivele de asigurare a unui nivel adecvat de securitate cibernetică a produselor TIC, a serviciilor TIC, a proceselor TIC și a serviciilor de securitate gestionate în Uniune și de îmbunătățire a funcționării pieței interne.	(2) The evaluation shall also assess the impact, effectiveness and efficiency of the provisions of Title III of this Regulation, including the procedures leading to the adoption of European cybersecurity certification schemes and their evidence bases, with regard to the objectives of ensuring an adequate level of cybersecurity of ICT products, ICT services, ICT processes and managed security services in the Union and improving			Prevederi UE neaplicabile		

	the functioning of the internal market.					
(3) Evaluarea examinează dacă sunt necesare cerințe esențiale de securitate cibernetică pentru a avea acces la piața internă, cu scopul de a împiedica ca produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care nu respectă cerințele de bază în materie de securitate cibernetică să intre pe piața internă.	(3) The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the internal market.			Prevederi UE neaplicabile		
(4) Până la 28 iunie 2024, și ulterior din cinci în cinci ani Comisia trimite raportul de evaluare împreună cu concluziile sale, Parlamentului European, Consiliului și consiliului de administrație. Concluziile raportului respectiv sunt făcute publice.	(4) By 28 June 2024, and every five years thereafter, the Commission shall transmit a report on the evaluation together with its conclusions to the European Parliament, to the Council and to the Management Board. The findings of that report shall be made public.			Prevederi UE neaplicabile		
Articolul 68 **Abrogare și succesiune**	**Article 68** **Repeal and succession**					
(1) Regulamentul (UE) nr. 526/2013 se abrogă cu efect de la 27 iunie 2019.	(1) Regulation (EU) No 526/2013 is repealed with effect from 27 June 2019.			Prevederi UE neaplicabile		
(2) Trimiterile la Regulamentul (UE) nr. 526/2013 și la ENISA astfel cum este instituită prin regulamentul respectiv se interpretează ca trimiteri la prezentul regulament și la ENISA astfel cum e instituită prin prezentul regulament.	(2) References to Regulation (EU) No 526/2013 and to the ENISA as established by that Regulation shall be construed as references to this Regulation and to ENISA as established by this Regulation.			Prevederi UE neaplicabile		
(3) ENISA astfel cum e instituită de prezentul regulament succedă ENISA astfel cum este instituită prin Regulamentul (UE) nr. 526/2013 în ceea ce privește toate aspectele legate de proprietate, acorduri, obligații juridice, contracte de muncă, angajamente financiare și răspunderi. Toate deciziile consiliului de administrație și ale	(3) ENISA as established by this Regulation shall succeed ENISA as established by Regulation (EU) No 526/2013 as regards all ownership, agreements, legal obligations, employment contracts, financial commitments and liabilities. All decisions of the Management Board and the Executive Board adopted in			Prevederi UE neaplicabile		

comitetului executiv adoptate cu conformitate cu Regulamentul (UE) nr. 526/2013 rămân valabile, cu condiția ca acestea să respecte prezentul regulament.	accordance with Regulation (EU) No 526/2013 shall remain valid, provided that they comply with this Regulation.					
(4) ENISA se înființează pentru o perioadă nedeterminată de la 27 iunie 2019.	(4) ENISA shall be established for an indefinite period as of 27 June 2019.			Prevederi UE neaplicabile		
(5) Directorul executiv numit în temeiul articolului 24 alineatul (4) din Regulamentul (UE) nr. 526/2013 rămâne în funcție și exercită funcțiile directorului executiv astfel cum sunt menționate la articolul 20 din prezentul regulament pentru perioada rămasă din mandatul său. Celelalte condiții ale contractului său rămân neschimbate.	(5) The Executive Director appointed pursuant to Article 24(4) of Regulation (EU) No 526/2013 shall remain in office and exercise the duties of the Executive Director as referred to in Article 20 of this Regulation for the remaining part of the Executive Director's term of office. The other conditions of his or her contract shall remain unchanged.			Prevederi UE neaplicabile		
(6) Membrii consiliului de administrație și supleanții acestora numiți în temeiul articolului 6 din Regulamentul (UE) nr. 526/2013 rămâne în funcție și exercită funcțiile consiliului de administrație astfel cum sunt menționate la articolul 15 din prezentul regulament și supleanții acestora pentru perioada rămasă din mandatul lor.	(6) The members of the Management Board and their alternates appointed pursuant to Article 6 of Regulation (EU) No 526/2013 shall remain in office and exercise the functions of the Management Board as referred to in Article 15 of this Regulation for the remaining part of their term of office.			Prevederi UE neaplicabile		
Articolul 69 **Intrare în vigoare**	**Article 69** **Entry into force**					
(1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene.	(1) This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.			Prevederi UE neaplicabile		
(2) Articolele 58, 60, 61, 63, 64 și 65 se aplică de la 28 iunie 2021.	(2) Articles 58, 60, 61, 63, 64 and 65 shall apply from 28 June 2021. This Regulation shall be binding in its entirety and			Prevederi UE neaplicabile		

	directly applicable in all Member States.					
ANEXĂ	**ANNEX**					
CERINȚE CARE TREBUIE ÎNDEPLINITE DE ORGANISMELE DE EVALUARE A CONFORMITĂȚII	**REQUIREMENTS TO BE MET BY CONFORMITY ASSESSMENT BODIES**	**Articolul 22. Cerințe care trebuie îndeplinite de organismele de evaluare a conformității**				
Organismele de evaluare a conformității care doresc să fie acreditate îndeplinesc următoarele cerințe: 1. Un organism de evaluare a conformității trebuie să fie înființat în temeiul dreptului intern și să aibă personalitate juridică. 2. Un organism de evaluare a conformității trebuie să fie un organism terț care este independent de organizația sau de produsele TIC, de serviciile TIC, de procesele TIC sau de serviciile de securitate gestionate pe care le evaluează. 3. Un organism care aparține unei asociații de întreprinderi sau unei federații profesionale care reprezintă întreprinderile implicate în conceperea, producerea, furnizarea, asamblarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate 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. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi	Conformity assessment bodies that wish to be accredited shall meet the following requirements: 1. A conformity assessment body shall be established under national law and shall have legal personality. 2. A conformity assessment body shall be a third-party body that is independent of the organisation or the ICT products, ICT services, ICT processes or managed security services that it assesses. 3. A body that belongs to a business association or professional federation representing undertakings involved in the design, manufacturing, provision, assembly, use or maintenance of ICT products, ICT services, ICT processes or managed security services which it assesses may be considered to be a conformity assessment body, provided that its independence and the absence of any conflict of interest are demonstrated. 4. The conformity assessment bodies, their top level management and the persons responsible for carrying out the conformity assessment tasks shall not be the designer, manufacturer, supplier, installer, purchaser, owner, user or maintainer of the ICT	Organismele de evaluare a conformității care doresc să fie acreditate îndeplinesc 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 care este independent de organizația sau de produsele TIC, de serviciile TIC, de procesele TIC sau de serviciile de securitate gestionate pe care le evaluează. 3) Un organism care aparține unei asociații de întreprinderi sau unei federații profesionale care reprezintă întreprinderile implicate în conceperea, producerea, furnizarea, asamblarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate 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) Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi		Compatibil	Pct. 15: obligația de a încheia asigurare de răspundere civilă se aplică tuturor organismelor de evaluare a conformității; ipotezele în care răspunderea este asumată de statul membru sau statul membru este direct responsabil de evaluarea conformității nu au fost preluate.	

