Amendamentul 2
Cristian-Silviu Buşoi
în numele Comisiei pentru industrie, cercetare şi energie

Raport **A9-0307/2023**
Josianne Cutajar
Serviciile de securitate gestionate
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Propunere de regulament
–

AMENDAMENTELE PARLAMENTULUI EUROPEAN*

la propunerea Comisiei

REGULAMENTUL (UE) 2024/...
AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

din ...

de modificare a Regulamentului (UE) 2019/881 în ceea ce priveşte serviciile de securitate gestionate

(Text cu relevanţă pentru SEE)

PARLAMENTUL EUROPEAN ŞI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naţionale,

---

* Amendamente: textul nou sau modificat este marcat cu caractere cursive aldine; textul eliminat este marcat prin simbolul ▌.

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

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară[2],

[1] ***JO C 349, 29.9.2023, p. 167.***

[2] ***Poziția Parlamentului European din ... [(JO …)/(republicată încă în Jurnalul Oficial)] și decizia Consiliului din …***

întrucât:

(1) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[3] stabilește 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 ***din domeniul tehnologiei informației și comunicațiilor (***TIC***)***, a serviciilor TIC și a proceselor TIC în Uniune, precum și cu scopul de a evita fragmentarea pieței interne în ceea ce privește sistemele de certificare a securității cibernetice din Uniune.

(2) Pentru a asigura reziliența Uniunii la atacurile cibernetice și pentru a preveni orice vulnerabilități de pe piața Uniunii, prezentul regulament este destinat să completeze cadrul de reglementare orizontal care stabilește cerințe cuprinzătoare în materie de securitate cibernetică pentru toate produsele cu elemente digitale în conformitate cu Regulamentul (UE).../... al Parlamentului European și al Consiliului[4] (2022/0272(COD)), stabilind cerințe esențiale pentru serviciile de securitate cibernetică gestionate, pentru aplicarea și fiabilitatea acestora.

---

3 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) (JO L 151, 7.6.2019, p. 15).

4 ***Regulamentul (UE) .../... al Parlamentului European și al Consiliului din ... privind ... (JO L, …, ELI: …).***

(3) Serviciile de securitate gestionate ***sunt servicii furnizate de furnizorii de servicii de securitate gestionate conform definiției de la articolul 6 punctul 40 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[5]. Prin urmare, definiția serviciilor de securitate gestionate din prezentul regulament ar trebui să fie în concordanță cu cea a furnizorilor de servicii de securitate gestionate din Directiva (UE) 2022/2555. Serviciile respective*** constau în desfășurarea de activități legate de gestionarea riscurilor în materie de securitate cibernetică ale clienților lor sau în furnizarea de asistență pentru astfel de activități, ***și*** au dobândit o importanță din ce în ce mai mare în prevenirea și atenuarea incidentelor de securitate cibernetică. În consecință, furnizorii acestor servicii sunt considerați entități esențiale sau importante care aparțin unui sector cu o importanță critică ridicată în temeiul Directivei (UE) 2022/2555 ▌. În conformitate cu considerentul 86 din directiva respectivă, furnizorii de servicii de securitate gestionate în domenii precum răspunsul în caz de incidente, testele de penetrare, auditurile de securitate și consultanța joacă un rol deosebit de important în sprijinirea entităților în eforturile lor de a preveni și de a detecta incidente, de a răspunde la acestea și de a se redresa după incidente. Totuși, și furnizorii de servicii de securitate gestionate au fost ținta atacurilor cibernetice și prezintă un risc deosebit din cauza integrării lor strânse în operațiunile clienților lor. Prin urmare, entitățile esențiale și entitățile importante în sensul Directivei (UE) 2022/2555 ar trebui să dea dovadă de o diligență sporită în selectarea unui furnizor de servicii de securitate gestionate.

