Parlamentul European
2019-2024

Document de ședință

A9-0307/2023

26.10.2023

***I
RAPORT

referitor la propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Comisia pentru industrie, cercetare și energie

Raportoare: Josianne Cutajar

Legenda simbolurilor utilizate

*	Procedura de consultare
***	Procedura de aprobare
***I	Procedura legislativă ordinară (prima lectură)
***II	Procedura legislativă ordinară (a doua lectură)
***III	Procedura legislativă ordinară (a treia lectură)

(Procedura indicată se bazează pe temeiul juridic propus în proiectul de act.)

Amendamente la un proiect de act

Amendamentele Parlamentului prezentate pe două coloane

Textul eliminat este evidențiat prin caractere ***cursive aldine*** în coloana din stânga. Textul înlocuit este evidențiat prin caractere ***cursive aldine*** în ambele coloane. Textul nou este evidențiat prin caractere ***cursive aldine*** în coloana din dreapta.

În primul și în al doilea rând din antetul fiecărui amendament se identifică fragmentul vizat din proiectul de act supus examinării. În cazul în care un amendament vizează un act existent care urmează să fie modificat prin proiectul de act, antetul conține două rânduri suplimentare în care se indică actul existent și, respectiv, dispoziția din acesta vizată de modificare.

Amendamentele Parlamentului prezentate sub formă de text consolidat

Părțile de text noi sunt evidențiate prin caractere ***cursive aldine***. Părțile de text eliminate sunt indicate prin simbolul ▌ sau sunt tăiate. Înlocuirile sunt semnalate prin evidențierea cu caractere ***cursive aldine*** a textului nou și prin eliminarea sau tăierea textului înlocuit.
Fac excepție de la regulă și nu se evidențiază modificările de natură strict tehnică efectuate de serviciile competente în vederea elaborării textului final.

CUPRINS

Pagina

PROIECT DE REZOLUȚIE LEGISLATIVĂ A PARLAMENTULUI EUROPEAN

referitoare la propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate

(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

(Procedura legislativă ordinară: prima lectură)

Parlamentul European,

– având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2023)0208),

– având în vedere articolul 294 alineatul (2) și articolul 114 din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată de către Comisie (C9-0137/2023),

– având în vedere articolul 294 alineatul (3) din Tratatul privind funcționarea Uniunii Europene,

– având în vedere avizul Comitetului Economic și Social European din 13 iulie 2023[1],

– având în vedere articolul 59 din Regulamentul său de procedură,

– având în vedere scrisoarea Comisiei pentru piața internă și protecția consumatorilor,

– având în vedere raportul Comisiei pentru industrie, cercetare și energie (A9-0307/2023),

1. adoptă poziția sa în primă lectură prezentată în continuare;

2. solicită Comisiei să îl sesizeze din nou în cazul în care își înlocuiește, își modifică în mod substanțial sau intenționează să-și modifice în mod substanțial propunerea;

3. încredințează Președintei sarcina de a transmite Consiliului și Comisiei, precum și parlamentelor naționale poziția Parlamentului.

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

Amendamentul 1

AMENDAMENTELE PARLAMENTULUI EUROPEAN*

la propunerea Comisiei

2023/0108 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

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],

având în vedere avizul Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară[2],

---

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

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

2 ***Poziția Parlamentului European din ... (nepublicată 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.

(1a) 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.

(2) Serviciile de securitate gestionate, care 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, ***inclusiv în detectarea, răspunsul la incidente sau capacitatea de recuperare în urma acestora,*** au dobândit o importanță din ce în ce mai mare în prevenirea și atenuarea incidentelor de securitate cibernetică. ***Activitățile furnizorilor de servicii de securitate gestionate constau în servicii legate de prevenire, identificare, protecție, detectare, analiză, limitare a incidentelor, răspuns și recuperare, inclusiv, dar fără a se limita la furnizarea de informații operative privind amenințările cibernetice, monitorizarea în timp real a amenințărilor prin tehnici proactive, inclusiv securitatea din faza de proiectare, evaluarea riscurilor, detectarea extinsă, remedierea și răspunsul.*** În consecință,

---

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 ... privind ... (JO L, …, ELI: …).

furnizorii acestor servicii sunt considerați entități esențiale sau importante care aparțin unui sector cu o importanță critică ridicată în temeiul Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului[5]. 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.