proiectantul, producătorul, furnizorul, instalatorul, cumpărătorul, proprietarul, utilizatorul sau operatorul de întreținere al produsului TIC, al serviciului TIC, al procesului TIC sau al serviciului de securitate gestionat care este evaluat ori reprezentantul autorizat al vreuneia dintre aceste părți. Această interdicție nu împiedică utilizarea produselor TIC evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea acestor produse TIC în scopuri personale. 5. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi direct implicate în conceperea, producerea sau construcția, furnizarea, comercializarea, instalarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care sunt evaluate și nu pot reprezenta părțile angajate în acele activități. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu se implică în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității. Această interdicție se aplică în	product, ICT service, ICT process or managed security service which is assessed, or the authorised representative of any of those parties. That prohibition shall not preclude the use of the ICT products assessed that are necessary for the operations of the conformity assessment body or the use of such ICT products for personal purposes. 5. The conformity assessment bodies, their top level management and the persons responsible for carrying out the conformity assessment tasks shall not be directly involved in the design, manufacture or construction, the provision, the marketing, installation, use or maintenance of the ICT products, ICT services, ICT processes or managed security services which are assessed, or represent parties engaged in those activities. The conformity assessment bodies, their top level management and the persons responsible for carrying out the conformity assessment tasks shall not engage in any activity that may conflict with their independence of judgement or integrity in relation to their conformity assessment activities. That prohibition shall apply, in particular, to consultancy services. 6. If a conformity assessment body is owned or operated by a public entity or institution, the independence and absence of any conflict of interest shall be ensured between the	proiectantul, producătorul, furnizorul, instalatorul, cumpărătorul, proprietarul, utilizatorul sau operatorul de întreținere al produsului TIC, al serviciului TIC, al procesului TIC sau al serviciului de securitate gestionat care este evaluat ori reprezentantul autorizat al vreuneia dintre aceste părți. Această interdicție nu împiedică utilizarea produselor TIC evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea acestor produse TIC în scopuri personale. 5) Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu pot fi direct implicate în conceperea, producerea sau construcția, furnizarea, comercializarea, instalarea, utilizarea sau întreținerea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate care sunt evaluate și nu pot reprezenta părțile angajate în acele activități. Organismele de evaluare a conformității, personalul de conducere de nivel superior al acestora și persoanele responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu se implică în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității. Această interdicție se aplică în special serviciilor de consultanță. 6) Dacă un organism de evaluare a conformității este				

special serviciilor de consultanță. 6. Dacă un organism de evaluare a conformității este deținut sau gestionat de o entitate sau de o instituție publică, se asigură și se documentează independența și absența oricărui conflict de interese între autoritatea națională de certificare a securității cibernetice, pe de o parte, și organismul de evaluare a conformității, pe de altă parte. 7. Organismele de evaluare a conformității se asigură că activitățile filialelor și ale subcontractanților lor nu afectează confidențialitatea, obiectivitatea sau imparțialitatea activităților lor de evaluare a conformității. 8. Organismele de evaluare a conformității și personalul acestora îndeplinesc activitățile de evaluare a conformității cu cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și nu sunt supuse 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. 9. Un organism de evaluare a conformității trebuie să fie capabil să efectueze toate atribuțiile de evaluare a conformității care îi sunt atribuite în temeiul prezentului regulament, indiferent dacă atribuțiile respective sunt realizate în mod direct de	national cybersecurity certification authority and the conformity assessment body, and shall be documented. 7. Conformity assessment bodies shall ensure that the activities of their subsidiaries and subcontractors do not affect the confidentiality, objectivity or impartiality of their conformity assessment activities. 8. Conformity assessment bodies and their staff shall carry out conformity assessment activities with the highest degree of professional integrity and the requisite technical competence in the specific field, and shall be free from all pressures and inducements which might influence their judgement or the results of their conformity assessment activities, including pressures and inducements of a financial nature, especially as regards persons or groups of persons with an interest in the results of those activities. 9. A conformity assessment body shall be capable of carrying out all the conformity assessment tasks assigned to it under this Regulation, regardless of whether those tasks are carried out by the conformity assessment body itself or on its behalf and under its responsibility. Any subcontracting to, or consultation of, external staff shall be properly documented, shall not involve any intermediaries and shall be subject to a written agreement covering, among other things,	deținut sau gestionat de o autoritate sau de o instituție publică, se asigură și se documentează independența și absența oricărui conflict de interese între Agenție, pe de o parte, și organismul de evaluare a conformității, pe de altă parte. 7) Organismele de evaluare a conformității se asigură că activitățile filialelor și ale subcontractanților lor nu afectează confidențialitatea, obiectivitatea sau imparțialitatea activităților lor de evaluare a conformității. 8) Organismele de evaluare a conformității și personalul acestora îndeplinesc activitățile de evaluare a conformității cu cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și nu sunt supuse 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. 9) Un organism de evaluare a conformității trebuie să fie capabil să efectueze toate atribuțiile de evaluare a conformității care îi sunt atribuite în temeiul prezentei legi, indiferent dacă atribuțiile respective sunt realizate în mod direct de organismul de evaluare a conformității sau în numele său și pe răspunderea sa. Orice subcontractare sau consultare a personalului extern este documentată în mod adecvat, nu				

organismul de evaluare a conformității sau în numele său și pe răspunderea sa. Orice subcontractare sau consultare a personalului extern este documentată în mod adecvat, nu implică intermediari și face obiectul unui acord scris care vizează, între altele, confidențialitatea și conflictele de interese. Organismul de evaluare a conformității în cauză își asumă întreaga răspundere pentru atribuțiile îndeplinite. 10. În orice moment și pentru fiecare procedură de evaluare a conformității și fiecare tip, categorie sau subcategorie de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, organismul de evaluare a conformității dispune de: (a) personalul necesar având cunoștințele tehnice necesare și experiența suficientă și corespunzătoare pentru a efectua atribuțiile 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 prevede politicile și procedurile adecvate care fac distincție între atribuțiile îndeplinite ca organism notificat în temeiul articolului 61 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	confidentiality and conflicts of interest. The conformity assessment body in question shall take full responsibility for the tasks performed. 10. At all times and for each conformity assessment procedure and each type, category or sub-category of ICT products, ICT services, ICT processes or managed security services, a conformity assessment body shall have at its disposal the necessary: (a) staff with technical knowledge and sufficient and appropriate experience to perform the conformity assessment tasks; (b) descriptions of procedures in accordance with which conformity assessment is to be carried out, to ensure the transparency of those procedures and the possibility of reproducing them. It shall have in place appropriate policies and procedures that distinguish between tasks that it carries out as a body notified pursuant to Article 61 and its other activities; (c) procedures for the performance of activities which take due account of the size of an undertaking, the sector in which it operates, its structure, the degree of complexity of the technology of the ICT product, ICT service, ICT process or managed security service in question and the mass or serial nature of the production process. 11. A conformity assessment body shall have the means necessary to perform the	implică intermediari și face obiectul unui acord scris care vizează, între altele, confidențialitatea și conflictele de interese. Organismul de evaluare a conformității în cauză își asumă întreaga răspundere pentru atribuțiile îndeplinite. 10) În orice moment și pentru fiecare procedură de evaluare a conformității și fiecare tip, categorie sau subcategorie de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate, organismul de evaluare a conformității dispune de: a) personalul necesar având cunoștințele tehnice necesare și experiența suficientă și corespunzătoare pentru a efectua atribuțiile 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. 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 TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat în cauză, precum și de caracterul de serie sau de masă al procesului de producție. 11) Un organism de evaluare a conformității dispune de mijloacele necesare pentru a îndeplini în mod corespunzător atribuțiile tehnice și				