---

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

(4) Definiția serviciilor de securitate gestionate în temeiul prezentului regulament include o listă neexhaustivă a serviciilor de securitate gestionate care s-ar putea califica pentru sisteme de certificare, cum ar fi gestionarea incidentelor, testele de penetrare, auditurile de securitate și consultanța legată de asistența tehnică. Serviciile de securitate gestionate ar putea include servicii de securitate cibernetică care sprijină pregătirea, prevenirea, detectarea, analiza, atenuarea, răspunsul la incidentele de securitate cibernetică și redresarea în urma acestora. Furnizarea de informații privind amenințările cibernetice și evaluarea riscurilor legate de asistența tehnică ar putea fi, de asemenea, considerate servicii de securitate gestionate. Pot exista sisteme europene de certificare a securității cibernetice separate pentru diferite servicii de securitate gestionate. Certificatele europene de securitate cibernetică eliberate în conformitate cu astfel de sisteme ar trebui să se refere la servicii de securitate gestionate specifice ale unui anumit furnizor de astfel de servicii.

(5) Furnizorii de servicii de securitate gestionate ***pot juca***, de asemenea, un rol important în ***ceea ce privește acțiunile Uniunii de sprijinire a răspunsului și a redresării*** imediate ▌ în cazul unor incidente de securitate cibernetică semnificative și de mare amploare***, bazându-se pe servicii furnizate de furnizori privați de încredere și pe testarea entităților critice pentru potențiale vulnerabilități pe baza evaluărilor riscurilor la nivelul UE. Certificarea serviciilor de securitate gestionate poate juca un rol în selectarea furnizorilor*** de încredere ▌ .

(6) Certificarea serviciilor de securitate gestionate nu este relevantă numai în procesul de selecție pentru rezerva pentru securitate cibernetică a UE, ci este și un indicator de calitate esențial pentru entitățile private și publice care intenționează să achiziționeze astfel de servicii. Având în vedere caracterul critic al serviciilor de securitate gestionate și sensibilitatea datelor pe care le prelucrează, certificarea ar putea oferi potențialilor clienți orientări și asigurări importante cu privire la credibilitatea acestor servicii. Sistemele europene de certificare pentru serviciile de securitate gestionate contribuie la evitarea fragmentării pieței unice. Prin urmare, prezentul regulament vizează îmbunătățirea funcționării pieței interne.

(7) ***Sistemele europene de certificare pentru serviciile de securitate gestionate ar trebui să conducă la adoptarea acestor servicii și la creșterea concurenței între furnizorii care oferă servicii de securitate gestionate. Fără a aduce atingere obiectivului de a asigura niveluri suficiente și adecvate de cunoștințe tehnice relevante și de integritate profesională a acestor furnizori, sistemele de certificare ar trebui, prin urmare, să faciliteze intrarea pe piață și oferirea de servicii de securitate gestionate, prin simplificarea, în măsura posibilului, a sarcinii de reglementare, administrative și financiare potențiale cu care s-ar putea confrunta furnizorii, în special microîntreprinderile sau întreprinderile mici și mijlocii (IMM-uri), atunci când oferă servicii de securitate gestionate. În plus, pentru a încuraja adoptarea și stimularea cererii de servicii de securitate gestionate, sistemele ar trebui să contribuie la accesibilitatea acestora, în special pentru actorii mai mici, cum ar fi microîntreprinderile și IMM-urile, precum și pentru autoritățile locale și regionale care au capacitate și resurse limitate, dar care sunt mai predispuse la încălcări ale securității cibernetice cu implicații financiare, juridice, legate de reputație și operaționale.***

(8) Este important să se ofere sprijin microîntreprinderilor și întreprinderilor mici și mijlocii (IMM-uri) în punerea în aplicare a prezentului regulament și în recrutarea competențelor și a expertizei specializate în materie de securitate cibernetică necesare pentru a furniza servicii de securitate gestionate în conformitate cu cerințele prevăzute în prezentul regulament. Programul Europa digitală și alte programe relevante ale Uniunii prevăd instituirea de către Comisie a unui sprijin financiar și tehnic care să permită acestor întreprinderi să contribuie la creșterea economiei europene și la consolidarea nivelului comun de securitate cibernetică europeană în peisajul UE, inclusiv prin raționalizarea sprijinului financiar din partea programului Europa digitală și a altor programe relevante ale Uniunii și prin sprijinirea microîntreprinderilor și a IMM-urilor.