(3) Furnizorii de servicii de securitate gestionate joacă, de asemenea, un rol important în rezerva pentru securitate cibernetică a UE, a cărei instituire treptată este sprijinită de Regulamentul (UE).../... [de stabilire a unor măsuri de consolidare a solidarității și a capacităților în Uniune de detectare, de pregătire și de răspuns la amenințările și incidentele de securitate cibernetică]. Rezerva UE de securitate cibernetică urmează să fie utilizată pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative și de mare amploare. Regulamentul (UE).../... [de stabilire a unor măsuri de consolidare a solidarității și a capacităților în Uniune de detectare, de pregătire și de răspuns la amenințările și incidentele de securitate cibernetică] stabilește un proces de selecție pentru furnizorii care formează rezerva pentru securitate cibernetică a UE, care ar trebui, printre altele, să ia în considerare dacă furnizorul în cauză a obținut o certificare a securității cibernetice la nivel european sau național. Serviciile relevante furnizate de „furnizorii de încredere” în conformitate cu Regulamentul (UE).../... [de stabilire a unor măsuri de consolidare a solidarității și a capacităților în Uniune de detectare, de pregătire și de răspuns la amenințările și incidentele de securitate cibernetică]

---

[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).

corespund „serviciilor de securitate gestionate” în conformitate cu prezentul regulament.

(4) 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.

(4a) Sistemele europene de certificare pentru serviciile de securitate gestionate ar trebui să conducă la adoptarea acestor servicii și la creșterea concurenței în domeniu, ținând seama atât de nevoile specifice ale furnizorilor, cât și ale beneficiarilor. Prin urmare, aceste sisteme ar trebui să găsească un echilibru între obiectivul lor și eventuala sarcină de reglementare, administrativă și financiară cu care s-ar putea confrunta furnizorii, în special microîntreprinderile sau întreprinderile mici și mijlocii (IMM-uri). În plus, sistemele ar trebui să încurajeze utilizarea serviciilor de securitate gestionate certificate, contribuind 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 o capacitate și resurse limitate, dar care sunt mai expuse la încălcări ale securității cibernetice cu implicații financiare, juridice, de reputație și operaționale.

(4b) Sistemul de certificare al Uniunii pentru serviciile de securitate gestionate ar trebui să asigure disponibilitatea unor servicii securizate și de înaltă calitate care să garanteze o tranziție digitală sigură și să contribuie 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.

(4c) În actualul peisaj digital și tehnologic care evoluează rapid, oferta de resurse educaționale și de cursuri de formare formală este variată, iar cunoștințele pot fi dobândite în diferite moduri, atât formale, de exemplu, prin studii universitare sau cursuri, cât și non-formale, de exemplu prin cursuri de formare la locul de muncă sau prin experiență profesională de lungă durată în domeniul relevant.

(5) 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 unui serviciu de securitate gestionat pot face obiectul unui sistem de certificare ***specific***, este necesar să se modifice Regulamentul (UE) 2019/881. ***Dezvoltarea unor sisteme de certificare instituite în temeiul prezentului regulament ar trebui să țină seama de rezultatele și recomandările evaluării și revizuirii prevăzute în prezentul regulament.***

(5a) Pentru a facilita creșterea unei piețe fiabile a Uniunii, creând în același timp parteneriate cu țări terțe care împărtășesc aceeași viziune, inclusiv în lumina dispozițiilor Regulamentului (UE).../... al Parlamentului European și al Consiliului[6] (2023/0109(COD)) în ceea ce privește accesul la rezerva UE pentru securitate cibernetică, procesul de certificare instituit în cadrul stabilit prin prezentul regulament ar trebui să fie raționalizat pentru a asigura recunoașterea internațională și alinierea la standardele internaționale.