complexitate a tehnologiei produsului TIC, serviciului TIC, procesului TIC sau serviciului de securitate gestionat în cauză, precum și de caracterul de serie sau de masă al procesului de producție. 11. Un organism de evaluare a conformității dispune de mijloacele necesare pentru a îndeplini în mod corespunzător atribuțiile tehnice și administrative legate de activitățile de evaluare a conformității și să aibă acces la toate echipamentele sau facilitățile necesare. 12. Personalul responsabil cu îndeplinirea activităților de evaluare a conformității posedă următoarele calități: (a) o bună pregătire tehnică și profesională care acoperă toate activitățile de evaluare a conformității; (b) cunoștințe satisfăcătoare ale cerințelor evaluărilor conformității 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 conformității au fost realizate. 13. Se garantează imparțialitatea organismelor de evaluare a conformității, a personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității, precum și a subcontractanților.	technical and administrative tasks connected with the conformity assessment activities in an appropriate manner, and shall have access to all necessary equipment and facilities. 12. The persons responsible for carrying out conformity assessment activities shall have the following: (d) sound technical and vocational training covering all conformity assessment activities; (e) satisfactory knowledge of the requirements of the conformity assessments they carry out and adequate authority to carry out those assessments; (f) appropriate knowledge and understanding of the applicable requirements and testing standards; (g) the ability to draw up certificates, records and reports demonstrating that conformity assessments have been carried out. 13. The impartiality of the conformity assessment bodies, of their top-level management, of the persons responsible for carrying out conformity assessment activities, and of any subcontractors shall be guaranteed. 14. The remuneration of the top-level management and of the persons responsible for carrying out conformity assessment activities shall not depend on the number of conformity assessments carried out or on the results of those assessments.	administrative legate de activitățile de evaluare a conformității și să aibă acces la toate echipamentele sau facilitățile necesare. 12) Personalul responsabil cu îndeplinirea activităților de evaluare a conformității posedă următoarele calități: a) o bună pregătire tehnică și profesională care acoperă toate activitățile de evaluare a conformității; b) cunoștințe satisfăcătoare ale cerințelor evaluărilor conformității 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 conformității au fost realizate. 13) Se garantează imparțialitatea organismelor de evaluare a conformității, a personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității, precum și a subcontractanților. 14) Remunerația personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu depinde de numărul de evaluări ale conformității realizate sau de rezultatele evaluărilor respective.				

14. Remunerația personalului de conducere de nivel superior și a persoanelor responsabile cu îndeplinirea atribuțiilor de evaluare a conformității nu depinde de numărul de evaluări ale conformității realizate sau de rezultatele evaluărilor respective. 15. Organismele de evaluare a conformității încheie o asigurare de răspundere civilă în cazul în care răspunderea nu este asumată de statul membru în conformitate cu dreptul intern sau statul membru nu este direct responsabil de evaluarea conformității. 16. Organismul de evaluare a conformității și personalul său, comitetele, filialele, subcontractanții și orice organism asociat sau personalul organismelor externe ale unui organism de evaluare a conformității păstrează confidențialitatea și secretul profesional în legătură cu toate informațiile obținute în îndeplinirea atribuțiilor de evaluare a conformității care le revin în temeiul prezentului regulament sau al oricărei dispoziții de drept intern care pune în aplicare prezentul regulament, cu excepția cazului în care divulgarea este cerută prin dreptul Uniunii sau al statului membru care se aplică respectivelor persoane și cu excepția relației cu autoritățile competente ale statului membru în care își îndeplinesc activitățile. Drepturile de autor sunt protejate. Organismul de evaluare a conformității dispune de proceduri documentate în	15. Conformity assessment bodies shall take out liability insurance unless liability is assumed by the Member State in accordance with its national law, or the Member State itself is directly responsible for the conformity assessment. 16. The conformity assessment body and its staff, its committees, its subsidiaries, its subcontractors, and any associated body or the staff of external bodies of a conformity assessment body shall maintain confidentiality and observe professional secrecy with regard to all information obtained in carrying out their conformity assessment tasks under this Regulation or pursuant to any provision of national law giving effect to this Regulation, except where disclosure is required by Union or Member State law to which such persons are subject, and except in relation to the competent authorities of the Member States in which its activities are carried out. Intellectual property rights shall be protected. The conformity assessment body shall have documented procedures in place in respect of the requirements of this point. 17. With the exception of point 16, the requirements of this Annex shall not preclude exchanges of technical information and regulatory guidance between a conformity assessment body and a person who applies for	15) Organismele de evaluare a conformității încheie o asigurare de răspundere civilă. 16) Organismul de evaluare a conformității și personalul său, comitetele, filialele, subcontractanții și orice organism asociat sau personalul organismelor externe ale unui organism de evaluare a conformității păstrează confidențialitatea și secretul profesional în legătură cu toate informațiile obținute în îndeplinirea atribuțiilor de evaluare a conformității care le revin în temeiul prezentei legi, cu excepția cazului în care divulgarea este cerută de legislație și cu excepția relației cu autoritățile competente. Drepturile de proprietate intelectuală sunt protejate. Organismul de evaluare a conformității dispune de proceduri documentate în ceea ce privește cerințele prezentului punct. 17) Cu excepția pct. 16, cerințele din prezentul articol nu împiedică în schimburile de informații tehnice și de orientări în materie de reglementare între un organism de evaluare a conformității și o persoană care solicită certificarea, sau care intenționează să solicite certificarea. 18) Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termeni și condiții coerente, echitabile și rezonabile, ținând seama de interesele IMM-urilor, în ceea ce privește taxele. 19) Organismele de evaluare a conformității				