(9) Sistemul de certificare al Uniunii pentru serviciile de securitate gestionate ar trebui să contribuie la disponibilitatea unor servicii securizate și de înaltă calitate care să garanteze o tranziție digitală sigură și la atingerea obiectivelor stabilite în programul de politică privind deceniul digital, în special corelat cu obiectivul ca 75 % dintre întreprinderile Uniunii să înceapă să utilizeze cloud, IA sau volumele mari de date, ca peste 90 % dintre microîntreprinderi și IMM-uri să atingă cel puțin un nivel de bază de intensitate digitală și ca serviciile publice esențiale să fie oferite online.

(10) Pe lângă implementarea produselor TIC, a serviciilor TIC sau a proceselor TIC, serviciile de securitate gestionate oferă adesea caracteristici suplimentare ale serviciilor care se bazează pe competențele, calificările și experiența personalului lor. Un nivel foarte ridicat al acestor competențe și calificări și al acestei experiențe, precum și proceduri interne adecvate ar trebui să facă parte din obiectivele de securitate pentru a asigura un nivel foarte înalt al calității serviciilor de securitate gestionate furnizate. Prin urmare, pentru a se asigura că toate aspectele ***serviciilor de securitate gestionate*** pot face obiectul ***unor sisteme*** de certificare ***specifice***, este necesar să se modifice Regulamentul (UE) 2019/881. ***Ar trebui luate în considerare rezultatele și recomandările evaluării și revizuirii prevăzute în*** Regulamentul (UE) ***2019/881.***

(11) Pentru a facilita creșterea unei piețe fiabile a Uniunii, creând în același timp parteneriate cu țări terțe care împărtășesc aceeași viziune, procesul de certificare instituit în cadrul stabilit prin prezentul regulament ar trebui să fie raționalizat pentru a facilita recunoașterea internațională și alinierea la standardele internaționale.

(12) Uniunea se confruntă cu o penurie de talente, caracterizată de un deficit de profesioniști calificați, și cu evoluția rapidă a amenințărilor, după cum se recunoaște în comunicarea Comisiei din 18 aprilie 2023 privind Academia de competențe în materie de securitate cibernetică. Resursele educaționale și tipurile de formare formală diferă, iar cunoștințele pot fi dobândite în diferite moduri, atât formale, de exemplu prin universități sau cursuri, cât și informale, de exemplu prin formare la locul de muncă sau experiență profesională în domeniul relevant. Prin urmare, pentru a facilita apariția unor servicii de securitate gestionate esențiale și de înaltă calitate și pentru a avea o imagine de ansamblu mai bună asupra componenței forței de muncă din Uniune în domeniul securității cibernetice, este important ca cooperarea dintre statele membre, Comisie, ENISA și părțile interesate, inclusiv sectorul privat și mediul academic, să fie întărită prin dezvoltarea de parteneriate public-privat, prin sprijinirea inițiativelor de cercetare și inovare, prin elaborarea și recunoașterea reciprocă a unor standarde comune și certificarea competențelor în securitate cibernetică, inclusiv prin Cadrul european de competențe în materie de securitate cibernetică. O astfel de cooperare ar facilita deopotrivă mobilitatea profesioniștilor din domeniul securității cibernetice în interiorul Uniunii, cât și integrarea cunoștințelor de securitate cibernetică în programele educaționale și de formare, asigurând în același timp accesul la ucenicii și stagii pentru tineri, inclusiv pentru persoanele care trăiesc în regiuni defavorizate, cum ar fi insulele, zonele slab populate, zonele rurale și îndepărtate. Este important ca aceste măsuri să vizeze atragerea unui număr mai mare de femei și fete în domeniu și să contribuie la abordarea disparității de gen în domeniul științei, tehnologiei, ingineriei și matematicii și ca sectorul privat să urmărească să ofere cursuri de formare la locul de muncă care să abordeze competențele cele mai solicitate, implicând administrația publică și întreprinderile nou-înființate, precum și microîntreprinderile și IMM-urile. De asemenea, este important ca furnizorii și statele membre să colaboreze și să contribuie la colectarea de date privind situația și evoluția pieței forței de muncă în domeniul securității cibernetice.

(13) ENISA joacă un rol important în pregătirea propunerilor de sisteme europene de certificare. La elaborarea proiectului de buget general al Uniunii, Comisia ar trebui să evalueze resursele bugetare necesare pentru schema de personal a ENISA, în conformitate cu procedura prevăzută la articolul 29 din Regulamentul (UE) 2019/881.