(5b) Pentru a asigura dezvoltarea unei piețe fiabile a Uniunii pentru serviciile de securitate gestionate, furnizorii acestora și statele membre ar trebui să colaboreze și să contribuie la colectarea datelor privind situația și evoluția pieței muncii în materie de securitate cibernetică.

---

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

(5c) O abordare coordonată la nivelul Uniunii pentru consolidarea rezilienței infrastructurii critice se bazează pe consolidarea capacităților statelor membre. Cu toate acestea, 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. 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, cooperarea dintre statele membre, Comisie, ENISA și părțile interesate, inclusiv sectorul privat și mediul academic, ar trebui 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. Aceasta ar facilita deopotrivă mobilitatea profesioniștilor din domeniul securității cibernetice în interiorul Uniunii precum 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. Aceste măsuri ar trebui, de asemenea, să vizeze atragerea unui număr mai mare de femei și fete în domeniu și să contribuie la abordarea disparității de gen în știință, tehnologie, inginerie și matematică. Sectorul privat ar trebui să urmărească, de asemenea, furnizarea de cursuri de formare la locul de muncă care să vizeze competențele cele mai solicitate, implicând administrația publică și întreprinderile nou-înființate, precum și microîntreprinderile și IMM-urile.

(5d) Ar trebui să se asigure finanțare și resurse adecvate pentru sarcinile suplimentare încredințate ENISA prin modificările aduse Regulamentului (UE) 2019/881 introduse prin prezentul regulament.

(5e) Pentru a completa anumite elemente neesențiale ale prezentului regulament, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene ar trebui delegată Comisiei cu scopul de a

prevedea un sistem european de certificare a securității cibernetice pentru produsele TIC, serviciile TIC, procesele TIC și serviciile de securitate gestionate. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, iar respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[7]. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

(5e) 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 și a emis un aviz la [ZZ.LL.AAAA][8],

ADOPTĂ PREZENTUL REGULAMENT:

---

7 JO L 123, 12.5.2016, p. 1

8 ***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 de activități legate de gestionarea riscurilor în materie de securitate cibernetică, inclusiv ***administrarea incidentului***, testele de rezistență la intruziuni, auditurile de securitate și consultanța, sau în furnizarea de asistență sau ***consultanță*** pentru astfel de activități;”;

(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 foarte ridicat 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. ***În acest context, Comisia poate include o evaluare aprofundată a parcursurilor de formare existente pentru a elimina lacunele identificate în materie de competențe și o listă de propuneri pentru abordarea nevoilor de personal calificat și a tipurilor de competențe.***

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

„(7) Pe baza propunerii de sistem pregătite de ENISA, Comisia ***este împuternicită să adopte acte delegate în conformitate cu articolul 65a, completând prezentul regulament prin prevederea de*** 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, 52 și 54***.”;***

(b) se introduce următorul alineat:

„(7a) Înainte de adoptarea unor astfel de acte delegate, Comisia, în cooperare cu ENISA, efectuează și publică o evaluare a impactului sistemului european propus de certificare a securității cibernetice. La pregătirea evaluării impactului, Comisia efectuează consultări publice și consultări cu SCCG și ECCG.";

(8) 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:";

(9) Se introduce următorul articol:

„Articolul 51aObiectivele 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) să asigure că serviciile de securitate gestionate sunt furnizate de personal care are competența, calificările și experiența necesare, inclusiv un nivel foarte ridicat de cunoștințe tehnice și competențe în domeniul specific, experiență suficientă și adecvată și cel mai înalt grad de integritate profesională;

(b) să asigure că furnizorul dispune de proceduri interne adecvate pentru a se asigura că serviciile de securitate gestionate sunt furnizate la un nivel foarte ridicat 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) să asigure 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) să asigure că persoanele, programele sau dispozitivele autorizate pot avea acces numai la datele, serviciile sau funcțiile la care se referă drepturile lor de acces;

