2025/37

15.1.2025

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

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

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

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară ([2]),

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 internă, 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 temeiul Regulamentului (UE) 2024/2847 al Parlamentului European și al Consiliului ([4]), stabilind obiective de securitate pentru serviciile de securitate gestionate, precum și pentru aplicarea și fiabilitatea serviciilor respective.

(3) Serviciile de securitate gestionate sunt furnizate de furnizorii de servicii de securitate gestionate, în sensul definiției de la articolul 6 punctul 40 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului ([5]). Definiția serviciilor de securitate gestionate din prezentul regulament ar trebui, prin urmare, 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. 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. Astfel cum se prevede în considerentul 86 din directiva respectivă, furnizorii de servicii de securitate gestionate în domenii precum răspunsul în caz de incidente, testele de rezistență la intruziuni, 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. Cu toate acestea, 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, este important ca entitățile esențiale și entitățile importante, în înțelesul Directivei (UE) 2022/2555, să dea dovadă de o diligență sporită în selectarea furnizorilor de servicii de securitate gestionate.

([1]) JO C 349, 29.9.2023, p. 167.

([2]) Poziția Parlamentului European din 24 aprilie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 2 decembrie 2024.

([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) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([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 europene de certificare a securității cibernetice, cum ar fi gestionarea incidentelor, testele de rezistență la intruziuni, 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 incidente 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. Ar putea 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 inițiale în cazul unor incidente semnificative și al unor incidente de securitate cibernetică de mare amploare, bazându-se pe servicii furnizate de furnizori privați de încredere și pe testarea entităților critice pentru potențiale vulnerabilități pe baza evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate. Certificarea serviciilor de securitate gestionate ar putea juca un rol în selectarea furnizorilor de încredere de servicii de securitate gestionate, în sensul definiției din Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului ([6]).

(6) Certificarea serviciilor de securitate gestionate nu este relevantă numai în procesul de selecție pentru rezerva UE pentru securitate cibernetică instituită prin Regulamentul (UE) 2025/38, 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 prelucrate, certificarea ar putea oferi potențialilor clienți orientări și asigurări importante cu privire la credibilitatea serviciilor respective. Sistemele europene de certificare a securității cibernetice pentru serviciile de securitate gestionate sunt destinate să contribuie la evitarea fragmentării pieței interne. Prin urmare, prezentul regulament vizează îmbunătățirea funcționării pieței interne.

(7) Sistemele europene de certificare a securității cibernetice pentru serviciile de securitate gestionate ar trebui să conducă la adoptarea serviciilor respective și la creșterea concurenței între furnizorii de 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 întreprinderile mici și mijlocii (IMM-uri), inclusiv microîntreprinderile, atunci când oferă servicii de securitate gestionate. În plus, pentru a încuraja adoptarea și stimularea cererii de servicii de securitate gestionate, sistemele europene de certificare a securității cibernetice ar trebui să contribuie la accesibilitatea acestora, în special pentru actorii mai mici, cum ar fi IMM-urile, inclusiv microîntreprinderile, 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 IMM-urilor, inclusiv microîntreprinderilor, 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” instituit prin Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului ([7]) și alte programe relevante ale Uniunii prevăd instituirea de către Comisie a unui sprijin financiar și tehnic care să permită întreprinderilor respective să contribuie la creșterea economiei Uniunii și la consolidarea nivelului comun de securitate cibernetică în Uniune, inclusiv prin raționalizarea sprijinului financiar din partea programului Europa digitală și a altor programe relevante ale Uniunii și prin sprijinirea IMM-urilor, inclusiv a microîntreprinderilor.

(9) Sistemele europene de certificare a securității cibernetice 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 țintelor stabilite în programul de politică pentru 2030 privind deceniul digital instituit prin Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului ([8]), în special corelat cu obiectivul ca 75 % dintre întreprinderile Uniunii să înceapă să utilizeze servicii de tip cloud computing, volume mari de date sau inteligență artificială, ca peste 90 % dintre IMM-uri, inclusiv microîntreprinderi, să atingă cel puțin un nivel de bază de

([6]) Regulamentul (UE) 2025/38 al Parlamentului European și al Consiliului din 19 decembrie 2024 de stabilire a unor măsuri de consolidare a solidarității și a capacităților la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și răspunsul la acestea și de modificare a Regulamentului (UE) 2021/694 (Regulamentul privind solidaritatea cibernetică) (JO L, 2025/38 , 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Regulamentul (UE) 2021/694 al Parlamentului European și al Consiliului din 29 aprilie 2021 de instituire a programului „Europa digitală” și de abrogare a Deciziei (UE) 2015/2240 (JO L 166, 11.5.2021, p. 1).

([8]) Decizia (UE) 2022/2481 a Parlamentului European și a Consiliului din 14 decembrie 2022 de instituire a programului de politică pentru 2030 privind deceniul digital (JO L 323, 19.12.2022, p. 4).

intensitate digitală și ca serviciile publice esențiale să fie accesibile 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, expertiza și experiența personalului furnizorilor de astfel de servicii. Un nivel foarte ridicat al acestor competențe și al acestei expertize și 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 europene de certificare a securității cibernetice specifice, este necesar să se modifice Regulamentul (UE) 2019/881. Ar trebui să fie luate în considerare rezultatele și recomandările evaluării și revizuirii prevăzute în Regulamentul (UE) 2019/881.

(11) Pentru a facilita creșterea unei piețe fiabile interne, creând în același timp parteneriate cu țări terțe cu valori comune, procesul de certificare instituit în cadrul european de certificare a securității cibernetice prevăzut în Regulamentul (UE) 2019/881 ar trebui să fie implementat într-un mod care facilitează 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 intitulată „Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE («Academia de competențe în materie de securitate cibernetică»)". Resursele educaționale și tipurile de formare formală diferă, iar cunoștințele pot fi dobândite în diferite moduri: formale, de exemplu prin universități sau cursuri, sau 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 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, Agenția Uniunii Europene pentru Securitate Cibernetică instituită prin Regulamentul (UE) 2019/881 (ENISA) și părțile interesate, inclusiv din 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 și a formării în acest domeniu în programele educaționale, 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 o astfel de cooperare 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 IMM-urile, inclusiv microîntreprinderile. 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 a securității cibernetice. 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 permite instituirea de sisteme europene de certificare a securității cibernetice pentru serviciile de securitate gestionate. În acest sens, prezentul regulament specifică și clarifică, de asemenea, anumite dispoziții din regulamentul respectiv 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 privind informațiile pe care ENISA trebuie să le furnizeze atunci când transmite o propunere de sistem, grupurile de lucru ad-hoc instituite pentru fiecare propunere de sistem și informarea și consultarea în legătură cu sistemele europene de certificare a securității cibernetice, nu ar trebui să aducă atingere în niciun fel evaluării și revizuirii mai ample a regulamentului respectiv în temeiul articolul 67 din regulamentul menționat, în special evaluării impactului, eficacității și eficienței titlului din regulamentul respectiv referitor la cadrul european de certificare a securității cibernetice. Evaluarea și revizuirea titlului respectiv ar trebui să se bazeze pe o consultare amplă a părților interesate și pe o analiză completă și aprofundată a procedurilor implicate.

(15) Întrucât obiectivul prezentului regulament, și anume de a permite instituirea 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 amploarea și efectele sale, acesta poate fi realizat mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este prevăzut la articolul respectiv, 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 ([9]) și a emis un aviz la 10 ianuarie 2024,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modificarea 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 sau 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 consultanța de specialitate, în legătură cu asistența tehnică;”;

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

„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;

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

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 modifică după cum urmează:

(i) partea introductivă 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:";

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

„(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;";

(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. Articolul 46 se înlocuiește cu următorul text:

„Articolul 46

Cadrul european de certificare a securității cibernetice

(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 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 de cunoștințe tehnice relevante și de integritate profesională."

6. Articolul 47 se modifică după cum urmează:

(a) alineatul (2) se înlocuiește cu următorul text:

„(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.";

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

(i) partea introductivă se înlocuiește cu următorul text:

„(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:";

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

„(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 precădere în ceea ce privește riscul de fragmentare;";

(iii) se introduce următoarea literă:

„(ca) evoluțiile tehnologice și disponibilitatea și dezvoltarea sistemelor internaționale de certificare a securității cibernetice, a standardelor internaționale și a standardelor aplicate în industrie;".

7. Articolul 49 se modifică după cum urmează:

(a) alineatele (1)-(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 refuz al 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 temeiul alineatului (6), ENISA furnizează informații cu privire la modul în care a respectat prezentul alineat.

(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.";

(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 un sistem european de certificare a securității cibernetice pentru 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)."

8. Se introduce următorul articol:

„*Articolul 49a*

Informarea și consultarea 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, astfel cum se menționează la articolul 48.

(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 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.

(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.

(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.”

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) partea 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, 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."

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 sau 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 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 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 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."

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 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 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 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.”

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;”;

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

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

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

„(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;”;

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

„(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 UE, dar care nu sunt conforme cu cerințele sistemului;”;

(e) 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 sau servicii de securitate gestionate, cerințele de securitate și criteriile și metodele de evaluare și nivelurile de asigurare;”;

(f) 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, 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.”;

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

— 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;”;

— 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 IMM-urilor, inclusiv ale microîntreprinderilor;”;

(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 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.

(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.”

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 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;";

(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 sau a serviciilor de securitate gestionate cu cerințele prezentului regulament sau cu cerințele sistemelor europene de certificare a securității cibernetice specifice; 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 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.

(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."

19. Anexa se modifică în conformitate cu 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 Bruxelles, 19 decembrie 2024.

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*
R. METSOLA	BÓKA J.

ANEXĂ

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

1. Punctele 2-5 se înlocuiesc cu următorul text:

„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."

2. Punctul 10 se modifică după cum urmează:

(a) partea introductivă se înlocuiește cu următorul text:

„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:";

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

„(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."

3. Punctele 19 și 20 se înlocuiesc cu următorul text:

„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."

Cu privire la acest act legislativ a fost formulată o declarație care se regăsește în JO C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.