(14) Prezentul regulament prevede modificări specifice ale Regulamentului (UE) 2019/881 pentru a adăuga posibilitatea de a crea sisteme de certificare a securității cibernetice pentru furnizorii de servicii de securitate gestionate. În acest sens, specifică și clarifică, de asemenea, anumite dispoziții privind pregătirea și funcționarea tuturor sistemelor europene de certificare a securității cibernetice, în vederea asigurării transparenței și deschiderii acestora. Aceste din urmă modificări, care se limitează la specificarea sau clarificarea Regulamentului (UE) 2019/881, în special modificările aduse articolelor 49 și 49a, nu ar trebui să aducă atingere în niciun fel evaluării și revizuirii mai ample a regulamentului respectiv prevăzute la articolul 67, inclusiv, în mod specific, evaluării impactului, eficacității și eficienței titlului din regulamentul respectiv referitor la sistemele de certificare a securității cibernetice. Această evaluare și revizuire a titlului referitor la sistemele de certificare a securității cibernetice ar trebui să se bazeze pe o consultare amplă a părților interesate și pe o analiză completă și aprofundată a procedurilor implicate.

(15) Deoarece obiectivul prezentului regulament, și anume de a permite adoptarea unor sisteme europene de certificare a securității cibernetice pentru serviciile de securitate gestionate, nu poate fi realizat în mod satisfăcător de statele membre dar, având în vedere dimensiunile și efectele sale, poate fi realizat mai bine la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(16) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[6] și a emis un aviz la 10 ianuarie 2024[7],

ADOPTĂ PREZENTUL REGULAMENT:

---

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

7 ***JO C.../....***

Articolul 1

Modificări aduse Regulamentului (UE) 2019/881

Regulamentul (UE) 2019/881 se modifică după cum urmează:

1. La articolul 1 alineatul (1) primul paragraf, litera (b) se înlocuiește cu următorul text:

„(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 certificare a securității cibernetice din Uniune.”

2. Articolul 2 se modifică după cum urmează:

(a) punctele 9, 10 și 11 se înlocuiesc cu următoarele:

„9. «sistem european de certificare a securității cibernetice» înseamnă un 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;

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 și serviciilor de securitate gestionate care intră în domeniul de aplicare al sistemului în cauză;

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;”;

(b) se introduce următorul punct:

„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 consultanță de specialitate, în legătură cu asistența tehnică;***”;

(c) punctele 20, 21 și 22 se înlocuiesc cu următorul text:

„20. «specificații tehnice» 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;

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;

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;”;

3. La articolul 4, alineatul (6) se înlocuiește cu următorul text:

„(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.”

4. Articolul 8 se modifică după cum urmează:

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

„(1) ENISA sprijină și promovează elaborarea și punerea în aplicare a politicii Uniunii privind certificarea securității cibernetice 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).”

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

„(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.”

(c) alineatul (5) se înlocuiește cu următorul text:

„(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. La articolul 46, alineatele (1) și (2) se înlocuiesc cu următorul text:

„(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 securității cibernetice, în scopul creării unei piețe unice digitale pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate.

(2) Cadrul european de certificare a securității cibernetice prevede un mecanism de instituire a unor sisteme europene de certificare a securității cibernetice. Acesta atestă 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 aceste 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, calificările și experiența necesare, cu un nivel ***suficient și adecvat*** de cunoștințe tehnice relevante și de integritate profesională.”

6. La articolul 47, alineatele (2) și (3) se înlocuiesc cu următorul text:

„(2) Programul de activitate etapizat la nivelul Uniunii include îndeosebi o listă a produselor TIC, a serviciilor TIC, a proceselor TIC sau a categoriilor acestora și a serviciilor de securitate gestionate care pot beneficia de includerea în sfera de aplicare a unui sistem european de certificare a securității cibernetice.