(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) să asigure 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 sunt dotate cu software și hardware actualizate*****,** nu conțin vulnerabilități cunoscute și includ cele mai recente actualizări de securitate;*”;*

(10) 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.”;

(11) 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.”;

(12) 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 (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;”***;***

(13) 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 ***interesele și nevoile specifice ale microîntreprinderilor și ale IMM-urilor;”;***

(iii) se adaugă următorul paragraf:

„În ceea ce privește al treilea paragraf litera (d) de la prezentul articol, Comisia asigură un sprijin financiar adecvat în cadrul de reglementare al programelor existente ale Uniunii, în special pentru a reduce sarcina financiară asupra microîntreprinderilor și IMM-urilor, inclusiv asupra întreprinderilor nou-înființate care își desfășoară activitatea în domeniul serviciilor de securitate gestionate.”;

(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.”;

(14) 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 ***delegat*** 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.”;

(15) 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.”;

(16) 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);”;

(16a) se introduce următorul articol:

„Articolul 65a

Exercitarea delegării de competențe

(1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.

(2) Competența de a adopta acte delegate, menționată la articolul 49 alineatul (7), se conferă Comisiei pe o perioadă de cinci ani de la ... [data intrării în vigoare a regulamentului modificat]. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 49 alineatul (7) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în Jurnalul Oficial al Uniunii Europene sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

(4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

(5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

(6) Un act delegat adoptat în temeiul articolului 49 alineatul (7) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecțiuni în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării

termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecțiuni. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.;"

(17) Articolul 67 se înlocuiește cu următorul text:

„Articolul 67

Evaluare și revizuire

(1) Până la 28 iunie 2024 și la fiecare trei ani după aceea, Comisia evaluează impactul, eficacitatea și eficiența activității ENISA și a practicilor sale de lucru, posibila necesitate de a modifica mandatul ENISA și implicațiile financiare ale unei astfel de modificări. Evaluarea ține seama de orice punct de vedere comunicat către ENISA ca răspuns la activitățile sale. În cazul în care Comisia consideră că nu se mai justifică continuarea activității ENISA în raport cu obiectivele, mandatul și atribuțiile încredințate acesteia, Comisia poate propune modificarea prezentului regulament în ceea ce privește dispozițiile referitoare la ENISA.

(2) Evaluarea analizează impactul, eficacitatea și eficiența dispozițiilor din titlul III din prezentul regulament 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, de asemenea:

(a) eficiența și eficacitatea procedurilor care conduc la consultarea, pregătirea și adoptarea sistemelor europene de certificare de securitate cibernetică, precum și modalitățile de îmbunătățire și accelerare a acestor proceduri;

(b) 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.

(4) Până la 28 iunie 2024 și, ulterior, din trei în trei ani, Comisia trimite raportul de evaluare împreună cu concluziile sale Parlamentului European, Consiliului și consiliului de administrație. Concluziile raportului respectiv sunt făcute publice.”.

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*

EXPUNERE DE MOTIVE

Raportoarea sprijină propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate, înțelegând necesitatea ca acesta să actualizeze și să consolideze sistemul european de certificare a securității cibernetice, permițându-i să acopere servicii industriale importante și aflate în extindere. Având în vedere modul în care statele membre au început deja să adopte sisteme de certificare pentru serviciile de securitate gestionate, raportoarea consideră că această modificare a Regulamentului privind securitatea cibernetică este esențială pentru a preveni divergențe semnificative între sistemele naționale, ce ar duce la o formă de fragmentare a pieței care contravine intereselor economice și strategice ale Uniunii.

În această privință, se recunoaște modul în care prezenta propunere este concepută pentru a completa Regulamentul privind solidaritatea cibernetică. În special această extindere specifică a sistemului european de certificare a securității cibernetice va permite serviciilor de securitate gestionate – care corespund „furnizorilor de încredere” din Regulamentul privind solidaritatea cibernetică – să joace un rol important în viitoarea rezervă a UE pentru securitate cibernetică. Prin urmare, prezenta propunere este, de asemenea, foarte importantă pentru promovarea unei capacități mai ample a Uniunii în materie de securitate cibernetică, capacitate esențială pentru contracararea amenințărilor potențiale într-o realitate geopolitică în continuă evoluție.