ceea ce privește cerințele din prezentul punct. 17. Cu excepția punctului 16, cerințele din prezenta anexă nu împiedică în schimburile de informații tehnice și de orientări în materie de reglementare între un organism de evaluare a conformității și o persoană care solicită certificarea, sau care intenționează să solicite certificarea. 18. Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termeni și condiții coerente, echitabile și rezonabile, ținând seama de interesele IMM-urilor, în ceea ce privește taxele. 19. Organismele de evaluare a conformității îndeplinesc cerințele standardului armonizat relevant în sensul definiției de la articolul 2 punctul 9 din Regulamentul (CE) nr. 765/2008 pentru acreditarea organismelor de evaluare a conformității care efectuează certificarea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate. 20. Organismele de evaluare a conformității se asigură că laboratoarele de testare utilizate în scopul evaluării conformității respectă cerințele standardului armonizat relevant în sensul definiției de la articolul 2 punctul 9 din Regulamentul (CE) nr. 765/2008 pentru acreditarea laboratoarelor care efectuează testări.	certification or who is considering whether to apply for certification. 18. Conformity assessment bodies shall operate in accordance with a set of consistent, fair and reasonable terms and conditions, taking into account the interests of SMEs in relation to fees. 19. Conformity assessment bodies shall meet the requirements of the relevant harmonised standard as defined in Article 2, point (9), of Regulation (EC) No 765/2008 for the accreditation of conformity assessment bodies performing the certification of ICT products, ICT services, ICT processes or managed security services. 20. Conformity assessment bodies shall ensure that testing laboratories used for conformity assessment purposes meet the requirements of the relevant harmonised standard as defined in Article 2, point (9), of Regulation (EC) No 765/2008 for the accreditation of laboratories that perform testing.	îndeplinesc cerințele standardului relevant, armonizat la nivel național, pentru acreditarea organismelor de evaluare a conformității care efectuează certificarea produselor TIC, serviciilor TIC, proceselor TIC sau serviciilor de securitate gestionate. 20) Organismele de evaluare a conformității se asigură că laboratoarele de testare utilizate în scopul evaluării conformității respectă cerințele standardului relevant, armonizat la nivel național, pentru acreditarea laboratoarelor care efectuează testări.				

MINISTERUL DEZVOLTĂRII ECONOMICE ȘI DIGITALIZĂRII AL REPUBLICII MOLDOVA

CENTRUL NAȚIONAL DE ACREDITARE DIN REPUBLICA MOLDOVA (MOLDAC)

MINISTRY OF ECONOMIC DEVELOPMENT AND DIGITALIZATION OF THE REPUBLIC OF MOLDOVA

NATIONAL ACCREDITATION CENTRE OF THE REPUBLIC OF MOLDOVA (MOLDAC)

MD-2028, mun. Chișinău, st. Gh. Tudor 5, of.302
tel/fax. +373-22-210-316, **e-mail:** acreditare@moldac.gov.md
web : www.acreditare.md

MD-2028, mun. Chișinău, st. Gh. Tudor 5, of.302
tel/fax. +373-22-210-316, **e-mail:** acreditare@moldac.gov.md
web : www.acreditare.md

Nr. 24/400 DE-2 din 29.07.2026

Ministerul Dezvoltării Economice și Digitalizării

Prin prezenta, Centrul Național de Acreditare din Republica Moldova (MOLDAC), Vă informează, că a analizat proiectul de lege cu privire la aprobarea sistemului național de certificare a securității cibernetice nr. 14-2488 din 21.07.2026 (nr. intrare MOLDAC 455 din 22.07.2026).

În limitele competențelor funcționale, MOLDAC propune următoarele modificări pe textul proiectului de lege:

1. Art. 3 *Noțiuni*: se propune redactarea noțiunii *autoevaluare a conformității* în conformitate cu prevederile art.18 a prezentului proiect de lege;
2. Art.7, alin.(1): se propune excluderea sintagmei ”reprezentanți ai organismului național de acreditare”;
3. Art.8, alin.(2): reformulare aliniat în următoarea redacție:
   ” În cazul în care constată că un organism de evaluare a conformității nu mai îndeplinește condițiile prevăzute de prezenta lege sau de sistemul națională de certificare, Agenția poate solicita organismului național de acreditare reevaluarea, restrângerea, suspendarea sau retragerea acreditării organismului în cauză”.
4. Art.15, alin. (2) : reformulare aliniat în următoarea redacție:
   Certificarea securității cibernetice este voluntară, cu excepția cazurilor în care legislația Republicii Moldova prevede altfel.

De asemenea, propunem armonizarea textului cu cerințele Legii nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, în special cu prevederile din Cap. V *Organismele de evaluare a conformității*, Art.20. *Acreditarea organismelor de evaluare a conformității* referitoare la:

- caracterul acreditării ca atestare a competenței:

Alin. (1) Organismele de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare a securității cibernetice se acreditează de către organismul național de acreditare, în conformitate cu prevederile Legii nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității și cu cerințele aplicabile domeniului

securității cibernetice. Acreditarea se acordă numai organismelor de evaluare a conformității care demonstrează îndeplinirea cerințelor prevăzute de Legea nr. 235/2011, de standardele de acreditare aplicabile și de cerințele specifice domeniului securității cibernetice.

- acordarea și menținerea acreditării prin supraveghere periodică:

Alin. (2) Acreditarea se acordă pentru o perioadă de 4 ani, cu efectuarea supravegherii periodice pe durata ciclului de acreditare, şi poate fi reînnoită în condiţiile prevăzute de Legea nr. 235/2011, dacă organismul de evaluare a conformității continuă să îndeplinească cerințele de acreditare.

- posibilitatea extinderii, restrângerii, suspendării și retragerii acreditării:

Alin. (3) și (4) Măsurile aplicabile acreditării trebuie formulate în conformitate cu terminologia utilizată de Legea nr. 235/2011: extindere, restrângere, suspendare și retragere.
Notă: aceiaşi abordare trebuie
Condițiile de acordare și menținere a acreditării trebuie raportate la Legea nr. 235/2011 și la standardele de acreditare aplicabile, și nu exclusiv la anexa Legii privind certificarea securității cibernetice.

Se întâlnesc situații contradictorii, de exemplu:

- art.15 alin. (2) Certificarea securității cibernetice este voluntară, cu excepția cazului în care prin lege se prevede altfel, și
- art.38(2a) Se aplică amenzi de până la 200 000 de lei pentru (a) desfășurarea activităților de evaluare a conformității sau emiterea certificatelor de securitate cibernetică de către un organism neacreditat ori, după caz, neautorizat sau nerecunoscut în condițiile prezentei legi.

MOLDAC este deschis pentru colaborare, pentru atingerea obiectivelor comune.

Director **Iurie FRIPTULEAC**

Ex: Natalia Mihăescu
022 210 312

MINISTERUL FINANŢELOR
AL REPUBLICII MOLDOVA

data aplicării semnăturii electronice *nr.* *09/2-09/697*

la nr.14-3044 din 03.09.2026

Referitor la examinarea proiectului de lege privind certificarea securității cibernetice

Ministerul Dezvoltării Economice și Digitalizării
e-mail: secretariat@mded.gov.md

La demersul Ministerului Dezvoltării Economice și Digitalizării nr. 14-3044 din 03.09.2026, Ministerul Finanțelor a examinat proiectul de lege *privind certificarea securității cibernetice* și, în limita atribuțiilor funcționale, comunică următoarele obiecții și propuneri.

La proiectul legii

La art. 4 alin. (4) și (5) se propune excluderea acestora, întrucât nu se consideră necesară reglementarea, prin lege, a modului de finanțare a subdiviziunii respective, precum și accentuarea în cuprinsul legii a autorității competente pentru aprobarea regulamentului acesteia.