(3) Includerea unui anumit produs TIC, serviciu TIC, proces TIC sau a unei categorii a acestora ori a unor servicii de securitate gestionate în programul de activitate etapizat la nivelul Uniunii se justifică în baza unuia sau a mai multora dintre considerentele următoarele:

(a) disponibilitatea și dezvoltarea sistemelor naționale de certificare a securității cibernetice care se aplică oricărei categorii specifice de produse TIC, servicii TIC, sau procese TIC sau servicii de securitate gestionate, cu 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 și a standardelor internaționale și industriale;

(d) dezvoltările din domeniul amenințărilor cibernetice;

(e) solicitarea de pregătire a unei propuneri de sistem specifice de către ECCG.”

7. ▌Articolul 49 ***se modifică după cum urmează***:

(a) alineatele (1), (2), (3) și (4) se înlocuiesc cu următorul text:

„(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.

(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 refuzare a unei astfel de solicitări se ia de către consiliul de administrație.

(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 conformitate cu articolul 49 alineatul (6), ENISA furnizează informații cu privire la modul în care a respectat această obligație.

(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 oferi ENISA consiliere și expertiză specifice. Grupurile de lucru ad-hoc instituite în acest scop includ, după caz și fără a aduce atingere procedurilor și marjei de apreciere stabilite la articolul 20 alineatul (4), experți din administrațiile publice ale statelor membre, din instituțiile, organele, oficiile și agențiile Uniunii și din sectorul privat."

(b) alineatul (7) se înlocuiește cu următorul text:

„(7) Pe baza propunerii de sistem pregătite de ENISA, Comisia poate adopta acte de punere în aplicare care să prevadă sisteme europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care îndeplinesc cerințele 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)."

8. Se introduce următorul articol:

„Articolul 49a

Informații și consultare privind sistemele europene de certificare a securității cibernetice

(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 menționat la articolul 48.

(2) În cursul pregătirii de către ENISA a unei propuneri de sistem în conformitate cu articolul 49, Parlamentul European și Consiliul pot solicita Comisiei, în calitatea sa de președinte al Grupului european pentru certificarea securității cibernetice (ECCG) și al ENISA, să prezinte trimestrial informații relevante cu privire la un proiect de sistem. La cererea Parlamentului European 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 unui proiect de sistem, într-un mod adecvat nivelului de confidențialitate necesar și, după caz, în mod restrâns.

(3) Pentru a consolida dialogul dintre instituțiile Uniunii și pentru a contribui la un proces de consultare formal, deschis, transparent și favorabil incluziunii, Parlamentul European și Consiliul 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.

(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 conformitate cu articolul 67.”

9. Articolul 51 se modifică după cum urmează:

(a) titlul se înlocuiește cu următorul text:

„Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice pentru produsele TIC, serviciile TIC și procesele TIC”

(b) teza introductivă se înlocuiește cu următorul text:

„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:”

10. Se introduce următorul articol:

„Articolul 51a
Obiectivele de securitate ale sistemelor europene de certificare a securității cibernetice 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, calificările 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) să protejeze datele accesate, stocate, transmise sau prelucrate în alt mod în legătură cu furnizarea de servicii de securitate gestionate 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) să înregistreze și să permită să se evalueze 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 în mod implicit și începând cu momentul conceperii și***, după caz,*** includ cele mai recente actualizări de securitate ***și nu conțin vulnerabilități cunoscute public***.”

11. Articolul 52 se modifică după cum urmează:

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

„(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 probabilitate și impact al unui incident.”

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

„(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.”

(c) alineatele (5), (6) și (7) se înlocuiesc cu următorul text:

„(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 și serviciile de securitate gestionate pentru care se eliberează certificatul respectiv sau declarația de conformitate UE 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 atacuri cibernetice. Activitățile de evaluare 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 și 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 riscurilor de incidente și atacuri cibernetice desfășurate de actori cu competențe și resurse limitate. Activitățile de evaluare care trebuie întreprinse includ cel puțin următoarele: o examinare pentru a demonstra absența vulnerabilităților cunoscute public și testarea faptului 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 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 și 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 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.”

12. La articolul 53, alineatele (1), (2) și (3) se înlocuiesc cu următorul text:

„(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 și 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 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.