În limitele propunerii Comisiei, obiectivul raportoarei este de a consolida și de a clarifica și mai mult această modificare specifică a Regulamentului privind securitatea cibernetică. Acest lucru este ilustrat de modificările aduse de raportoare definiției serviciilor de securitate gestionate, clarificând faptul că acestea sunt „externalizate”, detaliind, în același timp, elementele care pot fi incluse în definiție. Amendamentele depuse cu privire la recunoașterea standardelor internaționale de securitate cibernetică sunt menite să promoveze un nivel mai ridicat de încredere, elaborând în același timp norme cuprinzătoare ale UE.

Prezentul proiect de raport pune un accent mai puternic pe abordarea lacunelor în materie de competențe și pe sprijinirea microîntreprinderilor și a întreprinderilor mici și mijlocii. În ceea ce privește cele dintâi, amendamentele depuse se bazează pe necesitatea deja implicită a

competențelor în sistemul de certificare cibernetică în ceea ce privește „competențele, expertiza și experiența necesare pentru personalul cu un nivel foarte ridicat de cunoștințe tehnice relevante și de integritate profesională”. În opinia raportoarei, deși promovează cooperarea între toți actorii implicați, precum și între statele membre, sectorul privat, mediul academic și instituțiile de cercetare, sistemul european de certificare trebuie să acționeze ca un catalizator al unei noi foi de parcurs pentru formarea și capacitarea forței de muncă, colectând mai multe date privind competențele necesare și contribuind la abordarea disparității de gen în domeniul STIM.

În același timp, microîntreprinderile și întreprinderile mici și mijlocii, care constituie coloana vertebrală a economiei europene și au cu siguranță un rol pozitiv în sectorul securității cibernetice, ar trebui să beneficieze de sprijin financiar adecvat în cadrul de reglementare al programelor existente ale Uniunii, pentru a reduce orice sarcină financiară disproporționată care le revine.

21.9.2023

SCRISOAREA COMISIEI PENTRU PIAȚA INTERNĂ ȘI PROTECȚIA CONSUMATORILOR

Domnului Cristian Silviu Buşoi
Președinte
Comisia pentru industrie, cercetare și energie
BRUXELLES

Subiect: Aviz referitor la propunerea de regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Domnule Președinte,

În cadrul procedurii menționate în subiect, Comisia pentru piața internă și protecția consumatorilor a fost solicitată pentru a transmite un aviz comisiei dumneavoastră. În cursul reuniunii din 23 mai 2023, s-a decis ca acest aviz să fie transmis sub formă de scrisoare. Chestiunea în cauză a fost examinată în cadrul reuniunii sale din 19 septembrie 2023, avizul fiind adoptat în cadrul aceleiași reuniuni.

În cadrul acestei reuniuni[1], a decis să recomande Comisiei pentru industrie, cercetare și energie (ITRE), care este comisie competentă, includerea următoarelor sugestii în raportul său legislativ.

Vă asigur, Domnule Președinte, de înalta mea considerație.

Anna Cavazzini

SUGESTII

Comisia pentru piața internă și protecția consumatorilor recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele sugestii:

A. întrucât, la 18 aprilie 2023, Comisia a publicat o propunere legislativă privind serviciile de securitate gestionate, care implică modificări specifice ale Regulamentului UE privind

[1] La votul final au fost prezenți: Anna Cavazzini (președintă), Andrus Ansip (vicepreședinte), Krzysztof Hetman (vicepreședinte), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoș, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

securitatea cibernetică[2];

B. întrucât, în ceea ce privește propunerea legislativă referitoare la Regulamentul UE privind securitatea cibernetică (2017/0225 (COD))[3], Comisia pentru piața internă și protecția consumatorilor (IMCO) a prezentat un aviz în temeiul fostului articol 54 din Regulamentul de procedură Comisiei pentru industrie, cercetare și energie (ITRE), cu competențe partajate privind cadrul de certificare a securității cibernetice, având în vedere competența clară a Comisiei IMCO în ceea ce privește sistemele de certificare și, în general, standardizarea, supravegherea pieței și punerea în aplicare a pieței unice digitale;