Agenția pentru Securitate Cibernetică, care urmează a fi desemnată în calitate de autoritate națională de certificare a securității cibernetice, este o autoritate administrativă din subordinea Ministerului Dezvoltării Economice și Digitalizării, cu statut de persoană juridică de drept public. Conform prevederilor *Legii privind administrația publică centrală de specialitate nr. 98/2012*, finanțarea și asigurarea tehnico-materială a activității ministerelor și a altor autorități administrative centrale se efectuează din contul mijloacelor prevăzute în legea bugetului de stat și din contul mijloacelor provenite din alte surse, conform legislației.

La art. 7, după alin. (2), se propune completarea cu un nou alineat cu următorul cuprins:
„(3) Activitatea membrilor Consiliului consultativ nu este remunerată.”

La art. 22 pct. 18), prevederea referitoare la stabilirea taxelor urmează a fi revizuită și clarificată, inclusiv din perspectiva impactului acestora asupra întreprinderilor mici și mijlocii.

Art. 38 se propune a fi exclus, iar prevederile privind sancțiunile contravenționale aplicate pentru încălcarea prevederilor proiectului urmează a fi incluse în *Codul contravențional al Republicii Moldova*, în vederea asigurării unei reglementări unitare a sancțiunilor contravenționale într-un singur act normativ și evitării dispersării acestora în legi distincte.

Totodată, în vederea respectării principiului proporționalității în aplicarea sancțiunilor, se consideră necesară stabilirea unor limite concrete ale cuantumului amenzii pentru fiecare încălcare, în funcție de natura și gravitatea acesteia, precum și de circumstanțele constatate.

Totodată, proiectul implică majorarea efectivului-limită de personal al Agenției pentru Securitate Cibernetică cu 4 unități, ceea ce ar genera un impact financiar de 1 242,8 mii lei anual. Respectiv, o asemenea extindere a efectivului-limită implică cheltuieli suplimentare, atât cu caracter unic, cât și recurente, care urmează a fi evaluate distinct și argumentate corespunzător, cu respectarea

principiilor, regulilor și responsabilităților statuate de *Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014*.

Suplimentar, se menționează că, potrivit raportului operativ lunar FD-050 privind statele și efectivul de personal din autoritățile/instituțiile bugetare, la situația din 31.08.2026, aparatul central al Ministerului Dezvoltării Economice și Digitalizării înregistra 75 de funcții vacante din 257 de unități de personal precizate, rata de încadrare constituind 70,8% din efectivul prevăzut. În cadrul Agenției pentru Securitate Cibernetică, numărul funcțiilor vacante constituia 13 unități, iar numărul funcțiilor efectiv ocupate – 31 de unități, rata de încadrare constituind 70,5%.

Aceiași indicatori, în medie, au fost raportați de Agenție pe parcursul anului 2026, respectiv 14/13 funcții vacante și 30/31 funcții ocupate. În acest sens, se conturează necesitatea identificării unor soluții optime pentru acoperirea necesarului de personal, inclusiv din contul funcțiilor vacante existente, precum și examinarea posibilității anulării, la solicitare, a moratoriului.

Optimizarea efectivului-limită, prin prisma funcțiilor exercitate și a necesităților reale de personal, reprezintă o condiție prioritară în contextul neadmiterii majorării ponderii cheltuielilor de personal în PIB, în raport cu indicatorul-țintă prestabilit.

La Nota de fundamentare

Nota de fundamentare nu reflectă impactul financiar integral aferent implementării proiectului. În aceasta sunt prezentate doar cheltuielile de personal aferente subdiviziunii, fără a fi prezentate argumentele privind necesitatea instituirii acesteia și stabilirii efectivului-limită de 4 unități.

Concomitent, nu este clarificat impactul posibil asupra bugetului de stat, având în vedere că organul național de acreditare MOLDAC va fi responsabil de acreditarea organismelor de evaluare a conformității în cadrul sistemelor naționale de certificare a securității cibernetice. În acest context, urmează a fi reflectate atât eventualele venituri rezultate din perceperea plăților pentru acreditare, cât și cheltuielile suplimentare aferente activității de acreditare a acestor organisme de către MOLDAC.

Subsidiar, proiectul prevede instituirea și ținerea, de către Agenția pentru Securitate Cibernetică, a Registrului certificatelor de securitate cibernetică și al declarațiilor de conformitate. Totodată, nu este clarificat dacă instituirea și administrarea registrului respectiv implică necesitatea alocării unor resurse financiare de la bugetul de stat. În cazul în care sunt necesare asemenea resurse, acestea urmează a fi estimate și argumentate în Nota de fundamentare.

În final, se menționează că estimarea și argumentarea costurilor aferente proiectului cu relevanță pentru procesul de integrare europeană urmează să fie efectuate în strictă conformitate cu prevederile *Hotărârii Guvernului cu privire la aprobarea Metodologiei de analiză a impactului de reglementare nr. 574/2024*.

Respectiv, proiectul urmează a fi îmbunătățit prin prisma celor menționate supra.

Secretar de stat **Ion GUMENE**

✍ Eugeniu Verlan
☎ *(022) 262-681 e-mail: eugeniu.verlan@mf.gov.md*

SINTEZA
proiectului de lege privind certificarea securității cibernetice
(denumirea proiectului actului normativ)

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Coordonare prealabilă			
Centrul Național de Acreditare din Republica Moldova (MOLDAC) (Nr. 24/400 DE-2 din 29.07.2026)	1.	Art. 3 Noțiuni: se propune redactarea noțiunii autoevaluare a conformității în conformitate cu prevederile art.18 a prezentului proiect de lege;	**Precizare.** Noțiunea „autoevaluare a conformității” expusă la art. 3 din proiect este în corespundere cu prevederile art. 18 din proiect. Totodată, este de menționat că atât definiția noțiunii, cât și prevederile art. 18 reprezintă o transpunere fidelă a art. 2 pct. 22 și a art. 53 din Regulamentul (UE) 2019/881.
	2.	Art.7, alin.(1): se propune excluderea sintagmei ”reprezentanți ai organismului național de acreditare”;	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	3.	Art.8, alin.(2): reformulare aliniat în următoarea redacție: ” În cazul în care constată că un organism de evaluare a conformității nu mai îndeplinește condițiile prevăzute de prezenta lege sau de sistemul națională de certificare, Agenția poate solicita organismului național de acreditare reevaluarea, restrângerea, suspendarea sau retragerea acreditării organismului în cauză”.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	4.	Art.15, alin. (2): reformulare aliniat în următoarea redacție: Certificarea securității cibernetice este voluntară, cu excepția cazurilor în care legislația Republicii Moldova prevede altfel.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	5.	De asemenea, propunem armonizarea textului cu cerințele Legii nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, în special cu prevederile din Cap. V Organismele de evaluare a conformității, Art.20. Acreditarea organismelor de evaluare a conformității referitoare la: -caracterul acreditării ca atestare a competenței: Alin. (1) Organismele de evaluare a conformității care desfășoară activități de evaluare în cadrul sistemelor naționale de certificare	**Se acceptă.** Proiectul a fost modificat conform propunerii.

		a securității cibernetice se acreditează de către organismul național de acreditare, în conformitate cu prevederile Legii nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității și cu cerințele aplicabile domeniului securității cibernetice. Acreditarea se acordă numai organismelor de evaluare a conformității care demonstrează îndeplinirea cerințelor prevăzute de Legea nr. 235/2011, de standardele de acreditare aplicabile și de cerințele specifice domeniului securității cibernetice. -acordarea și menținerea acreditării prin supraveghere periodică: Alin. (2) Acreditarea se acordă pentru o perioadă de 4 ani, cu efectuarea supravegherii periodice pe durata ciclului de acreditare, și poate fi reînnoită în condițiile prevăzute de Legea nr. 235/2011, dacă organismul de evaluare a conformității continuă să îndeplinească cerințele de acreditare. -posibilitatea extinderii, restrângerii, suspendării și retragerii acreditării: Alin. (3) și (4) Măsurile aplicabile acreditării trebuie formulate în conformitate cu terminologia utilizată de Legea nr. 235/2011: extindere, restrângere, suspendare și retragere. Notă: aceiași abordare trebuie Condițiile de acordare și menținere a acreditării trebuie raportate la Legea nr. 235/2011 și la standardele de acreditare aplicabile, și nu exclusiv la anexa Legii privind certificarea securității cibernetice.	**Se acceptă.** Proiectul a fost modificat conform propunerii. **Se acceptă.** Proiectul a fost modificat conform propunerii.
	6.	Se întâlnesc situații contradictorii, de exemplu: -art.15 alin. (2) Certificarea securității cibernetice este voluntară, cu excepția cazului în care prin lege se prevede altfel, și -art.38(2a) Se aplică amenzi de până la 200 000 de lei pentru (a) desfășurarea activităților de evaluare a conformității sau emiterea certificatelor de securitate cibernetică de către un organism neacreditat ori, după caz, neautorizat sau nerecunoscut în condițiile prezentei legi.	**Se acceptă.** Proiectul a fost modificat conform propunerii.

Agenția pentru Securitate Cibernetică (e-mail)	7.	Cu referire la proiectul de lege privind certificarea securității cibernetice, Agenția pentru Securitate Cibernetică comunică că transpunerea proiectului vine cu noi completări prin care vizează extinderea domeniului de reglementare a competențelor de certificare. În această ordine de idei, la tipurile de certificare a securității cibernetice care sunt reglementate prin Regulamentul UE, 12. „produs TIC” înseamnă un element sau un grup de elemente al unei rețele sau al unui sistem informatic; 13. „serviciu TIC” înseamnă un serviciu care constă integral sau preponderent în transmiterea, stocarea, extragerea sau prelucrarea informației prin intermediul rețelelor și al sistemelor informatice; 14. „proces TIC” înseamnă un set de activități desfășurate pentru a concepe, a dezvolta, a furniza sau a întreține un produs TIC sau un serviciu TIC; Se adaugă certificarea serviciilor de securitate gestionate serviciu de securitate gestionat - serviciu furnizat unei părți terțe care constă în desfășurarea sau furnizarea de asistență pentru activități legate de gestionarea riscurilor în materie de securitate cibernetică, cum ar fi gestionarea incidentelor cibernetice, testele de rezistență la intruziuni, auditurile de securitate și consultanța, inclusiv consultanța de specialitate, în legătură cu asistența tehnică; astfel, reglementarea proiectului la nivelul Republicii Moldova, depășește Regulamentul UE și nu este conform prin faptul că la tipurile de certificări UE se adaugă printr-o definiție noțiunea de serviciu de securitate gestionat care nu se încadrează armonios în proiectul de bază. Totodată, nivelurile de asigurare, de bază, substanțial și ridicat, presupun că Agenția are obligația de a urma anumite proceduri care nu pot fi aplicate pentru certificarea serviciilor de securitate gestionate.	**Precizare.** Prin Regulamentul (UE) 2025/37 al Parlamentului European și al Consiliului din 19 decembrie 2024 de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate, au fost incluse reglementări cu privire la certificarea serviciilor de securitate gestionate.

	8.	Regulamentul UE reglementează că fiecare certificare trebuie să cuprindă condițiile de recunoaștere reciprocă a certificatelor cu statele terțe. În această ordine de idei, la nivelul UE, statele membre nu reglementează procedura de certificare a serviciilor gestionate de securitate, iar Agenția va fi în imposibilitate să recunoască reciproc de exemplu un certificat de auditor emis într-un stat european dacă va reglementa certificarea auditorilor prin prezentul proiect, lucru care poate duce la conflicte de concurență neloială între Republica Moldova și statele membre UE.	**Precizare.** Proiectul de lege reglementează certificarea serviciilor de securitate gestionate, iar nu, în mod expres, certificarea individuală a auditorilor. Totuși, având în vedere că serviciile de securitate gestionate includ și auditurile de securitate, iar sistemele naționale de certificare pot stabili cerințe privind competența, expertiza și experiența personalului care prestează asemenea servicii, este necesar să se evite instituirea, prin sistemele naționale de certificare, a unor cerințe care ar echivala în fapt cu o certificare națională obligatorie a auditorilor sau a altor specialiști certificați în statele membre ale Uniunii Europene. În acest sens, proiectul prevade r că certificările sau acreditările relevante obținute în statele membre ale Uniunii Europene sunt recunoscute în condițiile cadrului european aplicabil, astfel încât cerințele naționale privind certificarea serviciilor de securitate gestionate să nu creeze bariere nejustificate pentru prestarea transfrontalieră a serviciilor și să nu genereze condiții concurențiale mai restrictive pentru operatorii din Uniunea Europeană decât cele aplicabile operatorilor naționali.

Ministerul Finanțelor (Nr. 09/2-09/697 din 21.09.2026)	9.	La art. 4 alin. (4) și (5) se propune excluderea acestora, întrucât nu se consideră necesară reglementarea, prin lege, a modului de finanțare a subdiviziunii respective, precum și accentuarea în cuprinsul legii a autorității competente pentru aprobarea regulamentului acesteia. Agenția pentru Securitate Cibernetică, care urmează a fi desemnată în calitate de autoritate națională de certificare a securității cibernetice, este o autoritate administrativă din subordinea Ministerului Dezvoltării Economice și Digitalizării, cu statut de persoană juridică de drept public. Conform prevederilor Legii privind administrația publică centrală de specialitate nr. 98/2012, finanțarea și asigurarea tehnico-materială a activității ministerelor și a altor autorități administrative centrale se efectuează din contul mijloacelor prevăzute în legea bugetului de stat și din contul mijloacelor provenite din alte surse, conform legislației.	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	10.	La art. 7, după alin. (2), se propune completarea cu un nou alineat cu următorul cuprins: „(3) Activitatea membrilor Consiliului consultativ nu este remunerată.”	**Se acceptă.** Proiectul a fost modificat conform propunerii.
	11.	La art. 22 pct. 18), prevederea referitoare la stabilirea taxelor urmează a fi revizuită și clarificată, inclusiv din perspectiva impactului acestora asupra întreprinderilor mici și mijlocii.	**Precizare.** Prevederea de la art. 22 pct. 18) din proiect reprezintă o transpunere fidelă a cerinței față de organismele de evaluare a conformității prevăzute la pct. 18 din anexa la Regulamentul (UE) 2019/881.
	12.	Art. 38 se propune a fi exclus, iar prevederile privind sancțiunile contravenționale aplicate pentru încălcarea prevederilor proiectului urmează a fi incluse în Codul contravențional al Republicii Moldova, în vederea asigurării unei reglementări unitare a sancțiunilor contravenționale într-un singur act normativ și evitării dispersării acestora în legi distincte. Totodată, în vederea respectării principiului proporționalității în aplicarea sancțiunilor, se consideră necesară stabilirea unor limite concrete ale cuantumului amenzii pentru fiecare încălcare, în funcție de natura și gravitatea acesteia, precum și de circumstanțele constatate.	**Nu se acceptă.** Art. 37–38 instituie un regim special de sancțiuni administrative, integrat în mecanismul de supraveghere și control în domeniul certificării securității cibernetice. Aceste sancțiuni sunt aplicate de Agenție în cadrul unei proceduri administrative speciale de constatare și investigare, finalizată printr-o decizie motivată, supusă controlului judecătoresc potrivit Codului administrativ.

			Menținerea sancțiunilor în legea specială este justificată prin caracterul specific al încălcărilor, care decurg nemijlocit din obligațiile, procedurile și mecanismele de certificare și supraveghere reglementate de proiect. Totodată, art. 37 asigură individualizarea sancțiunii în funcție de gravitatea și circumstanțele concrete ale încălcării, prin stabilirea unor limite maxime și a unor criterii de proporționalitate, inclusiv posibilitatea aplicării avertismentului pentru cazurile minore. În aceste condiții, transferarea art. 38 în Codul contravențional nu este justificată, întrucât ar separa sancțiunile de normele materiale și de mecanismul special de supraveghere, constatare și sancționare instituit prin proiect.
	13.	Totodată, proiectul implică majorarea efectivului-limită de personal al Agenției pentru Securitate Cibernetică cu 4 unități, ceea ce ar genera un impact financiar de 1 242,8 mii lei anual. Respectiv, o asemenea extindere a efectivului-limită implică cheltuieli suplimentare, atât cu caracter unic, cât și recurente, care urmează a fi evaluate distinct și argumentate corespunzător, cu respectarea principiilor, regulilor și responsabilităților statuate de Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014. Suplimentar, se menționează că, potrivit raportului operativ lunar FD-050 privind statele și efectivul de personal din autoritățile/instituțiile bugetare, la situația din 31.08.2026, aparatul central al Ministerului Dezvoltării Economice și Digitalizării înregistra 75 de funcții vacante din 257 de unități de personal precizate, rata de încadrare constituind 70,8% din efectivul prevăzut. În cadrul Agenției pentru Securitate Cibernetică, numărul funcțiilor vacante constituia 13 unități, iar numărul funcțiilor efectiv ocupate – 31 de unități, rata de încadrare constituind 70,5%. Aceiași indicatori, în medie, au fost raportați de Agenție pe parcursul anului 2026, respectiv 14/13 funcții vacante și 30/31 funcții ocupate. În acest sens, se conturează necesitatea identificării	**Nu se acceptă.** Proiectul de lege atribuie Agenției pentru Securitate Cibernetică un mandat nou, distinct de cel exercitat în prezent în temeiul Legii nr. 48/2023 privind securitatea cibernetică, și anume cel de autoritate națională de certificare a securității cibernetice (art. 4–6 din proiect). Atribuțiile aferente acestui mandat nu se regăsesc în Regulamentul de organizare și funcționare a Agenției, aprobat prin Hotărârea Guvernului nr. 1028/2023, și nici în fișele de post ale personalului existent. Este vorba, în special, de: elaborarea, consultarea, aprobarea și revizuirea periodică a sistemelor naționale de certificare; autorizarea și monitorizarea organismelor de evaluare a conformității, în cooperare cu MOLDAC; supravegherea titularilor de certificate și a producătorilor/furnizorilor care emit declarații de conformitate; recunoaș-

		unor soluții optime pentru acoperirea necesarului de personal, inclusiv din contul funcțiilor vacante existente, precum și examinarea posibilității anulării, la solicitare, a moratoriului. Optimizarea efectivului-limită, prin prisma funcțiilor exercitate și a necesităților reale de personal, reprezintă o condiție prioritară în contextul neadmiterii majorării ponderii cheltuielilor de personal în PIB, în raport cu indicatorul-țintă prestabilit.	terea certificatelor europene de securitate cibernetică; evidența certificatelor și al declarațiilor de conformitate; examinarea plângerilor, efectuarea investigațiilor, aplicarea măsurilor corective și a sancțiunilor (Capitolul VIII); cooperarea cu MOLDAC, ENISA și autoritățile naționale de certificare din statele membre ale UE; asigurarea secretariatului Consiliului consultativ pentru certificarea securității cibernetice și elaborarea raportului anual de sinteză. Structura propusă corespunde practicii statelor membre ale Uniunii Europene, în care atribuțiile de autoritate națională de certificare a securității cibernetice sunt exercitate, de regulă, de subdiviziuni dedicate din cadrul agențiilor naționale de securitate cibernetică (de exemplu, Direcția Evaluare și Certificare Securitate Cibernetică Noi Tehnologii, Produse și Servicii (EVAL) - Directoratul Național de Securitate Cibernetică (DNSC) - România, Certification and Compliance Division - Government Office of the Republic of Slovenia for Information Security (GISO), National Cybersecurity Certification Unit - National Security Authority (NBU) - Slovacia; National Cybersecurity Certification Authority (NCCA) - Centre for Cybersecurity Belgium (CCB) etc.). În etapa inițială, se preconizează ca certificatele de nivel „ridicat” să fie emise preponderent prin delegare către organisme de evaluare a conformității, în condițiile art. 16 alin. (2) din proiect; în cazul în care volumul activității de emitere a certificatelor de către Agenție o va justifica, necesarul de personal va fi reevaluat.

			La momentul actual, în cadrul Agenției pentru Securitate Cibernetică sunt prevăzute 44 de funcții, dintre care 31 sunt ocupate, iar 13 sunt vacante, ceea ce reprezintă o rată de încadrare de 70,5%. Acest nivel de ocupare nu indică existența unui surplus de personal, ci reflectă etapa de consolidare instituțională a Agenției, care este o autoritate relativ recent constituită și devenită funcțională în anul 2024. De la constituire și până în prezent, Agenția și-a consolidat treptat capacitatea administrativă și operațională, iar procesul de recrutare a personalului continuă, fiind planificate noi angajări în vederea ocupării funcțiilor vacante și asigurării capacității necesare pentru exercitarea integrală a atribuțiilor stabilite prin lege. Funcțiile vacante existente în cadrul Agenției sunt destinate exercitării atribuțiilor deja stabilite prin Legea nr. 48/2023 și Hotărârea Guvernului nr. 1028/2023, în special celor privind supravegherea entităților esențiale și importante, funcționarea echipei naționale de răspuns la incidente de securitate cibernetică (CSIRT), precum și gestionarea incidentelor și a crizelor de securitate cibernetică. Volumul acestor activități este în creștere, inclusiv ca urmare a extinderii obligațiilor ce decurg din procesul de transpunere și implementare a Directivei (UE) 2022/2555 (NIS 2). În aceste condiții, ocuparea funcțiilor vacante este necesară pentru asigurarea capacității Agenției de a-și exercita în mod corespunzător mandatul existent. Redirecționarea funcțiilor vacante către exercitarea noilor atribuții în domeniul certificării

			securității cibernetice nu ar conduce la acoperirea necesarului real de personal, ci la transferarea deficitului de resurse umane de la atribuțiile existente către noile atribuții. O asemenea soluție ar diminua capacitatea Agenției de a asigura supravegherea entităților reglementate, răspunsul la incidente și gestionarea crizelor cibernetice, domenii care prezintă, de asemenea, o importanță directă în contextul procesului de integrare europeană. Prin urmare, noile atribuții instituite prin proiect nu pot fi acoperite nici prin redistribuirea personalului existent, nici prin utilizarea funcțiilor vacante prevăzute pentru consolidarea capacității Agenției în domeniile deja reglementate. Personalul care urmează a fi recrutat pentru ocuparea acestor funcții este necesar pentru exercitarea atribuțiilor existente și nu reprezintă o rezervă de personal disponibilă pentru preluarea unor competențe suplimentare. În plus, exercitarea atribuțiilor de certificare a securității cibernetice presupune competențe profesionale specializate, distincte de cele necesare pentru supravegherea entităților și răspunsul la incidente. Acestea includ, după caz, competențe în domeniul evaluării conformității, standardelor ISO/IEC 17065 și ISO/IEC 17025, metodologiilor Common Criteria și EN 17640, precum și al standardizării și al schemelor europene de certificare a securității cibernetice. Prin urmare, pentru exercitarea efectivă și corespunzătoare a noilor atribuții este necesară alocarea unor resurse umane distincte, cu profil profesional adecvat domeniului certificării.

	14.	Nota de fundamentare nu reflectă impactul financiar integral aferent implementării proiectului. În aceasta sunt prezentate doar cheltuielile de personal aferente subdiviziunii, fără a fi prezentate argumentele privind necesitatea instituirii acesteia și stabilirii efectivului-limită de 4 unități. Concomitent, nu este clarificat impactul posibil asupra bugetului de stat, având în vedere că organul național de acreditare MOLDAC va fi responsabil de acreditarea organismelor de evaluare a conformității în cadrul sistemelor naționale de certificare a securității cibernetice. În acest context, urmează a fi reflectate atât eventualele venituri rezultate din perceperea plăților pentru acreditare, cât și cheltuielile suplimentare aferente activității de acreditare a acestor organisme de către MOLDAC. Subsidiar, proiectul prevede instituirea și ținerea, de către Agenția pentru Securitate Cibernetică, a Registrului certificatelor de securitate cibernetică și al declarațiilor de conformitate. Totodată, nu este clarificat dacă instituirea și administrarea registrului respectiv implică necesitatea alocării unor resurse financiare de la bugetul de stat. În cazul în care sunt necesare asemenea resurse, acestea urmează a fi estimate și argumentate în Nota de fundamentare. În final, se menționează că estimarea și argumentarea costurilor aferente proiectului cu relevanță pentru procesul de integrare europeană urmează să fie efectuate în strictă conformitate cu prevederile Hotărârii Guvernului cu privire la aprobarea Metodologiei de analiză a impactului de reglementare nr. 574/2024.	**Se acceptă.** Nota de fundamentare a fost revizuită ținând cont de propunerile formulate. Totodată, este de menționat că din prevederile legii a fost exclusă noțiunea de Registrul certificatelor de securitate cibernetică și al declarațiilor de conformitate, fiind stabilită doar responsabilitatea ASC de a ține evidența certificatelor de securitate cibernetică și al declarațiilor de conformitate și a asigura publicarea informațiilor relevante despre acestea pe pagina sa oficială, fapt care nu implică alocarea unor resurse de la bugetul de stat, altele decât cele pentru personal.
Avizare și consultare publică			

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 14 – 3407 din 02.10.2026

Cancelaria de Stat

În temeiul prevederilor pct. 38 și 185 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, se transmite *proiectul de lege privind certificarea securității cibernetice* pentru a fi inclus în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali.

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	**Criterii de înregistrare**	**Nota autorului**
1.	Categoria și denumirea proiectului	Proiectul de lege privind certificarea securității cibernetice.
2.	Autoritatea care a elaborat proiectul	Proiectul este elaborat de către Ministerul Dezvoltării Economice și Digitalizării.
3.	Justificarea depunerii cererii	Proiectul de lege este elaborat în vederea realizării: - acțiunea 51, Capitolul 10 *"Societatea informațională și mass-media"*, Clusterul 3 *"Competitivitate și Creștere Incluzivă"* din Programul Național de Aderare al Republicii Moldova la Uniunea Europeană (2025-2029), aprobat prin Hotărârea Guvernului nr. 306/2025. În conformitate cu acțiunea prevăzută, Ministerul Dezvoltării Economice și Digitalizării este responsabil de elaborarea proiectului de lege privind certificarea securității cibernetice, în vederea instituirii cadrului juridic și instituțional național pentru certificarea securității cibernetice a produselor, serviciilor și proceselor TIC, precum și a serviciilor de securitate gestionate, în conformitate cu cerințele și principiile Uniunii Europene. Elaborarea cadrului normativ presupune instituirea unui mecanism național de certificare, definirea rolurilor și responsabilităților autorităților și entităților implicate, precum și stabilirea procedurilor de certificare și evaluare a conformității.
4.	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte*	Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) –Clusterul 3, Capitolul 10, acțiunea 51.

	documente de planificare sectoriale)	
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător 3. Centrul de Armonizare a Legislaţiei 4. Centrul Naţional pentru Protecţia Datelor cu Caracter Personal 5. Ministerul Infrastructurii și Dezvoltării Regionale 6. Ministerul Finanțelor 7. Ministerul Mediului 8. Ministerul Sănătății 9. Ministerul Apărării 10. Ministerul Afacerilor Interne 11. Ministerul Afacerilor Externe 12. Serviciul de Informații și Securitate 13. Agenția Servicii Publice 14. Agenția Națională pentru Reglementare în Comunicații 15. Serviciul Tehnologia Informației și Securitate Cibernetică
6.	Termenul-limită pentru depunerea avizelor/expertizelor	Termen-limită de prezentare a avizelor - 10 zile lucrătoare.
7.	Persoana responsabilă de promovarea proiectului	Cușcă Andrei - Șef al Direcției politici în domeniul digitalizării serviciilor publice, securității cibernetice și serviciilor de încredere. Tel: 022250557; email: andrei.cusca@mded.gov.md Muntean Tatiana - consultant principal, Direcția politici în domeniul digitalizării serviciilor publice, securității cibernetice și serviciilor de încredere. Tel: 022 232327; email: tatiana.muntean@mded.gov.md
8.	Anexe	1. Proiectul de lege 2. Nota de fundamentare 3. Tabel de concordanță
9.	Data și ora depunerii cererii	
10.	Semnătura	/semnat electronic/

Ministru **Claudiu-Iulius-Gavril NĂSUI**

Ex: Tatiana Muntean
Tel: 022-23-23-27

Coordonare:

Șef, Direcția politici în domeniul digitalizării serviciilor publice, securității cibernetice și serviciilor de încredere	
Secretar de stat	