(3) Producătorul sau furnizorul de produse TIC, servicii TIC, procese TIC sau servicii de securitate gestionate pun la dispoziția autorității naționale de certificare a securității cibernetice menționată la articolul 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 produselor TIC, a serviciilor TIC sau a serviciilor de securitate gestionate cu sistemul. O copie a declarației de conformitate UE se transmite către autoritatea națională de certificare a securității cibernetice și către ENISA.”

13. La articolul 54, alineatul (1) se modifică după cum urmează:

(a) litera (a) se înlocuiește cu următorul text:

„(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;”;

(aa) litera (g) se înlocuiește cu următorul text:

„(g) criteriile și metodele specifice de evaluare, inclusiv tipurile de evaluări, utilizate pentru a demonstra că obiectivele de securitate aplicabile menționate la articolele 51 și 51a sunt îndeplinite;”;

(b) litera (j) se înlocuiește cu următorul text:

„(j) normele pentru monitorizarea conformității produselor TIC, serviciilor TIC, proceselor TIC și 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;”;

(c) litera (l) se înlocuiește cu următorul text:

„(l) normele privind consecințele neconformității produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate care au fost certificate sau pentru care a fost eliberată o declarație de conformitate UE, dar care nu sunt conforme cu cerințele sistemului;”;

(d) litera (o) se înlocuiește cu următorul text:

„(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 și servicii de securitate gestionate, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare;”;

(e) litera (q) se înlocuiește cu următorul text:

„(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;”;

14. Articolul 56 se modifică după cum urmează:

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

„(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.”

(b) alineatul (3) se modifică după cum urmează:

(i) primul paragraf se înlocuiește cu textul următor:

„Comisia evaluează periodic eficiența și utilizarea sistemelor europene de certificare a securității cibernetice adoptate și analizează dacă un anumit 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 a serviciilor de securitate gestionate în Uniune și pentru a se îmbunătăți funcționarea pieței interne. Prima 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.”

(ii) al treilea paragraf se modifică după cum urmează:

(aa) litera (a) se înlocuiește cu următorul text:

„(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;”;

(bb) litera (d) se înlocuiește cu următorul text:

„(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 microîntreprinderilor și ale*** IMM-urilor;”;

(c) alineatele (7) și (8) se înlocuiesc cu următorul text:

„(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 menționată la articolul 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.

(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 sau a serviciilor de securitate gestionate certificat(e), care pot avea un impact asupra conformității sale cu cerințele legate de certificare. Autoritatea sau organismul respectiv transmite aceste informații fără întârzieri nejustificate autorității naționale de certificare a securității cibernetice în cauză.”

15. La articolul 57, alineatele (1) și (2) se înlocuiesc cu următorul text:

„(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.

(2) Statele membre nu introduc noi sisteme naționale de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate care fac deja obiectul unui sistem european de certificare a securității cibernetice în vigoare.”

16. Articolul 58 se modifică după cum urmează:

(a) alineatul (7) se modifică după cum urmează:

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

„(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 eliberate pe teritoriile lor respective, în cooperare cu alte autorități relevante de supraveghere a pieței;

(b) monitorizează 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 pun în aplicare aceste obligații, în special 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;”;

(ii) litera (h) se înlocuiește cu următorul text:

„(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 și a serviciilor de securitate gestionate cu cerințele prezentului regulament sau cu cerințele sistemului european de certificare a securității cibernetice specific; și;”;

(b) alineatul (9) se înlocuiește cu următorul text:

„(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.”

17. La articolul 59 alineatul (3), literele (b) și (c) se înlocuiesc cu următorul text:

„(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);”;

18. La articolul 67, alineatele (2) și (3) se înlocuiesc cu următorul text:

„(2) Evaluarea analizează, de asemenea, impactul, eficacitatea și eficiența dispozițiilor din titlul III din prezentul regulament***, inclusiv procedurile care conduc la adoptarea sistemelor 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.

(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 Uniunii.”.

19. Anexa se înlocuiește cu textul prevăzut la anexa la prezentul regulament.

Articolul 2

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

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

Adoptat la ...,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

ANEXĂ

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 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 sau 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 implicați 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 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 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 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 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 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 relevant care este armonizat în temeiul Regulamentului (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 relevant care este armonizat în temeiul Regulamentului (CE) nr. 765/2008 pentru acreditarea laboratoarelor care efectuează testări.

Or. en