C. întrucât Regulamentul UE privind securitatea cibernetică[4] urmărește să atingă 1) un nivel ridicat de securitate cibernetică, reziliență cibernetică și încredere în UE prin stabilirea de obiective, sarcini și aspecte organizatorice pentru o Agenție a Uniunii Europene pentru Securitate Cibernetică (ENISA) consolidată și redenumită, cu un nou mandat permanent, și 2) un cadru pentru sistemele europene voluntare de certificare a securității cibernetice pentru produsele, serviciile și procesele din domeniul tehnologiei informației și comunicațiilor (TIC);

D. date fiind modificările specifice propuse pentru a include serviciile de securitate gestionate în domeniul de aplicare al Regulamentului UE privind securitatea cibernetică și pentru a adăuga o definiție a acestor servicii care este strâns aliniată la definiția din Directiva NIS 2[5]; întrucât modificările ar permite Comisiei, prin intermediul unor acte de punere în aplicare, adoptarea unor sisteme europene de certificare a securității cibernetice pentru serviciile de securitate gestionate, pe lângă produsele, serviciile și procesele din domeniul TIC, care sunt deja reglementate de Regulamentul UE privind securitatea cibernetică;

E. întrucât serviciile de securitate gestionate joacă un rol din ce în ce mai important în prevenirea și atenuarea incidentelor de securitate cibernetică,

1. recunoaște că la 23 mai 2022[6] Consiliul a solicitat o creștere a nivelului general de securitate cibernetică în UE prin facilitarea apariției și dezvoltării unor furnizori de încredere de servicii de securitate cibernetică; consideră că, printre altele, războiul din Ucraina, contextul geopolitic actual și amenințările continue din partea regimurilor țărilor terțe, precum și o piață în continuă creștere a tehnologiilor digitale și transformarea digitală a proceselor în general au condus la necesitatea unui nivel mai ridicat de securitate cibernetică în UE și în statele sale membre; recomandă Comisiei să ia măsuri proactive pentru a sprijini dezvoltarea unor furnizori de încredere de servicii de securitate cibernetică, cum ar fi finanțarea pentru cercetare și dezvoltare, programe de formare pentru consolidarea competențelor în materie de securitate cibernetică și stimulente pentru ca întreprinderile să investească în securitatea cibernetică; sugerează că UE ar trebui să își consolideze cooperarea cu NATO și cu alți parteneri internaționali pentru a răspunde amenințărilor cibernetice din partea regimurilor țărilor terțe, inclusiv schimbul de informații privind amenințările, exerciții comune și răspunsuri coordonate la atacurile

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52023PC0208
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)
[4] JO L 151, 7.6.2019, p. 15
[5] JO L 333/810, 27.12.2022
[6] 9364/22

cibernetice;

2. subliniază că certificarea serviciilor de securitate gestionate, bazată pe norme nediscriminatorii și care reflectă standardele europene și internaționale, este esențială pentru consolidarea și garantarea încrederii în calitatea acestor servicii, în special cu scopul de a atinge un nivel ridicat de protecție a consumatorilor; ia act de faptul că unele state membre au adoptat deja sisteme de certificare pentru serviciile de securitate gestionate și că, prin urmare, este esențial să se evite fragmentarea pieței interne și inconsecvențele, care pot afecta sectorul și întreprinderile din domeniul securității cibernetice, și să se permită o abordare armonizată prin crearea unui sistem european de certificare a securității cibernetice pentru astfel de servicii; solicită ca cadrul de certificare a securității cibernetice să includă cele mai bune practici din sistemele naționale de certificare existente și să fie elaborat în consultare cu principalele părți interesate din sectorul securității cibernetice;

3. subliniază că 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 important în sprijinirea entităților în eforturile lor de a preveni și de a detecta incidente cibernetice, de a răspunde la acestea și de a se redresa după ele; consideră că, întrucât din ce în ce mai multe întreprinderi întâmpină dificultăți în a menține diverse sisteme informatice complexe și rețele corporative interconectate, acestea se bazează în mod necesar pe furnizori de servicii de securitate gestionate și, prin urmare, acești furnizori ar trebui să fie considerați un element esențial în ecosistemul de securitate cibernetică al UE; observă, totuși, că furnizorii de servicii de securitate gestionate au fost și ei ținta atacurilor cibernetice și pot prezenta un risc deosebit din cauza integrării lor strânse în operațiunile clienților lor;

4. reamintește importanța Directivei NIS 2, recent adoptată, pentru a asigura un nivel mai ridicat de reziliență cibernetică în întreaga Uniune; solicită adoptarea și punerea în aplicare rapidă a actelor de punere în aplicare în temeiul prezentei directive pentru a se asigura că furnizorii de servicii de securitate gestionate respectă cerințele directivei privind măsurile de gestionare a riscurilor în materie de securitate cibernetică;

5. recomandă ca furnizorii de servicii de securitate gestionate să aibă obligația de a respecta standardele de securitate cibernetică relevante și de a face obiectul unor revizuiri periodice pentru a se asigura că sistemele lor sunt sigure pentru a proteja nu numai furnizorii înșiși, ci și entitățile pe care le deservesc; consideră că astfel de revizuiri ar trebui să evalueze respectarea de către furnizori a cadrului de certificare a securității cibernetice la nivelul UE și capacitatea acestora de a-și proteja atât sistemele, cât și pe cele ale clienților lor împotriva amenințărilor cibernetice;

6. salută propunerea legislativă privind serviciile de securitate gestionate, care vizează îmbunătățirea calității serviciilor de securitate gestionate și creșterea comparabilității acestora în beneficiul bunei funcționări a pieței interne și al punerii în aplicare a pieței unice digitale; subliniază că certificarea serviciilor de securitate gestionate este relevantă în procesul de selecție pentru rezerva pentru securitate cibernetică a UE, și este și un indicator de calitate și de încredere semnificativ pentru entitățile private și publice care intenționează să achiziționeze astfel de servicii;

7. ia act de faptul că propunerea consolidează rolul ENISA, care ar trebui să sprijine și să promoveze dezvoltarea și punerea în aplicare a politicii Uniunii privind certificarea securității cibernetice a produselor, serviciilor, proceselor și serviciilor de securitate gestionate din domeniul TIC, prin monitorizarea periodică a evoluțiilor din domeniile conexe de standardizare și prin recomandarea de specificații tehnice, în cazul în care standardele nu sunt disponibile; sugerează că ENISA ar trebui să primească resurse și autoritate suplimentare pentru a-și îndeplini rolul extins, inclusiv finanțarea pentru cercetare și dezvoltare, precum și un mandat clar de coordonare cu agențiile naționale de securitate cibernetică și cu părțile interesate din industrie; subliniază rolul esențial al echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) în crearea unui spațiu digital previzibil și sigur pentru întreprinderi și cetățeni;

8. invită Comisia și ENISA să sprijine și să asigure punerea în aplicare coerentă a sistemului european de certificare a securității cibernetice bazat pe norme nediscriminatorii și care să reflecte standardele europene și internaționale pentru autoevaluarea conformității de către producătorul sau furnizorul de produse, servicii, procese sau servicii de securitate gestionate din domeniul TIC, în conformitate cu Regulamentul UE privind securitatea cibernetică; consideră că punerea în aplicare ar trebui să contribuie la compensarea costurilor de acreditare și să încurajeze mai mulți producători sau furnizori să participe la sistem;

9. subliniază că fiecare sistem de certificare ar trebui să fie conceput în așa fel încât să stimuleze și să încurajeze toți actorii implicați în sectorul în cauză să elaboreze și să adopte standarde de securitate, norme tehnice și principii de securitate de la stadiul conceperii și de protejare a vieții private din faza de proiectare în toate etapele ciclului de viață al produsului sau al serviciului, care să fie actualizate periodic; subliniază că contribuțiile societății civile, ale cercetătorilor independenți din domeniul securității și ale părților interesate relevante trebuie să fie luate în considerare într-un mod mai sistematic atunci când se elaborează astfel de principii; consideră că sistemele de certificare ar trebui să fie coerente cu alte sisteme europene de certificare a securității cibernetice adoptate în conformitate cu Regulamentul UE privind securitatea cibernetică și ar trebui să evite sarcina disproporționată asupra furnizorilor; recomandă ca sistemele de certificare să includă orientări clare și detaliate cu privire la modul de punere în aplicare a principiilor de securitate de la stadiul conceperii și de protejare a vieții private începând cu momentul conceperii, în cazul în care aceste orientări sunt în conformitate cu dispozițiile care stabilesc cadrul pentru sistemele europene de securitate cibernetică din Regulamentul UE privind securitatea cibernetică; sugerează că, atunci când este necesar și proporțional, sistemele de certificare ar trebui să constea într-un mecanism de îmbunătățire continuă, cum ar fi revizuiri și actualizări periodice ale standardelor de securitate și ale normelor tehnice; consideră că mecanismul ar trebui să țină seama de cele mai recente evoluții în ceea ce privește amenințările și tehnologiile în materie de securitate cibernetică; solicită ca fiecare sistem de certificare să includă măsuri de promovare a transparenței și a responsabilității, cum ar fi publicarea rezultatelor certificării și sancțiuni pentru neconformitate;

10. solicită introducerea unei mărci de siguranță voluntare a UE pentru produsele, serviciile, procesele și serviciile de securitate gestionate din domeniul TIC certificate; subliniază, în acest sens, că eticheta ar putea contribui la creșterea gradului de conștientizare cu privire la securitatea cibernetică pe piața internă și ar putea oferi un avantaj competitiv

întreprinderilor cu competențe și experiență remarcabile în materie de securitate cibernetică; sugerează ca marca de siguranță a UE să fie concepută astfel încât să fie ușor de recunoscut și de înțeles de către consumatori și întreprinderi;

11. recomandă Comisiei și ENISA să instituie un program specific de cercetare și dezvoltare pentru securitatea cibernetică; recomandă Comisiei și ENISA să instituie un cadru de evaluare a riscurilor în materie de securitate cibernetică pentru întreprinderi, care să conțină orientări privind modul de identificare, evaluare și atenuare a riscurilor de securitate cibernetică și care ar putea fi adaptat la diferite sectoare și dimensiuni ale întreprinderilor; sugerează că Comisia și ENISA ar trebui să ofere ajutor și asistență statelor membre pentru a institui un mecanism de raportare a incidentelor de securitate cibernetică pentru consumatori și întreprinderi, pentru a facilita colectarea de date privind incidentele de securitate cibernetică, care ar putea fi utilizate pentru a îmbunătăți politicile și practicile în materie de securitate cibernetică.

PROCEDURA COMISIEI COMPETENTE

Titlu	Modificarea Regulamentului (UE) 2019/881 în ceea ce privește serviciile de securitate gestionate
Referințe	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Data prezentării în PE	19.4.2023
Comisie competentă Data anunțului în plen	ITRE 1.6.2023
Comisii sesizate pentru aviz Data anunțului în plen	IMCO LIBE 1.6.2023 1.6.2023
Avize care nu au fost emise Data deciziei	LIBE 30.5.2023
Raportoare Data numirii	Josianne Cutajar 2.5.2023
Examinare în comisie	19.7.2023 19.9.2023
Data adoptării	25.10.2023
Rezultatul votului final	+: 57 –: 0 0: 2
Membri titulari prezenți la votul final	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Membri supleanți prezenți la votul final	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Data depunerii	26.10.2023

VOT FINAL PRIN APEL NOMINAL ÎN COMISIA COMPETENTĂ

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri