Parlamentul European
2019-2024

Document de ședință

A9-0253/2023

26.7.2023

***I
RAPORT

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Comisia pentru industrie, cercetare și energie

Raportor: Nicola Danti

Raportor pentru avizul comisiilor asociate, în temeiul articolului 57 din Regulamentul de procedură:
Morten Løkkegaard, Comisia pentru piața internă și protecția consumatorilor

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 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

(Procedura legislativă ordinară: prima lectură)

Parlamentul European,

– având în vedere propunerea Comisiei prezentată Parlamentului European și Consiliului (COM(2022)0454),

– având în vedere articolul 294 alineatul (2) și articolul 114 din Tratatul privind funcționarea Uniunii Europene, în temeiul cărora propunerea a fost prezentată Parlamentului de către Comisie (C9-0308/2022),

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

– având în vedere avizul Comitetului Economic și Social European din 14 decembrie 2022[1],

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

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

– având în vedere raportul Comisiei pentru industrie, cercetare și energie (A9-0253/2023),

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

2. solicită Comisiei să modifice fișa financiară care însoțește propunerea prin majorarea schemei de personal a Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) cu 9,0 posturi suplimentare cu normă întreagă și prin furnizarea de credite suplimentare corespunzătoare pentru a se asigura că obligațiile ENISA în temeiul prezentului regulament pot fi îndeplinite și pentru a nu compromite obligațiile existente ale agenției în temeiul altor acte legislative ale Uniunii;

3. 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;

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

[1] JO C 100, 16.3.2023, p. 101.

Amendamentul 1

AMENDAMENTELE PARLAMENTULUI EUROPEAN*

la propunerea Comisiei

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020 *și a Directivei 2020/1828/CE (Actul privind reziliența cibernetică)*

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[2],

având în vedere avizul Comitetului Regiunilor[3],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) ***Securitatea cibernetică este una dintre principalele provocări pentru Uniune, iar numărul și varietatea dispozitivelor conectate vor crește exponențial în următorii ani. Atacurile cibernetice reprezintă o chestiune de interes public, deoarece au un impact critic nu numai asupra economiei Uniunii, ci și asupra democrației, precum***

---

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

2 JO C ***100***, ***16.3.2023***, p. ***101.***

3 JO C , , p. .

și asupra siguranței și sănătății consumatorilor. Este necesar***, prin urmare,*** să ***se întărească abordarea Uniunii în materie de securitate cibernetică, să se abordeze reziliența cibernetică la nivelul Uniunii și*** să se îmbunătățească funcționarea pieței interne prin stabilirea unui cadru juridic uniform pentru cerințele esențiale de securitate cibernetică pentru introducerea produselor cu elemente digitale pe piața Uniunii. Ar trebui abordate două probleme majore care generează costuri suplimentare pentru utilizatori și pentru societate: nivelul scăzut de securitate cibernetică a produselor cu elemente digitale, care se reflectă în răspândirea pe scară largă a vulnerabilităților și în furnizarea insuficientă și inconsecventă de actualizări de securitate pentru abordarea acestora, și accesul insuficient și înțelegerea insuficientă a informațiilor din partea utilizatorilor, ceea ce îi împiedică să aleagă produse cu caracteristici adecvate de securitate cibernetică sau să le utilizeze în mod securizat.

(2) Prezentul regulament are ca scop stabilirea condițiilor-limită pentru dezvoltarea de produse cu elemente digitale care să fie sigure prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu mai puține vulnerabilități și că producătorii tratează cu seriozitate securitatea pe parcursul întregului ciclu de viață al unui produs. De asemenea, prezentul regulament vizează crearea unor condiții care să le permită utilizatorilor să ia în considerare securitatea cibernetică atunci când selectează și utilizează produse cu elemente digitale***, de exemplu prin îmbunătățirea transparenței în ceea ce privește perioada de sprijinire a produselor introduse pe piață***.

(3) Legislația relevantă a Uniunii aflată în prezent în vigoare cuprinde mai multe seturi de norme orizontale care abordează anumite aspecte legate de securitatea cibernetică din diferite perspective, incluzând măsuri de îmbunătățire a securității lanțului de aprovizionare digital. Cu toate acestea, legislația existentă a Uniunii referitoare la securitatea cibernetică, inclusiv Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[4] ***și Directiva (UE) 2022/2555 a Parlamentului European***

[4] 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).

și a Consiliului[5], nu cuprinde în mod direct cerințele obligatorii de securitate a produselor cu elemente digitale.

(4) Deși legislația existentă a Uniunii se aplică anumitor produse cu elemente digitale, nu există un cadru de reglementare orizontal al Uniunii care să stabilească cerințe cuprinzătoare de securitate cibernetică pentru toate produsele cu elemente digitale. Diferitele acte și inițiative adoptate până în prezent la nivelul Uniunii și la nivel național abordează doar parțial problemele și riscurile identificate legate de securitatea cibernetică, creând un mozaic legislativ în cadrul pieței interne, sporind insecuritatea juridică atât pentru producătorii, cât și pentru utilizatorii acestor produse și adăugând o sarcină inutilă ***întreprinderilor și organizațiilor*** pentru respectarea unor cerințe pentru tipuri similare de produse. Securitatea cibernetică a acestor produse are o dimensiune transfrontalieră deosebit de puternică, deoarece produsele fabricate într-o țară sunt adesea utilizate de organizații și de consumatori din întreaga piață internă. Acest lucru face necesară reglementarea domeniului la nivelul Uniunii***, pentru a asigura un cadru de reglementare armonizat și clar pentru întreprinderi, în special pentru microîntreprinderi și întreprinderile mici și mijlocii***. Cadrul de reglementare al Uniunii ar trebui armonizat prin introducerea unor cerințe de securitate cibernetică pentru produsele cu elemente digitale. În plus, ar trebui să se asigure securitate juridică pentru operatori și utilizatori în întreaga Uniune, precum și o mai bună armonizare a pieței unice ***și proporționalitatea pentru microîntreprinderi și întreprinderile mici și mijlocii,*** creând astfel condiții mai viabile pentru operatorii ***economici*** care doresc să intre pe piața Uniunii.

(4a) Caracterul orizontal al prezentului regulament înseamnă că acesta va avea un impact asupra unor segmente foarte diferite ale economiei Uniunii. Prin urmare, este important ca particularitățile fiecărui sector să fie luate în considerare și ca cerințele de securitate cibernetică prevăzute în prezentul regulament să fie proporționale cu riscurile. Prin urmare, Comisia ar trebui să emită orientări care să explice în mod clar și detaliat modul de aplicare a prezentului regulament.

---

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).

Orientările ar trebui să cuprindă, printre altele, o explicație detaliată a domeniului de aplicare, în special a noțiunii de prelucrare a datelor la distanță și a implicațiilor pentru dezvoltatorii de software liber și cu sursă deschisă, criteriile utilizate pentru a stabili modul în care sunt clasificate produsele esențiale cu elemente digitale și interacțiunea dintre prezentul regulament și alte acte legislative ale Uniunii.

(4b) O întreprindere care își desfășoară activitatea online poate oferi o varietate de servicii diferite. În funcție de natura serviciilor prestate, aceeași entitate se poate încadra în mai multe categorii diferite de operatori economici. În cazul în care o entitate prestează servicii de intermediere online pentru un produs cu elemente digitale și este un prestator pe o piață online, astfel cum este definită la articolul 3 alineatul (14) din Regulamentul (UE) 2023/988 al Parlamentului European și al Consiliului[6], aceasta nu se califică drept operator economic, astfel cum este definit în prezentul regulament. În cazul în care aceeași entitate este un prestator pe o piață online și acționează în calitate de operator economic, astfel cum este definit în prezentul regulament, pentru vânzarea de produse cu elemente digitale, aceasta ar trebui să facă obiectul domeniului de aplicare al prezentului regulament în ceea ce privește astfel de produse. Dispozițiile Regulamentului (UE) 2023/988 sunt pe deplin aplicabile prezentului regulament. Având în vedere rolul proeminent pe care îl au piețele online în facilitarea comerțului electronic, acestea ar trebui să depună eforturi pentru a coopera cu autoritățile de supraveghere a pieței din statele membre pentru a se asigura că produsele achiziționate prin intermediul piețelor online respectă cerințele de securitate cibernetică prevăzute în prezentul regulament.

(5) La nivelul Uniunii, diverse documente programatice și politice, cum ar fi Strategia de securitate cibernetică a UE pentru deceniul digital[7], Concluziile Consiliului din 2 decembrie 2020 și din 23 mai 2022 sau Rezoluția Parlamentului European din

---

6 ***Regulamentul (UE) 2023/988 al Parlamentului European și al Consiliului din 10 mai 2023 privind siguranța generală a produselor, de modificare a Regulamentului (UE) nr. 1025/2012 al Parlamentului European și al Consiliului și a Directivei (UE) 2020/1828 a Parlamentului European și a Consiliului și de abrogare a Directivei 2001/95/CE a Parlamentului European și a Consiliului și a Directivei 87/357/CEE a Consiliului (JO L 135, 23.5.2023, p. 1).***

7 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=JOIN:2020:18:FIN.

10 iunie 2021[8], au solicitat cerințe specifice de securitate cibernetică ale Uniunii pentru produsele digitale sau conectate, mai multe țări din întreaga lume introducând măsuri pentru a aborda această chestiune din proprie inițiativă. În raportul final al Conferinței privind viitorul Europei[9], cetățenii au solicitat „un rol mai important al UE în contracararea amenințărilor la adresa securității cibernetice”. ***Pentru ca Uniunea să joace un rol de lider la nivel internațional în domeniul securității cibernetice, este important să se stabilească un cadru de reglementare cuprinzător ambițios.***

(6) Pentru a crește nivelul general de securitate cibernetică a tuturor produselor cu elemente digitale introduse pe piața internă, este necesar să se introducă cerințe esențiale de securitate cibernetică orientate către obiective și neutre din punct de vedere tehnologic pentru aceste produse, care să se aplice orizontal.

(7) În anumite condiții, toate produsele cu elemente digitale integrate într-un sistem electronic de informații mai mare sau conectate la un astfel de sistem pot servi drept vector de atac pentru actorii rău-intenționați. În consecință, chiar și hardware-ul și software-ul considerate mai puțin critice pot facilita compromiterea inițială a unui dispozitiv sau a unei rețele, permițând actorilor rău-intenționați să obțină un acces privilegiat la un sistem sau să se deplaseze lateral între sisteme. Prin urmare, producătorii ar trebui să se asigure că toate produsele conectabile cu elemente digitale sunt proiectate și dezvoltate în conformitate cu cerințele esențiale prevăzute în prezentul regulament. Sunt incluse atât produsele care pot fi conectate fizic prin interfețe hardware, cât și produsele care sunt conectate logic, de exemplu prin intermediul unor prize de rețea, canale, fișiere, interfețe de programare a aplicațiilor sau orice alt tip de interfață software. Întrucât amenințările la adresa securității cibernetice se pot propaga prin diverse produse cu elemente digitale înainte de a atinge un anumit obiectiv, de exemplu prin înlănțuirea mai multor exploatări de

---

8 2021/2568 (RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_RO.html.

9 *Conferința privind viitorul Europei – Raportul privind rezultatul final*, mai 2022, propunerea 28 punctul 2. Conferința s-a desfășurat în perioada aprilie 2021-mai 2022. Aceasta a reprezentat un exercițiu unic, condus de cetățeni, de democrație deliberativă la nivel paneuropean, la care au participat mii de cetățeni europeni, precum și actori politici, parteneri sociali, reprezentanți ai societății civile și principalele părți interesate.

vulnerabilități, producătorii ar trebui să asigure, de asemenea, securitatea cibernetică a produselor care sunt conectate doar indirect la alte dispozitive sau rețele.

(8) Prin stabilirea unor cerințe de securitate cibernetică pentru introducerea pe piață a produselor cu elemente digitale, securitatea cibernetică a acestor produse va fi îmbunătățită atât pentru consumatori, cât și pentru întreprinderi. Sunt incluse, de asemenea, cerințe privind introducerea pe piață a produselor de consum cu elemente digitale destinate consumatorilor vulnerabili, cum ar fi jucăriile și monitoarele pentru sugari. ***Aceste cerințe vor asigura, de asemenea, că securitatea cibernetică este luată în considerare de-a lungul lanțurilor de aprovizionare, îmbunătățind siguranța produselor finale cu elemente digitale. Acest lucru va reprezenta, la rândul său, un avantaj competitiv pentru producătorii stabiliți sau reprezentați în Uniune, care vor putea face publicitate pentru securitatea cibernetică a produselor lor.***

(9) Prezentul regulament asigură un nivel ridicat de securitate cibernetică a produselor cu elemente digitale ***și a soluțiilor integrate de prelucrare a datelor la distanță ale acestora***. ***Astfel de*** soluții de procesare a datelor la distanță referitoare la un produs cu elemente digitale ***sunt definite*** ca fiind orice procesare de date la distanță pentru care software-ul este conceput și dezvoltat de către ***sau în numele*** producătorului produsului în cauză ▌ și a cărui absență ar împiedica un astfel de produs cu elemente digitale să își îndeplinească una dintre funcțiile sale. ***De exemplu, funcționalitățile activate în cloud furnizate de producătorul dispozitivelor inteligente pentru casă care permit utilizatorilor să controleze dispozitivul de la distanță ar trebui să intre în domeniul de aplicare al prezentului regulament. Pe de altă parte, site-urile care nu sunt legate în mod indisolubil de un produs cu elemente digitale sau servicii de cloud în afara responsabilității producătorului nu ar trebui să fie considerate soluții de prelucrare a datelor la distanță în temeiul prezentului regulament. Directiva (UE) 2022/2555*** instituie cerințe de raportare a securității cibernetice și a incidentelor pentru entitățile esențiale și importante, cum ar fi infrastructura critică, în vederea creșterii rezilienței serviciilor pe care le furnizează. ***Deși Directiva (UE) 2022/2555*** se aplică serviciilor de cloud computing și modelelor de servicii de cloud, ***iar prezentul regulament nu se aplică serviciilor precum software-ul ca serviciu (SaaS), platforma ca serviciu (PaaS) sau infrastructura ca serviciu (IaaS), acestea pot intra în***

domeniul de aplicare al prezentului regulament în măsura în care corespund definiției soluțiilor de prelucrare a datelor la distanță. ▌

(9a) Software-ul și datele care sunt partajate în mod deschis și pe care utilizatorii le pot accesa, utiliza, modifica și redistribui în mod liber sau versiunile modificate ale acestora pot contribui la cercetarea și inovarea pe piață. De asemenea, studii ale Comisiei Europene[10] arată că software-ul liber și cu sursă deschisă poate avea o contribuție cifrată între 65 și 95 de miliarde EUR la PIB-ul Uniunii și poate oferi posibilități de creștere semnificative pentru economia acesteia. Utilizatorilor li se permite să ruleze, să copieze, să distribuie, să studieze, să modifice și să îmbunătățească software-ul și datele, inclusiv modelele, prin licențe libere și cu sursă deschisă. Pentru a încuraja dezvoltarea și implementarea de software liber și cu sursă deschisă, în special de către microîntreprinderi și întreprinderile mici și mijlocii, inclusiv întreprinderile nou-înființate, organizațiile non-profit, cercetarea universitară și persoanele fizice, prezentul regulament ar trebui să se aplice produselor software gratuite și cu sursă deschisă în cazuri specifice, pentru a ține seama de faptul că există diferite modele de dezvoltare a software-ului distribuit și dezvoltat în temeiul licențelor publice.

(10) ***Numai*** software-ul liber și cu sursă deschisă pus la dispoziție pe piață în cursul unei activități comerciale ar trebui ▌ să intre sub incidența prezentului regulament. ▌ ***Dacă un produs liber și cu sursă deschisă a fost pus la dispoziție ca parte a unei activități comerciale ar trebui să fie evaluat pentru fiecare produs în parte, analizând atât modelul de dezvoltare, cât și etapa de furnizare a produsului liber și cu sursă deschisă cu elemente digitale.***

(10a) De exemplu, un model de dezvoltare complet descentralizat, în care nicio entitate comercială nu exercită controlul asupra a ceea ce este acceptat în baza de coduri a proiectului, ar trebui să fie considerat o indicație a faptului că produsul a fost dezvoltat într-un cadru necomercial. Pe de altă parte, în cazul în care software-ul liber și cu sursă deschisă este dezvoltat de o singură organizație sau de o comunitate asimetrică, în cazul în care o singură organizație generează venituri din utilizarea

---

10 Impactul software-ului și hardware-ului cu sursă deschisă asupra independenței tehnologice, competitivității și inovării în economia UE", Comisia Europeană, 6 septembrie 2021 https://ec.europa.eu/newsroom/dae/redirection/document/79021

acestuia în cadrul unor relații de afaceri, acest lucru ar trebui să fie considerat ca fiind o activitate comercială. În mod similar, în cazul în care principalii contribuitori la proiectele gratuite și cu sursă deschisă sunt dezvoltatori angajați de entități comerciale și atunci când acești dezvoltatori sau angajatorul pot exercita controlul asupra modificărilor acceptate în baza de coduri, proiectul ar trebui, în general, să fie considerat a fi de natură comercială.

(10b) ***În ceea ce privește etapa de furnizare, în*** contextul software-ului liber și cu sursă deschisă, o activitate comercială ar putea fi caracterizată nu numai prin perceperea unui preț pentru un produs, ci și prin perceperea unui preț pentru serviciile de asistență tehnică, ***atunci când acestea nu servesc numai la recuperarea costurilor reale,*** prin furnizarea unei platforme software prin care producătorul își monetizează alte servicii sau prin utilizarea datelor cu caracter personal din alte motive decât exclusiv pentru îmbunătățirea securității, compatibilității sau interoperabilității software-ului. ***Acceptarea de donații fără intenția de a realiza un profit nu ar trebui considerată o activitate comercială, cu excepția cazului în care astfel de donații sunt făcute de entități comerciale și au un caracter recurent.***

(10c) ***Dezvoltatorii care contribuie individual la proiecte libere și cu sursă deschisă nu ar trebui să facă obiectul obligațiilor prevăzute în prezentul regulament.***

(10d) ***Simplul act de a găzdui software liber și cu sursă deschisă în arhive deschise nu constituie în sine punerea la dispoziție pe piață a unui produs cu elemente digitale. Ca atare, majoritatea gestionarilor de pachete, a platformelor de găzduire a codurilor și a platformelor de colaborare nu ar trebui să fie considerați distribuitori în sensul prezentului regulament.***

(10e) ***Pentru a se asigura că produsele sunt proiectate, dezvoltate și produse în concordanță cu cerințele esențiale prevăzute în anexa I secțiunea 1, producătorii ar trebui să exercite diligența necesară atunci când integrează componente provenite de la terți, inclusiv în cazul software-ului liber și cu sursă deschisă care nu a fost pus la dispoziție pe piață. Nivelul adecvat de diligență necesară depinde de natura și de nivelul de risc al componentei și poate include una sau mai multe dintre următoarele acțiuni: verificarea faptului dacă componenta poartă deja marcajul CE, verificarea istoricului actualizărilor de securitate, verificarea faptului că aceasta nu prezintă vulnerabilități înregistrate în baza de date europeană a***

vulnerabilităților sau în alte baze de date publice sau efectuarea de teste de securitate suplimentare. În cazul în care, în exercitarea diligenței necesare, producătorul produsului identifică o vulnerabilitate a unei componente, inclusiv a unei componente libere și cu sursă deschisă, acesta ar trebui să informeze dezvoltatorul componentei, să abordeze și să remedieze vulnerabilitatea și, după caz, să furnizeze dezvoltatorului soluția de securitate aplicată. Odată ce producătorul a introdus produsul pe piață, acesta ar trebui să fie responsabil de asigurarea faptului că vulnerabilitățile sunt gestionate pe parcursul întregii perioade de sprijin, inclusiv pentru componentele libere și cu sursă deschisă integrate în produsul cu elemente digitale.

(10f) Lipsa competențelor profesionale în domeniul securității cibernetice este o problemă esențială care trebuie abordată pentru ca prezentul regulament să fie aplicat cu succes. Ar trebui să se pună un accent deosebit pe lacunele în materie de competențe ale producătorilor, ale autorităților de supraveghere a pieței și ale organismelor notificate. Prin urmare, în conformitate cu comunicarea Comisiei 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»)”, ar trebui instituite măsuri specifice atât la nivelul Uniunii, cât și la nivelul statelor membre, pentru a evalua starea și evoluția pieței forței de muncă în domeniul securității cibernetice și sinergiile pentru ofertele de educație și formare în domeniul securității cibernetice, abordând, de asemenea, problema deficitului de gen în acest sector, cu scopul de a stabili o abordare comună la nivelul Uniunii în ceea ce privește formarea în domeniul securității cibernetice.

(11) Un internet sigur este indispensabil pentru funcționarea infrastructurilor critice și pentru societate în ansamblu. Directiva ***(UE) 2022/2555*** vizează asigurarea unui nivel ridicat de securitate cibernetică a serviciilor furnizate de entități esențiale și importante, inclusiv de furnizori de infrastructură digitală care sprijină funcțiile de bază ale internetului deschis și asigură accesul la internet și serviciile de internet. Prin urmare, este important ca produsele cu elemente digitale necesare pentru ca furnizorii de infrastructură digitală să asigure funcționarea internetului să fie dezvoltate în mod securizat și să respecte standardele consacrate în materie de securitate a internetului. Prezentul regulament, care se aplică tuturor produselor hardware și software conectabile, are ca scop, de asemenea, să faciliteze respectarea de către furnizorii de

infrastructură digitală a cerințelor lanțului de aprovizionare în temeiul Directivei ***(UE) 2022/2555***, prin asigurarea faptului că produsele cu elemente digitale pe care le utilizează pentru furnizarea serviciilor lor sunt dezvoltate în mod securizat și că au acces la actualizări de securitate în timp util pentru aceste produse.

(12) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului[11] stabilește norme privind dispozitivele medicale, iar Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului[12] stabilește norme privind dispozitivele medicale pentru diagnostic in vitro. Ambele regulamente vizează riscurile de securitate cibernetică și urmează abordări specifice care sunt vizate și în prezentul regulament. Mai precis, Regulamentele (UE) 2017/745 și (UE) 2017/746 stabilesc cerințe esențiale pentru dispozitivele medicale care funcționează printr-un sistem electronic sau care sunt ele însele software. Anumite tipuri de software neîncorporat și abordarea bazată pe întregul ciclu de viață sunt, de asemenea, vizate de regulamentele respective. Aceste cerințe le impun producătorilor să își dezvolte și să își construiască produsele aplicând principii de gestionare a riscurilor și stabilind cerințe privind măsurile de securitate informatică, precum și proceduri corespunzătoare de evaluare a conformității. În plus, din decembrie 2019 sunt în vigoare orientări specifice privind securitatea cibernetică a dispozitivelor medicale[13], care le oferă producătorilor de dispozitive medicale, inclusiv de dispozitive pentru diagnostic in vitro, orientări privind modul de îndeplinire a tuturor cerințelor esențiale relevante din anexa I la regulamentele respective în ceea ce privește securitatea cibernetică. Prin urmare, produsele cu elemente digitale cărora li se aplică unul dintre aceste regulamente nu ar trebui să facă obiectul prezentului regulament.

(12a) Produsele cu elemente digitale care sunt dezvoltate exclusiv în scopuri militare sau

---

11 Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1).

12 Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

13 MDCG 2019-16, aprobate de Grupul de coordonare privind dispozitivele medicale (Medical Device Coordination Group – MDCG) instituit prin articolul 103 din Regulamentul (UE) 2017/745.

de securitate națională sau produsele concepute în mod specific pentru prelucrarea informațiilor clasificate nu intră în domeniul de aplicare al prezentului regulament. Cu toate acestea, statele membre sunt încurajate să asigure același nivel de protecție sau un nivel mai ridicat de protecție pentru produsele respective ca și pentru cele care intră în domeniul de aplicare al prezentului regulament.

(13) Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului[14] stabilește cerințe pentru omologarea de tip a vehiculelor și a sistemelor și componentelor acestora, introducând anumite cerințe de securitate cibernetică, inclusiv în ceea ce privește funcționarea unui sistem certificat de gestionare a securității cibernetice, actualizările software-ului, acoperind politicile și procesele organizațiilor pentru riscurile cibernetice legate de întregul ciclu de viață al vehiculelor, echipamentelor și serviciilor în conformitate cu reglementările aplicabile ale Organizației Națiunilor Unite privind specificațiile tehnice și securitatea cibernetică[15] și prevăzând proceduri specifice de evaluare a conformității. În domeniul aviației, principalul obiectiv al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului[16] este stabilirea și menținerea unui nivel ridicat și uniform al siguranței aviației civile în

---

14 Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele pentru omologarea de tip a autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate unor astfel de vehicule, în ceea ce privește siguranța generală a acestora și protecția ocupanților vehiculului și a utilizatorilor vulnerabili ai drumurilor, de modificare a Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului și de abrogare a Regulamentelor (CE) nr. 78/2009, (CE) nr. 79/2009 și (CE) nr. 661/2009 ale Parlamentului European și ale Consiliului și a Regulamentelor (CE) nr. 631/2009, (UE) nr. 406/2010, (UE) nr. 672/2010, (UE) nr. 1003/2010, (UE) nr. 1005/2010, (UE) nr. 1008/2010, (UE) nr. 1009/2010, (UE) nr. 19/2011, (UE) nr. 109/2011, (UE) nr. 458/2011, (UE) nr. 65/2012, (UE) nr. 130/2012, (UE) nr. 347/2012, (UE) nr. 351/2012, (UE) nr. 1230/2012 și (UE) 2015/166 ale Comisiei ***(JO L 325, 16.12.2019, p. 1).***

15 Regulamentul ONU nr. 155 – Dispoziții uniforme referitoare la omologarea vehiculelor în ceea ce privește securitatea cibernetică și sistemul de gestionare a securității cibernetice [2021/387].

16 Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).

Uniune. Regulamentul respectiv creează un cadru pentru cerințele esențiale de navigabilitate pentru produsele, piesele și echipamentele aeronautice, printre care și software-ul, care țin seama de obligațiile de protecție împotriva amenințărilor la adresa securității informațiilor. Prin urmare, produsele cu elemente digitale cărora li se aplică Regulamentul (UE) 2019/2144 și produsele certificate în conformitate cu Regulamentul (UE) 2018/1139 nu fac obiectul cerințelor esențiale și al procedurilor de evaluare a conformității prevăzute în prezentul regulament. Procesul de certificare în temeiul Regulamentului (UE) 2018/1139 garantează nivelul de asigurare vizat de prezentul regulament.

(14) Prezentul regulament stabilește norme orizontale în materie de securitate cibernetică care nu sunt specifice sectoarelor sau anumitor produse cu elemente digitale. Cu toate acestea, ar putea fi introduse norme sectoriale sau specifice produselor la nivelul Uniunii, care să stabilească cerințe care să abordeze toate sau unele dintre riscurile acoperite de cerințele esențiale prevăzute de prezentul regulament. În astfel de cazuri, aplicarea prezentului regulament în cazul unor produse cu elemente digitale care fac obiectul altor norme ale Uniunii care stabilesc cerințe care abordează toate sau unele dintre riscurile acoperite de cerințele esențiale prevăzute în anexa I la prezentul regulament poate fi limitată sau exclusă dacă această limitare sau excludere este în concordanță cu cadrul general de reglementare aplicabil produselor respective și dacă normele sectoriale asigură același nivel de protecție ca cel prevăzut de prezentul regulament. Comisia este împuternicită să adopte acte delegate pentru a modifica prezentul regulament prin identificarea produselor și a normelor respective. În ceea ce privește legislația existentă a Uniunii în cazul căreia ar trebui să se aplice astfel de limitări sau excluderi, prezentul regulament conține dispoziții specifice pentru a clarifica relația sa cu legislația respectivă a Uniunii.

(14a) Pentru a se asigura că produsele puse la dispoziție pe piață pot fi reparate în mod eficace și că durabilitatea lor poate fi prelungită, ar trebui să se prevadă o derogare pentru piesele de schimb. Acest lucru ar trebui să fie valabil atât pentru piesele de schimb care au scopul de a repara produsele preexistente puse la dispoziție înainte de data aplicării prezentului regulament, cât și pentru piesele de schimb care au făcut deja obiectul unei proceduri de evaluare a conformității în temeiul prezentului regulament și care sunt furnizate de același producător.

(14b) Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului[17] stabilește o serie de cerințe pentru a se asigura securitatea rețelelor și a sistemelor informatice care sprijină procesele comerciale ale entităților financiare. Comisia ar trebui să monitorizeze punerea în aplicare a prezentului regulament în sectorul financiar pentru a asigura compatibilitatea și a evita suprapunerile pentru produsele cu elemente digitale care pot fi, de asemenea, reglementate de Regulamentul (UE) 2022/2554.

(14c) Vehiculele agricole și forestiere care intră în domeniul de aplicare al Regulamentului (UE) 167/2013 al Parlamentului European și al Consiliului[18] intră, de asemenea, în domeniul de aplicare al prezentului regulament. Viitoarele modificări ale Regulamentului (UE) nr. 167/2013 ar trebui să evite suprapunerile în materie de reglementare.

(15) Regulamentul delegat (UE) 2022/30 ***al Comisiei***[19] precizează că cerințele esențiale prevăzute la articolul 3 alineatul (3) litera (d) (prejudiciile aduse rețelei și utilizarea necorespunzătoare a resurselor acesteia), litera (e) (datele cu caracter personal și viața privată) și litera (f) (fraudele) din Directiva 2014/53/UE se aplică anumitor echipamente radio. [Decizia de punere în aplicare XXX/2022 a Comisiei privind o cerere de standardizare adresată organizațiilor europene de standardizare] stabilește cerințe pentru elaborarea unor standarde specifice care să detalieze modul în care ar trebui abordate aceste trei cerințe esențiale. Cerințele esențiale prevăzute de prezentul regulament includ toate elementele cerințelor esențiale menționate la articolul 3 alineatul (3) literele (d), (e) și (f) din Directiva 2014/53/UE. În plus, cerințele esențiale prevăzute de prezentul regulament sunt aliniate la obiectivele cerințelor pentru standardele specifice incluse în cererea de standardizare respectivă. Prin urmare,

---

17 ***Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 (JO L 333, 27.12.2022, p. 1).***

18 ***Regulamentul (UE) nr. 167/2013 al Parlamentului European și al Consiliului din 5 februarie 2013 privind omologarea și supravegherea pieței pentru vehiculele agricole și forestiere (JO L 60, 2.3.2013, p. 1).***

19 ***Regulamentul delegat (UE) 2022/30 al Comisiei din 29 octombrie 2021 de completare a Directivei 2014/53/UE a Parlamentului European și a Consiliului în ceea ce privește aplicarea cerințelor esențiale menționate la articolul 3 alineatul (3) literele (d), (e) și (f) din directiva respectivă (JO L 7, 12.1.2022, p. 6).***

atunci când Comisia ▌ modifică Regulamentul delegat (UE) 2022/30, cu consecința că acesta încetează să se aplice în cazul anumitor produse care fac obiectul prezentului regulament, Comisia și organizațiile europene de standardizare ar trebui să ia în considerare activitatea de standardizare desfășurată în contextul Deciziei de punere în aplicare C(2022) 5637 a Comisiei privind o cerere de standardizare pentru Regulamentul delegat (UE) 2022/30 RED atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a prezentului regulament. ***În cazul în care producătorii respectă prezentul regulament înainte de data aplicării sale, ar trebui să se considere că aceștia respectă, de asemenea, regulamentul delegat (UE) 2022/30 al Comisiei, până la abrogarea de către Comisie a regulamentului delegat respectiv.***

(16) Directiva 85/374/CEE ***a Consiliului***[20] este complementară prezentului regulament. Aceasta stabilește norme privind răspunderea pentru produsele cu defecte, pentru ca persoanele prejudiciate să poată solicita despăgubiri în cazul în care anumite produse cu defecte au provocat un prejudiciu. Directiva respectivă stabilește principiul conform căruia producătorul unui produs este răspunzător pentru prejudiciile provocate cauzate de lipsa de siguranță a produsului său, indiferent de culpă („răspundere obiectivă”). În cazul în care o astfel de lipsă de siguranță constă în lipsa actualizărilor de securitate după introducerea produsului pe piață, iar acest lucru provoacă prejudicii, ar putea fi angajată răspunderea producătorului. Prezentul regulament ar trebui să prevadă obligații pentru producători referitoare la furnizarea unor astfel de actualizări de securitate.

(17) Prezentul regulament nu ar trebui să aducă atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului[21], inclusiv dispozițiilor privind instituirea unor mecanisme de certificare în domeniul protecției datelor și a unor sigilii și mărcilor în materie de protecție a datelor, cu scopul de a demonstra conformitatea operațiunilor

---

20 Directiva 85/374/CEE a Consiliului din 25 iulie 1985 de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre cu privire la răspunderea pentru produsele cu defect, JO L 210, 7.8.1985, p. 29.

21 Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

de prelucrare efectuate de operatori și de persoanele împuternicite de operatori cu regulamentul respectiv. Astfel de operațiuni ar putea fi încorporate într-un produs cu elemente digitale. Protecția datelor începând cu momentul conceperii și în mod implicit, precum și securitatea cibernetică în general sunt elemente-cheie ale Regulamentului (UE) 2016/679. Prin protejarea consumatorilor și a organizațiilor de riscurile de securitate cibernetică, cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament trebuie, de asemenea, să contribuie la îmbunătățirea protecției datelor cu caracter personal și a vieții private a persoanelor. Ar trebui avute în vedere sinergii atât în ceea ce privește standardizarea, cât și certificarea cu privire la aspectele legate de securitatea cibernetică prin cooperarea dintre Comisie, organizațiile europene de standardizare, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Comitetul european pentru protecția datelor (CEPD) instituit prin Regulamentul (UE) 2016/679 și autoritățile naționale de supraveghere a protecției datelor. De asemenea, ar trebui create sinergii între prezentul regulament și legislația Uniunii în materie de protecție a datelor în domeniul supravegherii pieței și al asigurării respectării legislației. În acest scop, autoritățile naționale de supraveghere a pieței desemnate în temeiul prezentului regulament ar trebui să coopereze cu autoritățile care supraveghează legislația Uniunii în materie de protecție a datelor. De asemenea, acestea din urmă ar trebui să aibă acces la informațiile relevante pentru îndeplinirea sarcinilor lor.

(18) În măsura în care produsele lor intră în domeniul de aplicare al prezentului regulament, emitenții de portofele europene pentru identitatea digitală, astfel cum sunt menționate la articolul [articolul 6a alineatul (2) din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Propunerea de regulament de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană], ar trebui să respecte atât cerințele esențiale orizontale instituite prin prezentul regulament, cât și cerințele de securitate specifice prevăzute la articolul [articolul 6a din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Propunerea de regulament de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană]. Pentru a facilita respectarea acestora, emitenții de portofele ar trebui să poată demonstra conformitatea portofelelor europene pentru identitatea digitală cu cerințele prevăzute în ambele acte prin certificarea produselor lor în cadrul unui sistem european de

certificare de securitate cibernetică instituit în temeiul Regulamentului (UE) 2019/881 și pentru care Comisia a specificat, prin intermediul unui act de punere în aplicare, o prezumție de conformitate pentru prezentul regulament, în măsura în care certificatul sau anumite părți ale acestuia acoperă cerințele respective.

(18a) Atunci când achiziționează produse cu elemente digitale, statele membre ar trebui să acorde prioritate produselor care au un nivel ridicat de securitate cibernetică și o perioadă adecvată de asistență a produselor, pentru a îmbunătăți capacitatea acestora de a face față amenințărilor cibernetice, precum și pentru a asigura utilizarea eficientă a resurselor publice. În plus, statele membre ar trebui să se asigure că producătorii remediază de urgență vulnerabilitățile care afectează produsele achiziționate public cu elemente digitale, cât mai curând posibil, în cazul în care aceste produse au un profil semnificativ de risc.

(19) Anumite sarcini prevăzute în prezentul regulament ar trebui să fie îndeplinite de ENISA, în conformitate cu articolul 3 alineatul (2) din Regulamentul (UE) 2019/881. În special, ENISA ar trebui să primească notificări de la producători cu privire la vulnerabilitățile exploatate activ conținute în produsele cu elemente digitale, precum și cu privire la incidentele ***semnificative*** care au un impact asupra securității acestor produse. ***Vulnerabilitățile care fac obiectul raportării obligatorii se referă la cazurile în care un actor execută un cod rău-intenționat pe un produs cu elemente digitale pentru a genera o încălcare a securității, de exemplu prin exploatarea deficiențelor în ceea ce privește funcțiile de identificare și autentificare. Vulnerabilitățile descoperite fără intenție răuvoitoare în scopul testării, investigării, corectării sau divulgării cu bună-credință pentru a promova securitatea sau siguranța proprietarului sistemului și a utilizatorilor acestuia nu ar trebui să facă obiectul unor notificări obligatorii. Un incident semnificativ care are un impact asupra securității produsului cu elemente digitale se referă la un incident de securitate cibernetică care poate afecta grav procesele de dezvoltare, producție și întreținere ale producătorului și care, la rândul său, poate avea un impact semnificativ asupra securității produselor sale. Un incident semnificativ ar putea include o situație în care un atacator a compromis cu succes canalul de lansare prin care producătorul eliberează actualizări de securitate utilizatorilor.***

(19a) ENISA ar trebui, de asemenea, să transmită aceste notificări echipelor de intervenție

în caz de incidente de securitate informatică (CSIRT) relevante sau, respectiv, punctelor unice de contact relevante din statele membre desemnate în conformitate cu articolul [articolul X] din Directiva ***(UE) 2022/2555*** și să informeze autoritățile relevante de supraveghere a pieței cu privire la vulnerabilitatea notificată***. ENISA ar trebui să se asigure că notificările respective sunt primite, stocate și transmise prin canale securizate și că există protocoale clare cu privire la cine poate avea acces la ele și la modalitățile de transmitere ulterioară a acestora. ENISA ar trebui să asigure confidențialitatea notificărilor respective în special în ceea ce privește vulnerabilitățile pentru care încă nu este disponibilă o actualizare de securitate***. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită grupului de cooperare menționat în Directiva ***(UE) 2022/2555***. În plus, având în vedere expertiza și mandatul său, ENISA ar trebui să fie în măsură să sprijine procesul de punere în aplicare a prezentului regulament. În special, aceasta ar trebui să fie în măsură să propună activități comune care să fie desfășurate de autoritățile de supraveghere a pieței pe baza unor indicații sau informații privind o posibilă neconformitate cu prezentul regulament a produselor cu elemente digitale din mai multe state membre sau să identifice categoriile de produse pentru care ar trebui organizate acțiuni de control coordonate simultane. În circumstanțe excepționale, la cererea Comisiei, ENISA ar trebui să poată efectua evaluări cu privire la anumite produse cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică, în cazul în care este necesară o intervenție imediată pentru a menține buna funcționare a pieței interne.

(20) Produsele cu elemente digitale ar trebui să poarte marcajul CE pentru a indica ***în mod vizibil, lizibil și fără posibilitate de ștergere*** conformitatea lor cu prezentul regulament, astfel încât să poată circula liber în cadrul pieței interne. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață a produselor cu elemente digitale care sunt conforme cu cerințele prevăzute în prezentul regulament și care poartă marcajul CE. ***În plus, la târgurile comerciale, expoziții și demonstrații sau evenimente similare, statele membre nu împiedică prezentarea și utilizarea unui produs prototip cu elemente digitale.***

(21) Pentru a se asigura că producătorii pot lansa software în scopuri de testare înainte de a-și supune produsele unei evaluări a conformității, statele membre nu ar trebui să împiedice punerea la dispoziție ***într-o versiune care nu este în producție*** a software-ului nefinalizat, cum ar fi versiunile alfa, beta sau cele candidate la lansare, atât timp cât versiunea este pusă la dispoziție numai pentru perioada necesară pentru a o testa și a primi feedback. Producătorii ar trebui să se asigure că software-ul pus la dispoziție în aceste condiții este lansat numai în urma unei evaluări a riscurilor și că respectă, în măsura posibilului, cerințele de securitate referitoare la proprietățile produselor cu elemente digitale impuse de prezentul regulament. De asemenea, producătorii ar trebui să pună în aplicare, în măsura posibilului, cerințele de gestionare a vulnerabilităților. Producătorii nu ar trebui să oblige utilizatorii să treacă la versiunile lansate numai în scopul testării.

(22) Pentru a se asigura că produsele cu elemente digitale, atunci când sunt introduse pe piață, nu prezintă riscuri în materie de securitate cibernetică pentru persoane și organizații, ar trebui stabilite cerințe esențiale pentru astfel de produse. Atunci când produsele sunt modificate ulterior, prin mijloace fizice sau digitale, într-un mod care nu este prevăzut de producător și care poate implica faptul că acestea nu mai îndeplinesc cerințele esențiale relevante, modificarea ar trebui considerată substanțială. De exemplu, ***actualizările necesare de securitate***, actualizările sau reparațiile software-ului***, precum ajustările minore ale codului sursă care pot îmbunătăți securitatea și funcționarea, nu ar trebui considerate modificări substanțiale***, cu condiția ca acestea să nu modifice un produs deja introdus pe piață astfel încât să poată fi afectată conformitatea cu cerințele aplicabile sau să poată fi schimbată utilizarea preconizată pentru care a fost evaluat produsul. ***Acest lucru este valabil, în general, pentru noile versiuni de software care vizează îmbunătățirea performanței și remedierea vulnerabilităților. Actualizările minore ale funcționalității, cum ar fi îmbunătățirile vizuale, adăugarea de noi limbi la interfața pentru utilizatori sau a unui nou set de pictograme, nu ar trebui, în general, să fie considerate modificări substanțiale.*** La fel ca în cazul reparațiilor sau al modificărilor fizice, un produs cu elemente digitale ar trebui să fie considerat ca fiind modificat substanțial de o modificare a software-ului dacă actualizarea software-ului modifică tipul, performanța sau funcțiile inițiale preconizate ale produsului, iar aceste modificări nu au fost prevăzute în evaluarea inițială a riscurilor sau dacă natura pericolului s-a

schimbat sau nivelul de risc a crescut ca urmare a actualizării software-ului***, astfel cum este cazul revizuirilor de software***. ***Comisia ar trebui să emită orientări cu privire la modul de stabilire a ceea ce constituie o modificare substanțială***.

(23) În conformitate cu noțiunea stabilită de comun acord a modificării substanțiale pentru produsele reglementate de legislația de armonizare a Uniunii, ori de câte ori apare o modificare substanțială care ar putea afecta conformitatea produsului cu prezentul regulament sau atunci când scopul preconizat al produsului se modifică, este oportun ca conformitatea produsului cu elemente digitale să fie verificată și, după caz, ca acesta să fie supus unei noi evaluări a conformității. După caz, dacă producătorul efectuează o evaluare a conformității care implică un terț, modificările care ar putea duce la modificări substanțiale ar trebui notificate părții terțe.

(24) Recondiționarea, întreținerea și repararea unui produs cu elemente digitale, astfel cum sunt definite în regulament [Regulamentul privind proiectarea ecologică], nu conduc neapărat la o modificare substanțială a produsului, de exemplu în cazul în care utilizarea și funcționalitățile preconizate nu sunt modificate, iar nivelul de risc rămâne neafectat. Cu toate acestea, modernizarea unui produs de către producător ar putea duce la modificări ale proiectării și dezvoltării produsului și, prin urmare, ar putea afecta utilizarea preconizată și conformitatea produsului cu cerințele stabilite în prezentul regulament.

(25) Produsele cu elemente digitale ar trebui considerate critice dacă impactul negativ al exploatării potențialelor vulnerabilități în materie de securitate cibernetică ale produsului poate fi grav din cauza, printre altele, a funcționalității legate de securitatea cibernetică sau a utilizării preconizate. În special, vulnerabilitățile produselor cu elemente digitale care au o funcționalitate legată de securitatea cibernetică, de exemplu elementele de securitate, pot conduce la o propagare a problemelor de securitate în întregul lanț de aprovizionare. Gravitatea impactului unui incident de securitate cibernetică poate crește, de asemenea, atunci când se ia în considerare utilizarea preconizată a produsului, de exemplu într-un cadru industrial sau în contextul unei entități esențiale de tipul celor menționate în anexa [anexa I] la Directiva ***(UE) 2022/2555*** sau ▌ îndeplinirea unor funcții critice sau sensibile, ***care au un efect asupra sănătății, siguranței sau drepturilor fundamentale.***

(26) Produsele critice cu elemente digitale ar trebui să facă obiectul unor proceduri mai stricte de evaluare a conformității, menținând, în același timp, o abordare proporțională. În acest scop, produsele critice cu elemente digitale ar trebui împărțite în două clase, în funcție de nivelul de risc de securitate cibernetică legat de aceste categorii de produse. Un potențial incident cibernetic care implică produse din clasa II ar putea avea un impact negativ mai mare decât un incident care implică produse din clasa I, de exemplu din cauza naturii funcției lor legate de securitatea cibernetică sau a utilizării preconizate în medii ***cu risc ridicat***, și, prin urmare, ar trebui să facă obiectul unei proceduri mai stricte de evaluare a conformității.

(27) Categoriile de produse critice cu elemente digitale menționate în anexa III la prezentul regulament ar trebui înțelese ca fiind produsele care au funcționalitatea de bază de tipul inclus în anexa III la prezentul regulament. De exemplu, anexa III la prezentul regulament enumeră produsele care sunt definite prin funcționalitatea lor de bază ca microprocesoare de uz general din clasa I. În consecință, utilizarea generală a microprocesoarelor face obiectul evaluării obligatorii de conformitate de către terți. Acest lucru nu este valabil pentru alte produse care nu sunt menționate în mod explicit în anexa III la prezentul regulament și care pot integra un microprocesor de uz general. Comisia ar trebui să adopte acte delegate [în termen de ***6*** luni de la intrarea în vigoare a prezentului regulament] pentru a preciza definițiile categoriilor de produse incluse în clasele I și II, astfel cum sunt prevăzute în anexa III. ***În vederea asigurării clarității și securității juridice, precum și a previzibilității pentru ca părțile interesate să se conformeze prezentului regulament, ar trebui aduse modificări listei din anexa III cel mai devreme la doi ani de la intrarea în vigoare a prezentului regulament și, din nou, cel mai devreme la doi ani ulterior. Comisia ar trebui să instituie un proces în baza căruia un produs care este candidat pentru a deveni produs critic să poată fi revizuit, într-un proces de colaborare, de toate părțile interesate relevante, inclusiv de către producători și utilizatori, cu scopul de a evalua riscul de securitate pe care îl prezintă potențialele probleme de securitate cibernetică a produsului, dacă și cât de mult desemnarea produsului drept critic ar putea reduce acest risc, precum și costurile asociate desemnării produsului drept critic, înainte de adoptarea actelor delegate relevante.***

(27a) Comisia ar trebui să înființeze un grup de experți privind reziliența cibernetică

(denumit în continuare „grupul de experți”), cu o componență largă și diversă. Grupul de experți ar trebui să sprijine Comisia pentru a asigura punerea în aplicare corespunzătoare a prezentului regulament, de exemplu prin consilierea Comisiei cu privire la posibilele modificări ale listei de produse critice, astfel cum figurează în anexa III, sau prin analizarea modului în care standardele europene și internaționale pot permite respectarea cerințelor esențiale ale prezentului regulament. Comisia ar trebui să consulte grupul de experți și să organizeze consultări publice atunci când pregătește acte delegate și acte de punere în aplicare în temeiul prezentului regulament, pentru a se asigura că toate părțile interesate pot furniza contribuțiile necesare.

(28) Prezentul regulament abordează riscurile de securitate cibernetică într-un mod specific. Cu toate acestea, produsele cu elemente digitale ar putea prezenta și alte riscuri în materie de siguranță, care să nu fie ***întotdeauna*** legate de securitatea cibernetică***, dar care pot fi consecința unei încălcări a securității***. Aceste riscuri ar trebui să fie reglementate în continuare de alte acte legislative relevante ale Uniunii privind produsele. În cazul în care nu este aplicabil niciun alt act din legislația de armonizare a Uniunii, acestea ar trebui să facă obiectul Regulamentului ***(UE) 2023/988***. Prin urmare, având în vedere caracterul specific al prezentului regulament, prin derogare de la articolul 2 alineatul (1) al treilea paragraf litera (b) din Regulamentul ***(UE) 2023/988***produselor cu elemente digitale ar trebui să li se aplice capitolul III secțiunea 1, capitolele V și VII și capitolele IX-XI din Regulamentul ***(UE) 2023/988*** în ceea ce privește riscurile în materie de siguranță care nu sunt acoperite de prezentul regulament, dacă produsele respective nu fac obiectul unor cerințe specifice impuse de alte acte din legislația de armonizare a Uniunii în sensul articolului 3 punctului 25 din Regulamentul ***(UE) 2023/988***.

(29) Produsele cu elemente digitale clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul 6 din Regulamentul [Regulamentul privind inteligența artificială][22] care intră în domeniul de aplicare al prezentului regulament ar trebui să respecte cerințele esențiale prevăzute în prezentul regulament. Atunci când aceste sisteme de IA cu grad ridicat de risc îndeplinesc cerințele esențiale ale prezentului regulament, acestea ar trebui să fie considerate conforme cu cerințele de securitate

[22] Regulamentul [Regulamentul privind inteligența artificială].

cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], în măsura în care cerințele respective sunt acoperite de declarația de conformitate UE sau de anumite părți ale acesteia, emisă în temeiul prezentului regulament. În ceea ce privește procedurile de evaluare a conformității referitoare la cerințele esențiale de securitate cibernetică ale unui produs cu elemente digitale care face obiectul prezentului regulament și este clasificat ca sistem de IA cu grad ridicat de risc, dispozițiile relevante ale articolului 43 din Regulamentul [Regulamentul privind inteligența artificială] ar trebui să se aplice de regulă în locul dispozițiilor respective din prezentul regulament. Totuși, această regulă nu ar trebui să conducă la reducerea nivelului necesar de asigurare pentru produsele critice cu elemente digitale care intră sub incidența prezentului regulament. Prin urmare, prin derogare de la această regulă, sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al Regulamentului [Regulamentul privind inteligența artificială] și sunt, de asemenea, clasificate drept produse critice cu elemente digitale în temeiul prezentului regulament și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa VI la Regulamentul [Regulamentul privind inteligența artificială] ar trebui să facă obiectul dispozițiilor privind evaluarea conformității ale prezentului regulament în ceea ce privește cerințele esențiale ale prezentului regulament. În acest caz, pentru toate celelalte aspecte vizate de Regulamentul [Regulamentul privind inteligența artificială] ar trebui să se aplice dispozițiile privind evaluarea conformității bazată pe control intern prevăzute în anexa VI la Regulamentul [Regulamentul privind inteligența artificială].

(30) Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului ***(UE) 2023/1230 al Parlamentului European și al Consiliului***[23] care sunt produse cu elemente digitale în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate pe baza prezentului regulament ar trebui considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul ***(UE) 2023/1230*** în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control, în măsura în care

[23] Regulamentul (UE) 2023/1230 al Parlamentului European și al Consiliului din 14 iunie 2023 privind mașinile și de abrogare a Directivei 2006/42/CE a Parlamentului European și a Directivei Consiliului 73/361/CEE, (JO L 165, 29.6.2023, p. 1).

conformitatea cu cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.

(31) Regulamentul [Propunerea de regulament referitor la spațiul european al datelor privind sănătatea] completează cerințele esențiale prevăzute în prezentul regulament. Prin urmare, sistemele de dosare electronice de sănătate („sistemele DES”) care intră în domeniul de aplicare al Regulamentului [Propunerea de regulament referitor la spațiul european al datelor privind sănătatea] și care sunt produse cu elemente digitale în sensul prezentului regulament ar trebui să respecte și cerințele esențiale prevăzute în prezentul regulament. Producătorii acestora ar trebui să demonstreze conformitatea astfel cum se solicită în Regulamentul [Propunerea de regulament referitor la spațiul european al datelor privind sănătatea]. Pentru a facilita conformarea, producătorii pot întocmi o singură documentație tehnică care să conțină elementele prevăzute de ambele acte juridice. Întrucât prezentul regulament nu acoperă SaaS ca atare, sistemele DES oferite prin intermediul modelului de acordare de licențe și de livrare SaaS nu intră în domeniul de aplicare al prezentului regulament. În mod similar, sistemele DES care sunt dezvoltate și utilizate intern ***nu intră*** în domeniul de aplicare al prezentului regulament, deoarece nu sunt introduse pe piață.

(32) Pentru a se asigura faptul că produsele cu elemente digitale sunt sigure atât în momentul introducerii lor pe piață, cât și pe parcursul întregului lor ciclu de viață, este necesar să se stabilească cerințe esențiale pentru gestionarea vulnerabilităților și cerințe esențiale de securitate cibernetică legate de proprietățile produselor cu elemente digitale. Deși producătorii ar trebui să respecte toate cerințele esențiale legate de gestionarea vulnerabilităților ***pe întreaga perioadă de asistență***, aceștia ar trebui să stabilească celelalte cerințe esențiale legate de proprietățile produsului care sunt relevante pentru tipul de produs în cauză. În acest scop, producătorii ar trebui să efectueze o evaluare a riscurilor de securitate cibernetică asociate unui produs cu elemente digitale pentru a identifica riscurile relevante și cerințele esențiale relevante și pentru ***a face disponibile produsele fără vulnerabilități exploatabile cunoscute care ar putea avea un impact asupra securității produselor respective și pentru*** a aplica în mod corespunzător standarde armonizate**,** specificații comune ***sau standarde internaționale*** adecvate.

(32a) Producătorii ar trebui să stabilească perioada de asistență în cursul căreia se

asigură că vulnerabilitățile sunt gestionate, ținând seama în mod corespunzător de diverse criterii, inclusiv de durata de viață preconizată a produsului, de natura produsului în sine, de disponibilitatea mediului de operare, de așteptările utilizatorilor, în special ale consumatorilor, și, dacă este posibil, de perioada de asistență a altor componente principale integrate în produs. Producătorii ar trebui să se asigure că perioada de asistență reflectă în mod adecvat necesitatea de a promova securitatea cibernetică pe piața Uniunii și este stabilită ținând seama în mod corespunzător de perioada în care se preconizează că un produs cu elemente digitale va fi disponibil pe piață. Autoritățile de supraveghere a pieței ar trebui să se asigure în mod proactiv că producătorii aplică aceste criterii în mod adecvat. Autoritățile de supraveghere a pieței și Comisia ar trebui să colecteze și să analizeze date cu privire la perioadele de sprijin stabilite de producători și la durata de viață preconizată a produselor, pentru a se asigura că prezentul regulament își îndeplinește obiectivul de promovare a securității cibernetice a produselor cu elemente digitale. Astfel de analize ar trebui, printre altele, să informeze Comisia cu privire la evaluarea prezentului regulament, odată ce acesta se aplică.

(32b) Producătorii ar trebui să se asigure, atunci când acest lucru este fezabil din punct de vedere tehnic, că produsele cu elemente digitale fac o distincție clară între actualizările de securitate și cele de funcționalitate. Actualizările de securitate, menite să reducă nivelul de risc sau să remedieze vulnerabilitățile potențiale, ar trebui să fie instalate automat, în special în cazul produselor de consum. Utilizatorii ar trebui să aibă în continuare posibilitatea de a dezactiva această funcție, cu un mecanism clar și ușor de utilizat. Odată ce producătorul nu mai asigură gestionarea vulnerabilităților produsului cu elemente digitale, ar trebui să informeze utilizatorii într-un mod simplu și clar, de exemplu prin afișarea unei notificări ușor de utilizat.

(32c) În cazul în care producătorii stabilesc perioada de asistență pentru mai puțin de cinci ani și nu mai oferă gestionarea vulnerabilităților pentru produsul cu elemente digitale, aceștia ar trebui să poată să își pună codul sursă la dispoziția întreprinderilor care doresc să furnizeze actualizări de securitate și alte servicii similare. Un astfel de acces ar trebui să fie pus la dispoziție numai ca parte a unui acord contractual care protejează proprietatea asupra produsului cu elemente digitale și împiedică diseminarea codului sursă către publicul larg, cu excepția

cazului în care acest cod a fost deja furnizat pe baza unei licențe libere și cu sursă deschisă.

(33) Pentru a îmbunătăți securitatea produselor cu elemente digitale introduse pe piața internă, este necesar să se stabilească cerințe esențiale. Aceste cerințe esențiale nu ar trebui să aducă atingere evaluărilor coordonate la nivelul UE ale riscurilor pentru lanțurile de aprovizionare critice instituite prin ▌ Directiva ***(UE) 2022/2555*** ▌ care iau în considerare atât factori de risc tehnici, cât și, după caz, factori de risc netehnici, cum ar fi influența nejustificată a unei țări terțe asupra furnizorilor. În plus, nu ar trebui să se aducă atingere prerogativelor statelor membre de a stabili cerințe suplimentare care să țină seama de factori netehnici în scopul asigurării unui nivel ridicat de reziliență, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul Uniunii a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G convenit de Grupul de cooperare NIS, astfel cum se menționează în Directiva ***(UE) 2022/2555***.

(34) Pentru a se asigura că echipele CSIRT naționale și punctele unice de contact desemnate în conformitate cu ▌ Directiva ***(UE) 2022/2555*** primesc informațiile necesare pentru îndeplinirea sarcinilor lor și pentru creșterea nivelului general de securitate cibernetică a entităților esențiale și importante, precum și pentru a asigura funcționarea eficace a autorităților de supraveghere a pieței, producătorii de produse cu elemente digitale ar trebui să informeze ENISA cu privire la vulnerabilitățile care sunt exploatate activ. Întrucât majoritatea produselor cu elemente digitale sunt comercializate pe întreaga piață internă, orice vulnerabilitate exploatată a unui produs cu elemente digitale ar trebui considerată o amenințare la adresa funcționării pieței interne. Producătorii ar trebui să ***divulge*** vulnerabilitățile remediate în baza de date europeană privind vulnerabilitățile instituită în temeiul Directivei ***(UE) 2022/2555*** și gestionată de ENISA ▌. ***ENISA ar trebui, de asemenea, să publice vulnerabilitățile notificate în baza de date europeană a vulnerabilităților și ar trebui să dispună de o procedură adecvată privind procesul de publicare, pentru a acorda producătorilor timpul necesar elaborării actualizărilor de securitate necesare și utilizatorilor timpul necesar pentru a le pune în aplicare sau pentru a lua alte măsuri corective sau de atenuare. Baza de date europeană a vulnerabilităților ar trebui să îi ajute pe***

producători să depisteze vulnerabilitățile exploatabile identificate în produsele lor, pentru a garanta introducerea pe piață a unor produse sigure.

(34a) Uniunea trebuie să maximizeze beneficiile deschiderii sale economice, reducând în același timp la minimum riscurile generate de dependențele economice de furnizorii cu risc ridicat, prin intermediul unui cadru strategic comun pentru securitatea economică a Uniunii[24]. Dependențele de furnizorii cu risc ridicat de produse critice cu elemente digitale prezintă un risc strategic care ar trebui abordat la nivelul Uniunii, în special atunci când produsele critice cu elemente digitale sunt destinate utilizării de către entități esențiale de tipul celor menționate în Directiva (UE) 2022/2555. Astfel de riscuri pot fi legate de jurisdicția aplicabilă producătorului, de caracteristicile acționariatului său și de legăturile de control cu guvernul unei țări terțe în care acesta este stabilit, în special în cazul în care o țară se angajează în spionaj economic și legislația sa impune accesul arbitrar la orice tip de operațiuni sau date ale întreprinderilor, inclusiv date sensibile din punct de vedere comercial, și poate impune obligații legate de culegerea de informații fără respectarea principiului echilibrului democratic al puterilor, fără instituirea unui mecanism de supraveghere, respectarea normelor privind un proces echitabil sau a dreptului de a introduce o cale de atac în fața unui sistem judiciar independent. Autoritățile de supraveghere a pieței și Comisia ar trebui să ofere orientări și recomandări specifice operatorilor economici pentru a garanta faptul că sunt instituite acțiuni corective adecvate în cazul în care există motive suficiente pentru a considera că un produs cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, având în vedere astfel de factori de risc netehnici.

(35) Producătorii ar trebui, de asemenea, să raporteze către ENISA orice incident ***semnificativ*** care are un impact asupra securității produsului cu elemente digitale. Fără a aduce atingere obligațiilor de raportare a incidentelor prevăzute în ***Directiva (UE) 2022/2555*** pentru entitățile esențiale și importante, este esențial ca ENISA, punctele unice de contact desemnate de statele membre în conformitate cu articolul [articolul X] din ***Directiva (UE) 2022/2555*** și autoritățile de supraveghere a pieței să primească

---

24 ***A se vedea JOIN (2023)20 Comunicarea comună către Parlamentul European, Consiliul European și Consiliu privind „Strategia europeană pentru securitate economică”.***

informații de la producătorii de produse cu elemente digitale care să le permită să evalueze securitatea acestor produse. Pentru a se asigura că utilizatorii pot reacționa rapid la incidentele ***semnificative*** care au un impact asupra securității produselor lor cu elemente digitale, producătorii ar trebui, de asemenea, să își informeze utilizatorii cu privire la orice astfel de incident și, după caz, cu privire la orice măsuri corective pe care utilizatorii le pot adopta pentru a atenua impactul incidentului, de exemplu prin publicarea informațiilor relevante pe site-urile lor sau, dacă producătorul poate să contacteze utilizatorii și dacă riscurile justifică acest lucru, prin contactarea directă a utilizatorilor.

(35a) Producătorii, precum și alte entități și actori ar trebui, de asemenea, să poată raporta ENISA, în mod voluntar, cu privire la alte incidente de securitate cibernetică, amenințări cibernetice, incidente evitate la limită și orice altă vulnerabilitate.

(35b) ENISA ar trebui să instituie un mecanism digital securizat de raportare care, pentru a simplifica raportarea în cazul producătorilor, ar trebui să servească drept punct unic de intrare pentru obligațiile de raportare stabilite în temeiul prezentului regulament. Producătorii de produse cu elemente digitale se află adesea într-o situație în care, din cauza caracteristicilor sale, un anumit incident trebuie raportat mai multor autorități ca urmare a obligațiilor de notificare incluse în diferite instrumente juridice. Utilizarea mecanismului sus-menționat ar permite, acolo unde este posibil, efectuarea de raportări în temeiul altor acte legislative ale Uniunii, cum ar fi Regulamentul (UE) 2016/679, Directiva (UE) 2022/2555 și Directiva 2002/58/CE a Parlamentului European și a Consiliului[25], prin intermediul aceluiași mecanism. Mecanismul poate fi utilizat, de asemenea, pentru notificările voluntare din partea producătorilor și a altor entități și actori. ENISA ar trebui să se asigure că au fost instituite proceduri pentru a gestiona informațiile clasificate în mod securizat și confidențial.

(35c) Entitățile și persoanele fizice care cercetează vulnerabilități pot fi expuse, în unele state membre, răspunderii penale și civile. Comisia ar trebui să emită orientări cu privire la neurmărirea penală a cercetătorilor în domeniul securității informațiilor

---

[25] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (JO L 201, 31.7.2002, p. 37).

și exonerarea de răspundere civilă pentru activitățile desfășurate de aceștia.

(36) Producătorii de produse cu elemente digitale ar trebui să instituie politici coordonate de divulgare a vulnerabilităților pentru a facilita raportarea vulnerabilităților de către persoane fizice sau entități ***fie direct, către producător, fie indirect și, la cerere, în mod anonim, prin intermediul echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) desemnate drept coordonatori în scopul divulgării coordonate a vulnerabilităților în conformitate cu articolul 12 alineatul (1) din Directiva (UE) 2022/2555***. O politică coordonată de divulgare a vulnerabilităților ***pusă în aplicare de producători*** ar trebui să precizeze un proces structurat prin care vulnerabilitățile să fie raportate producătorului într-un mod care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitățile respective înainte ca informațiile detaliate referitoare la acestea să fie divulgate terților sau publicului. Având în vedere faptul că informațiile privind vulnerabilitățile exploatabile ale produselor cu elemente digitale care sunt utilizate pe scară largă pot fi vândute la prețuri ridicate pe piața neagră, producătorii de astfel de produse ar trebui să poată utiliza, ca parte a politicilor lor coordonate de divulgare a vulnerabilităților, programe prin care să stimuleze raportarea vulnerabilităților, asigurându-se că persoanele sau entitățile primesc recunoaștere și compensații pentru eforturile lor (așa-numitele „programe de stimulare a identificării bugurilor”).

(36a) Statele membre și ENISA ar trebui să se asigure că vulnerabilitățile raportate în temeiul prezentului regulament nu sunt utilizate de organismele publice în scopuri de culegere de informații, de supraveghere sau ofensive.

(37) Pentru a facilita analiza vulnerabilităților, producătorii ar trebui să identifice și să documenteze componentele conținute în produsele cu elemente digitale, inclusiv prin întocmirea unei liste a materialelor software ***(SBOM)***. ***SBOM*** le poate oferi celor care produc, achiziționează și exploatează software informații care le îmbunătățesc înțelegerea lanțului de aprovizionare, ceea ce aduce multiple avantaje, în special ajută producătorii și utilizatorii să urmărească vulnerabilitățile și riscurile nou apărute cunoscute. Este deosebit de important ca producătorii să se asigure că produsele lor nu conțin componente vulnerabile dezvoltate de terți. ***Cu toate acestea, producătorul nu ar trebui să fie obligat să facă publică lista materialelor software, deoarece acest***

lucru poate avea consecințe nedorite asupra securității cibernetice a produselor sale cu elemente digitale.

(38) Pentru a facilita evaluarea conformității cu cerințele prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu standardele armonizate, care transpun cerințele esențiale ale prezentului regulament în specificații tehnice detaliate și care sunt adoptate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[26]. Regulamentul (UE) nr. 1025/2012 prevede o procedură pentru formularea de obiecții cu privire la standardele armonizate în cazul în care standardele respective nu îndeplinesc în totalitate cerințele prezentului regulament. ***Procesul de standardizare ar trebui să asigure o reprezentare echilibrată a intereselor și participarea eficace a părților interesate din cadrul societății civile, inclusiv a organizațiilor de consumatori. De asemenea, ar trebui să se țină seama de standardele internaționale, pentru a simplifica elaborarea de standarde armonizate și punerea în aplicare a prezentului regulament, precum și pentru a reduce barierele tehnice netarifare din calea comerțului.***

(38a) Ținând cont de domeniul amplu de aplicare al prezentului regulament, dezvoltarea la timp a unor standarde armonizate reprezintă o provocare semnificativă. Comisia ar trebui să se asigure că vor fi instituite standarde armonizate până la data aplicării prezentului regulament, cu scopul de a garanta punerea în aplicare cu succes a prezentului regulament.

(39) Regulamentul (UE) 2019/881 stabilește un cadru european voluntar de certificare de securitate cibernetică pentru produsele, procesele și serviciile TIC. Sistemele europene de certificare de securitate cibernetică pot ***oferi un cadru comun de încredere pentru utilizatori, care să le permită să utilizeze produsele*** cu elemente digitale care fac obiectul prezentului regulament. Prezentul regulament ar trebui***, prin urmare,*** să

---

[26] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

creeze sinergii cu Regulamentul (UE) 2019/881. Pentru a facilita evaluarea conformității cu cerințele prevăzute în prezentul regulament, produsele cu elemente digitale care sunt certificate sau pentru care a fost emisă o declarație de conformitate în cadrul unui sistem de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 și care au fost identificate de Comisie într-un act de punere în aplicare sunt considerate a fi conforme cu cerințele esențiale ale prezentului regulament în măsura în care certificatul de securitate cibernetică sau declarația de conformitate ori anumite părți ale acestora acoperă cerințele respective. În lumina prezentului regulament ar trebui evaluată necesitatea unor noi sisteme europene de certificare de securitate cibernetică pentru produsele cu elemente digitale. Astfel de sisteme europene viitoare de certificare de securitate cibernetică care vor acoperi produsele cu elemente digitale ar trebui să țină seama de cerințele esențiale prevăzute în prezentul regulament și să faciliteze respectarea prezentului regulament. Comisia ar trebui să fie împuternicită să precizeze, prin intermediul unor acte ***delegate***, sistemele europene de certificare de securitate cibernetică care pot fi utilizate pentru a demonstra***, în cazul produselor cu elemente digitale,*** conformitatea cu cerințele esențiale prevăzute în prezentul regulament. În plus, pentru a evita o sarcină administrativă nejustificată pentru producători, ***nu ar trebui să existe o obligație a*** producătorilor de a efectua o evaluare a conformității de către terți, astfel cum se prevede în prezentul regulament pentru cerințele corespunzătoare***, în cazul în care un certificat de securitate cibernetică a fost emis în conformitate cu aceste sisteme europene de certificare de securitate cibernetică, la un nivel substanțial sau ridicat.***

(39a) Pentru a facilita respectarea prezentului regulament, Comisia ar trebui să actualizeze programul de activitate etapizat la nivelul Uniunii și să solicite ENISA să pregătească propunerile de sisteme care lipsesc în conformitate cu articolul 48 din Regulamentul (UE) 2019/881.

(40) La intrarea în vigoare a actului de punere în aplicare prin care se stabilește [Regulamentul de punere în aplicare (UE) nr. .../... al Comisiei din XXX privind sistemul european de certificare de securitate cibernetică bazat pe criterii comune] (EUCC) care se referă la produsele hardware care fac obiectul prezentului regulament, cum ar fi modulele de securitate hardware și microprocesoarele, Comisia poate preciza, prin intermediul unui act de punere în aplicare, modul în care EUCC oferă o

prezumție de conformitate cu cerințele esențiale menționate în anexa I la prezentul regulament sau cu anumite părți ale acestora. În plus, un astfel de act de punere în aplicare poate preciza modul în care un certificat emis în temeiul EUCC elimină obligația producătorilor de a efectua o evaluare de către terți, solicitată de prezentul regulament pentru cerințele corespunzătoare.

(41) În cazul în care nu se adoptă standarde armonizate sau în cazul în care standardele armonizate nu abordează suficient cerințele esențiale ale prezentului regulament, Comisia ar trebui să poată adopta specificații comune prin intermediul unor acte ***delegate, după ce au fost luate în considerare standardele internaționale***. ***O astfel de opțiune ar trebui privită ca o soluție excepțională de rezervă, atunci când procesul*** de standardizare ***este blocat, atunci când există*** întârzieri nejustificate în stabilirea standardelor armonizate adecvate ***sau atunci când rezultatele nu respectă cererea inițială*** din partea Comisiei. Pentru a facilita evaluarea conformității cu cerințele esențiale prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu specificațiile comune adoptate de Comisie în temeiul prezentului regulament în scopul exprimării specificațiilor tehnice detaliate ale cerințelor respective.

(42) Producătorii ar trebui să elaboreze o declarație de conformitate UE pentru a oferi informațiile necesare în temeiul prezentului regulament cu privire la conformitatea produselor cu elemente digitale cu cerințele esențiale ale prezentului regulament și, după caz, ale altor acte relevante din legislația de armonizare a Uniunii sub incidența cărora intră produsul respectiv. De asemenea, producătorilor li se poate impune, în temeiul altor acte legislative ale Uniunii, obligația de a întocmi o declarație de conformitate UE. Pentru a asigura accesul efectiv la informații în scopul supravegherii pieței, trebuie întocmită o declarație de conformitate UE unică cu privire la respectarea tuturor actelor relevante ale Uniunii. Pentru a reduce sarcina administrativă a operatorilor economici, respectiva declarație de conformitate UE unică trebuie să poată fi un dosar care să cuprindă declarațiile de conformitate individuale relevante.

(43) Marcajul CE, ca indicație a conformității unui produs, este consecința vizibilă a unui întreg proces care cuprinde evaluarea conformității în sens larg. Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului stabilește principiile generale

care reglementează marcajul CE[27]. Prezentul regulament ar trebui să prevadă norme de reglementare a aplicării marcajului CE pe produsele cu elemente digitale. Marcajul CE ar trebui să fie singurul marcaj care garantează faptul că produsele cu elemente digitale sunt conforme cu cerințele prezentului regulament.

(44) Pentru a permite operatorilor economici să demonstreze conformitatea cu cerințele esențiale prevăzute în prezentul regulament și pentru a permite autorităților de supraveghere a pieței să se asigure că produsele cu elemente digitale puse la dispoziție pe piață respectă aceste cerințe, este necesar să se prevadă proceduri de evaluare a conformității. Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului[28] stabilește module pentru procedurile de evaluare a conformității proporțional cu nivelul de risc implicat și cu nivelul de securitate necesar. Pentru a asigura coerența intersectorială și pentru a evita variantele ad-hoc, procedurile de evaluare a conformității adecvate pentru verificarea conformității produselor cu elemente digitale cu cerințele esențiale prevăzute în prezentul regulament s-au bazat pe modulele respective. Procedurile de evaluare a conformității ar trebui să examineze și să verifice atât cerințele referitoare la produse, cât și pe cele referitoare la procese care acoperă întregul ciclu de viață al produselor cu elemente digitale, inclusiv planificarea, proiectarea, dezvoltarea sau producția, testarea și întreținerea produsului.

(45) Ca regulă generală, evaluarea conformității produselor cu elemente digitale ar trebui ***să se bazeze pe riscuri și, în majoritatea cazurilor,*** să fie efectuată de producător pe propria răspundere, urmând procedura bazată pe modulul A din Decizia nr. 768/2008/CE. Producătorul ar trebui să păstreze flexibilitatea de a alege o procedură mai strictă de evaluare a conformității care să implice o parte terță. În cazul în care produsul este clasificat ca produs critic din clasa I, este necesară o asigurare suplimentară pentru a demonstra conformitatea cu cerințele esențiale prevăzute în prezentul regulament. Producătorul ar trebui să aplice standardele armonizate, specificațiile comune sau sistemele de certificare de securitate cibernetică în temeiul

---

27 Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

28 Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului din 9 iulie 2008 privind un cadru comun pentru comercializarea produselor și de abrogare a Deciziei 93/465/CEE a Consiliului (JO L 218, 13.8.2008, p. 82).

Regulamentului (UE) 2019/881 care au fost identificate de Comisie într-un act de punere în aplicare, dacă dorește să efectueze evaluarea conformității pe propria răspundere (modulul A). În cazul în care ***respectivele standarde armonizate, specificații comune sau sisteme de certificare de securitate cibernetică au fost instituite pentru o perioadă minimă de timp care le permite producătorilor să le adopte, iar un anumit producător*** nu ***le*** aplică ▌, producătorul ar trebui să fie supus unei evaluări a conformității care implică o parte terță. Ținând seama de sarcina administrativă a producătorilor și de faptul că securitatea cibernetică joacă un rol important în etapa de proiectare și dezvoltare a produselor cu elemente digitale, fizice sau nu, procedurile de evaluare a conformității bazate pe modulele B+C sau, respectiv, pe modulul H din Decizia nr. 768/2008/CE au fost alese ca fiind cele mai adecvate pentru evaluarea conformității produselor critice cu elemente digitale în mod proporțional și eficace. Producătorul care efectuează evaluarea conformității de către terți poate alege procedura care se potrivește cel mai bine procesului său de proiectare și de producție. Având în vedere riscul și mai mare de securitate cibernetică legat de utilizarea produselor clasificate ca produse critice din clasa II, evaluarea conformității ar trebui să implice întotdeauna o parte terță.

(46) În timp ce crearea de produse fizice cu elemente digitale necesită, de obicei, ca producătorii să depună eforturi substanțiale pe parcursul etapelor de proiectare, dezvoltare și producție, crearea de produse cu elemente digitale sub formă de software se axează aproape exclusiv pe proiectare și dezvoltare, iar etapa de producție joacă un rol minor. Cu toate acestea, în multe cazuri, produsele software trebuie să fie compilate, construite, ambalate, puse la dispoziție pentru descărcare sau copiate pe suport fizic înainte de a fi introduse pe piață. Aceste activități ar trebui considerate activități echivalente cu producția atunci când se aplică modulele relevante de evaluare a conformității pentru a verifica conformitatea produsului cu cerințele esențiale ale prezentului regulament în etapele de proiectare, dezvoltare și producție.

(47) Pentru a efectua evaluarea conformității de către terți a produselor cu elemente digitale, autoritățile naționale de notificare ar trebui să notifice Comisiei și celorlalte state membre organismele de evaluare a conformității, cu condiția ca acestea să respecte un set de cerințe, în special în ceea ce privește independența, competența și absența conflictelor de interese.

(48) Pentru a se asigura un nivel omogen al calității în realizarea evaluării conformității pentru produsele cu elemente digitale, este necesar, de asemenea, să se stabilească cerințele pentru autoritățile de notificare și celelalte organisme implicate în evaluarea, notificarea și monitorizarea organismelor notificate. Sistemul prevăzut în prezentul regulament ar trebui să fie completat de sistemul de acreditare prevăzut în Regulamentul (CE) nr. 765/2008. Întrucât acreditarea este un mijloc esențial de verificare a competenței organismelor de evaluare a conformității, aceasta ar trebui utilizată și în vederea notificării.

(49) Acreditarea transparentă, astfel cum este prevăzută în Regulamentul (CE) nr. 765/2008, care asigură nivelul necesar de încredere în certificatele de conformitate, ar trebui să fie considerată de către autoritățile publice naționale din întreaga Uniune ca fiind modalitatea preferată de a demonstra competența tehnică a organismelor de evaluare a conformității. Cu toate acestea, autoritățile naționale pot considera că dispun de mijloacele adecvate pentru a realiza ele însele această evaluare. În astfel de cazuri, pentru a asigura un nivel adecvat de credibilitate al evaluărilor realizate de alte autorități naționale, acestea ar trebui să prezinte Comisiei și celorlalte state membre documentele necesare pentru a demonstra că organismele de evaluare a conformității care au fost evaluate îndeplinesc cerințele reglementare relevante.

(50) Organismele de evaluare a conformității subcontractează deseori părți ale activităților lor legate de evaluarea conformității sau recurg la o filială. În vederea asigurării nivelului de protecție cerut pentru produsele cu elemente digitale care urmează să fie introduse pe piață, este esențial ca subcontractanții și filialele care efectuează procedura de evaluare a conformității să îndeplinească aceleași cerințe ca organismele notificate în ceea ce privește executarea atribuțiilor de evaluare a conformității.

(51) Notificarea unui organism de evaluare a conformității ar trebui trimisă de autoritatea de notificare Comisiei și celorlalte state membre prin intermediul sistemului informațional NANDO (*New Approach Notified and Designated Organisations* – Noua abordare privind organizațiile notificate și desemnate). NANDO este instrumentul de notificare electronică dezvoltat și gestionat de Comisie, în care se găsește o listă a tuturor organismelor notificate.

(52) Întrucât organismele notificate își pot oferi serviciile în întreaga Uniune, este adecvat să se acorde celorlalte state membre și Comisiei posibilitatea de a ridica obiecții cu

privire la un organism notificat. De aceea este important să se acorde o perioadă de timp în care orice îndoieli sau preocupări privind competența organismelor de evaluare a conformității să poată fi clarificate, înainte ca acestea să înceapă să funcționeze ca organisme notificate.

(53) Din rațiuni de competitivitate, este fundamental ca organismele notificate să aplice procedurile de evaluare a conformității fără a crea o sarcină inutilă pentru operatorii economici***, în special pentru microîntreprinderi și pentru întreprinderile mici și mijlocii***. ***În acest sens, statele membre, cu sprijinul Comisiei, ar trebui să se asigure că există o disponibilitate adecvată a profesioniștilor calificați, pentru a garanta faptul că organismele notificate își pot desfășura activitățile în mod eficient, reducând astfel la minimum posibilele obstacole, evitând blocajele și facilitând respectarea prezentului regulament de către operatorii economici.*** Din același motiv și pentru a asigura tratamentul egal al operatorilor economici, este necesară asigurarea coerenței în aplicarea tehnică a procedurilor de evaluare a conformității. Acest lucru ar trebui realizat cel mai bine printr-o coordonare și o cooperare adecvată între organismele notificate.

(53a) Cu scopul de a îmbunătăți eficiența și transparența, statele membre ar trebui să asigure, înainte de data aplicării prezentului regulament, faptul că în Uniune există un număr suficient de organisme notificate pentru efectuarea de evaluări ale conformității. Comisia ar trebui să monitorizeze evoluțiile pieței și să sprijine statele membre în acest demers, pentru a evita blocajele și obstacolele în calea intrării pe piață.

(54) Supravegherea pieței este un instrument esențial, deoarece asigură aplicarea corespunzătoare și uniformă a legislației Uniunii. Prin urmare, este necesară instituirea unui cadru juridic în care supravegherea pieței să poată fi realizată în mod adecvat. Normele privind supravegherea pieței Uniunii și controlul produselor care intră pe piața Uniunii prevăzute în Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[29] se aplică produselor cu elemente digitale care fac obiectul prezentului regulament.

---

[29] Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a

(55) În conformitate cu Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru respectiv. Prezentul regulament nu ar trebui să împiedice statele membre să aleagă autoritățile competente pentru îndeplinirea sarcinilor respective. Fiecare stat membru ar trebui să desemneze una sau mai multe autorități de supraveghere a pieței pe teritoriul său. Statele membre pot alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile naționale competente menționate ***în*** Directiva ***(UE) 2022/2555*** sau autoritățile naționale desemnate de certificare a securității cibernetice menționate la articolul 58 din Regulamentul (UE) 2019/881. Operatorii economici ar trebui să coopereze pe deplin cu autoritățile de supraveghere a pieței și cu alte autorități competente. Fiecare stat membru ar trebui să informeze Comisia și celelalte state membre cu privire la autoritățile sale de supraveghere a pieței și la domeniile de competență ale fiecăreia dintre aceste autorități și ar trebui să asigure resursele și competențele necesare pentru îndeplinirea sarcinilor de supraveghere legate de prezentul regulament. În conformitate cu articolul 10 alineatele (2) și (3) din Regulamentul (UE) 2019/1020, fiecare stat membru ar trebui să numească un birou unic de legătură care ar trebui să fie responsabil, printre altele, de reprezentarea poziției coordonate a autorităților de supraveghere a pieței și de acordarea de asistență pentru cooperarea dintre autoritățile de supraveghere a pieței din diferite state membre.

(56) Ar trebui instituit un grup specific de cooperare administrativă (ADCO) pentru ***reziliența cibernetică a produselor cu elemente digitale, astfel încât să se asigure*** aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO ar trebui să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate și, dacă este cazul, din reprezentanți ai birourilor unice de legătură. Comisia ar trebui să sprijine și să încurajeze cooperarea dintre autoritățile de supraveghere a pieței prin intermediul Rețelei Uniunii pentru conformitatea produselor, instituită în temeiul articolului 29 din Regulamentul (UE) 2019/1020 și alcătuită din reprezentanți ai fiecărui stat membru, inclusiv un reprezentant al fiecărui birou unic de legătură menționat la articolul 10 din

---

Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011 (JO L 169, 25.6.2019, p. 1).

Regulamentul (UE) 2019/1020 și un expert național opțional, președinții ADCO și reprezentanți ai Comisiei. Comisia ar trebui să participe la reuniunile rețelei, ale subgrupurilor sale și ale ADCO respectiv. Aceasta ar trebui, de asemenea, să asiste ADCO prin intermediul unui secretariat executiv care să ofere sprijin tehnic și logistic.

(57) Pentru a asigura măsuri prompte, proporționale și eficace în legătură cu produsele cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică, ar trebui să se prevadă o procedură de salvgardare la nivelul Uniunii prin care părțile interesate să fie informate cu privire la măsurile preconizate referitoare la astfel de produse. De asemenea, această procedură ar trebui să le permită autorităților de supraveghere a pieței ca, în cooperare cu operatorii economici relevanți, să acționeze din timp, dacă este necesar. În cazul în care statele membre și Comisia sunt de acord cu privire la justificarea unei măsuri luate de un stat membru, nu ar trebui să mai fie necesară intervenția ulterioară a Comisiei, cu excepția cazurilor în care neconformitatea poate fi atribuită unor deficiențe ale unui standard armonizat.

(58) În anumite cazuri, un produs cu elemente digitale care respectă prezentul regulament poate prezenta totuși un risc semnificativ în materie de securitate cibernetică sau poate prezenta un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin utilizarea unui sistem electronic de informații de către entitățile esențiale de tipul celor menționate în ▌Directiva ***(UE) 2022/2555*** sau în ceea ce privește alte aspecte ale protecției interesului public. Prin urmare, este necesar să se stabilească norme care să asigure atenuarea acestor riscuri. În consecință, autoritățile de supraveghere a pieței ar trebui să ia măsuri pentru a solicita operatorului economic să se asigure că produsul nu mai prezintă riscul respectiv, să îl recheme sau să îl retragă, în funcție de risc. De îndată ce o autoritate de supraveghere a pieței restricționează sau interzice libera circulație a unui produs în acest mod, statul membru în cauză ar trebui să informeze fără întârziere Comisia și celelalte state membre cu privire la măsurile provizorii, justificându-și și motivându-și decizia. Atunci când o autoritate de supraveghere a pieței adoptă astfel de măsuri în ceea ce privește produsele care prezintă un risc, Comisia ar trebui să inițieze fără întârziere consultări cu statele membre și cu operatorul economic sau operatorii

economici în cauză și ar trebui să evalueze măsura națională. Pe baza rezultatelor acestei evaluări, Comisia ar trebui să decidă dacă măsura națională este sau nu justificată. Comisia ar trebui să adreseze decizia sa tuturor statelor membre și să o comunice imediat acestora și operatorului (operatorilor) economic(i) în cauză. Dacă măsura este considerată justificată, Comisia poate avea în vedere, de asemenea, adoptarea unor propuneri de revizuire a legislației respective a Uniunii.

(59) În cazul produselor cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică și dacă există motive să se creadă că acestea nu sunt conforme cu prezentul regulament sau în cazul produselor care sunt conforme cu prezentul regulament, dar care prezintă alte riscuri importante, precum riscuri la adresa sănătății sau siguranței persoanelor, a drepturilor fundamentale sau a furnizării de servicii de către entități esențiale de tipul celor menționate în ▌Directiva ***(UE) 2022/2555***, Comisia poate solicita ENISA să efectueze o evaluare. Pe baza evaluării respective, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea produselor respective, într-un termen rezonabil, proporțional cu natura riscului. Comisia poate recurge la o astfel de intervenție numai în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne și numai în cazul în care autoritățile de supraveghere nu au luat măsuri eficace pentru remedierea situației. Astfel de circumstanțe excepționale pot fi situații de urgență în care, de exemplu, un produs neconform este pus la dispoziție pe scară largă de către producător în mai multe state membre, este utilizat și în sectoare-cheie de către entități ***care intră în domeniul de aplicare a*** Directivei ***(UE) 2022/2555***, acesta conținând vulnerabilități cunoscute care sunt exploatate de actori rău-intenționați și pentru care producătorul nu oferă corecții disponibile. Comisia poate interveni în astfel de situații de urgență numai pe durata circumstanțelor excepționale și dacă neconformitatea cu prezentul regulament sau riscurile importante prezentate persistă.

(60) În cazurile în care există indicii ale unei neconformități cu prezentul regulament în mai multe state membre, autoritățile de supraveghere a pieței ar trebui să poată desfășura activități comune cu alte autorități, în vederea verificării conformității și a identificării riscurilor de securitate cibernetică ale produselor cu elemente digitale.

(61) Acțiunile de control coordonate simultane („acțiuni de verificare”) sunt acțiuni specifice de asigurare a respectării legislației întreprinse de autoritățile de supraveghere a pieței care pot spori și mai mult securitatea produselor. În special, ar trebui efectuate acțiuni de verificare atunci când tendințele pieței, reclamațiile consumatorilor sau alte indicii sugerează că anumite categorii de produse sunt adesea considerate ca prezentând riscuri de securitate cibernetică. ENISA ar trebui să prezinte autorităților de supraveghere a pieței propuneri de categorii de produse pentru care ***ar trebui*** organizate acțiuni de verificare, bazate, printre altele, pe notificările pe care le primește cu privire la vulnerabilități ale produselor și la incidente. ***Comisia ar trebui, de asemenea, să coordoneze autoritățile de supraveghere a pieței în cadrul inspecțiilor periodice ale produselor cu elemente digitale care ar putea prezenta un risc de securitate pentru Uniune, inclusiv având în vedere factorul de risc fără caracter tehnic.***

(62) Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul 290 din tratat pentru a actualiza lista produselor critice din anexa III și pentru a preciza definițiile acestor categorii de produse. Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv pentru a identifica produsele cu elemente digitale care fac obiectul altor norme ale Uniunii care asigură același nivel de protecție ca prezentul regulament, specificând dacă va fi necesară o limitare sau o excludere din domeniul de aplicare al prezentului regulament, precum și domeniul de aplicare al limitării respective, dacă este cazul. De asemenea, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv în ceea ce privește ***specificarea sistemelor europene de certificare a securității cibernetice adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu părți ale acestora prevăzute în anexa I la prezentul regulament,*** eventuala impunere a certificării anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor referitoare la caracterul critic prevăzute în prezentul regulament, precum și în ceea ce privește precizarea conținutului minim al declarației de conformitate UE și completarea elementelor care trebuie incluse în documentația tehnică. ***De asemenea, Comisiei ar trebui să îi fie delegată competența de a adopta acte pentru a specifica formatul și elementele listei materialelor software și pentru a preciza în detaliu***

formatul și procedura pentru notificările transmise ENISA de către producători cu privire la vulnerabilitățile exploatate în mod activ și la incidentele semnificative. Dacă este necesar, Comisia ar trebui să fie împuternicită să adopte acte delegate pentru a adopta specificații comune cu privire la cerințele esențiale prevăzute în anexa I. Este deosebit de important ca, în cursul activității sale pregătitoare, Comisia să organizeze consultări corespunzătoare, inclusiv la nivel de experți, și ca aceste consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016[30]. 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. ***În scopul elaborării de acte delegate în temeiul prezentului regulament, Comisia ar trebui să consulte Grupul de experți privind reziliența cibernetică. Comisia ar trebui, de asemenea, să poarte un dialog structural periodic cu operatorii economici și să organizeze consultări publice, printre altele în scopul de a evalua domeniul de aplicare al prezentului regulament și dacă anumite categorii de produse ar trebui incluse sau excluse.***

(63) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să îi fie conferite competențe de executare: ▌ pentru a stabili specificații tehnice pentru ***sistemele de etichetare, inclusiv pentru etichetele armonizate,*** pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale și mecanisme de promovare a utilizării acestora, pentru a decide măsuri corective sau restrictive la nivelul Uniunii în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne. Respectivele competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[31].

(64) Pentru a asigura o cooperare bazată pe încredere și constructivă a autorităților de supraveghere a pieței de la nivelul Uniunii și de la nivel național, toate părțile implicate

---

30 JO L 123, 12.5.2016, p. 1.

31 Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

în aplicarea prezentului regulament ar trebui să respecte confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor lor.

(65) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezentul regulament, fiecare autoritate de supraveghere a pieței ar trebui să aibă competența de a impune sau de a solicita impunerea de amenzi administrative. Prin urmare, ar trebui stabilite niveluri maxime ale amenzilor administrative, care să fie prevăzute în legislația națională, pentru nerespectarea obligațiilor prevăzute în prezentul regulament. Atunci când se decide cuantumul amenzii administrative în fiecare caz în parte, ar trebui să se țină seama de toate circumstanțele relevante ale situației specifice și, cel puțin, de cele stabilite în mod explicit în prezentul regulament, inclusiv dacă producătorul este ***o microîntreprindere, o întreprindere mică sau mijlocie sau o întreprindere nou-înființată și dacă*** alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator pentru încălcări similare. Aceste circumstanțe pot fi fie agravante, în situațiile în care încălcarea săvârșită de același operator persistă pe teritoriul altor state membre decât cel în care s-a aplicat deja o amendă administrativă, fie atenuante, pentru a se asigura că orice altă amendă administrativă avută în vedere de o altă autoritate de supraveghere a pieței pentru același operator economic sau pentru același tip de încălcare ia deja în considerare, împreună cu alte circumstanțe specifice relevante, o sancțiune impusă într-un alt stat membru și cuantumul acesteia. În toate aceste cazuri, amenda administrativă cumulată care ar putea fi aplicată de autoritățile de supraveghere a pieței din mai multe state membre aceluiași operator economic pentru același tip de încălcare ar trebui să asigure respectarea principiului proporționalității.

(66) În cazul în care se impun amenzi administrative unor persoane care nu sunt întreprinderi, autoritatea competentă ar trebui să țină seama de nivelul general al veniturilor din statul membru respectiv, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii. Competența de a stabili dacă și în ce măsură autoritățile publice ar trebui să facă obiectul unor amenzi administrative ar trebui să le revină statelor membre.

(66a) Veniturile generate din plata sancțiunilor ar trebui utilizate pentru a consolida nivelul de securitate cibernetică din Uniune, inclusiv prin dezvoltarea capacităților și a competențelor legate de securitatea cibernetică, prin îmbunătățirea rezilienței

cibernetice a operatorilor economici, în special a microîntreprinderilor și a întreprinderilor mici și mijlocii și, în general, prin informarea publicului cu privire la aspectele legate de securitatea cibernetică.

(67) În relațiile sale cu țările terțe, UE urmărește, în special, să promoveze comerțul internațional cu produsele reglementate. Există o gamă largă de măsuri care pot fi aplicate pentru a facilita comerțul, inclusiv mai multe instrumente juridice, cum ar fi acordurile bilaterale (interguvernamentale) de recunoaștere reciprocă (ARR) pentru evaluarea conformității și marcarea produselor reglementate. Acordurile de recunoaștere reciprocă sunt încheiate între Uniune și țările terțe care beneficiază de un nivel de dezvoltare tehnică comparabil și care au o abordare compatibilă privind evaluarea conformității. Acordurile se bazează pe acceptarea reciprocă a certificatelor, a mărcilor de conformitate și a rapoartelor de testare emise de organismele de evaluare a conformității ale uneia dintre cele două părți, în conformitate cu legislația celeilalte părți. În prezent sunt în vigoare acorduri de recunoaștere reciprocă pentru mai multe țări. Acordurile respective sunt încheiate într-o serie de sectoare specifice, care pot varia de la o țară la alta. Pentru a facilita și mai mult comerțul și având în vedere că lanțurile de aprovizionare ale produselor cu elemente digitale sunt globale, Uniunea poate încheia, în conformitate cu articolul 218 din TFUE, acorduri de recunoaștere reciprocă referitoare la evaluarea conformității pentru produsele reglementate de prezentul regulament. Cooperarea cu țările partenere este, de asemenea, importantă pentru consolidarea rezilienței cibernetice la nivel mondial, deoarece, pe termen lung, acest lucru va contribui la consolidarea cadrului de securitate cibernetică atât în interiorul, cât și în afara UE.

(68) Comisia ar trebui să reexamineze periodic prezentul regulament, consultându-se cu ***Grupul de experți și cu alte*** părți interesate, în special pentru a stabili dacă este necesară efectuarea unor modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață.

(69) Operatorilor economici ar trebui să li se acorde suficient timp pentru a se adapta la cerințele prevăzute de prezentul regulament. Prezentul regulament ar trebui să se aplice la [***36*** de luni] de la intrarea sa în vigoare, cu excepția obligațiilor de raportare privind vulnerabilitățile exploatate activ și incidentele, care ar trebui să se aplice la [***18*** luni] de la intrarea în vigoare a regulamentului.

(69a) Prezentul regulament va genera costuri suplimentare pentru microîntreprinderi și pentru întreprinderile mici și mijlocii, inclusiv pentru întreprinderile nou-înființate. Pentru a sprijini aceste întreprinderi, Comisia ar trebui să stabilească un sprijin financiar și tehnic care să le permită acestora să contribuie la creșterea economiei europene și la peisajul european al securității cibernetice, inclusiv prin raționalizarea sprijinului financiar din programul Europa digitală și din alte programe relevante ale Uniunii, precum și prin sprijinirea întreprinderilor și organizațiilor din sectorul public prin centrele europene de inovare digitală. În plus, statele membre ar trebui să ia în considerare toate acțiunile complementare posibile menite să ofere orientări și sprijin microîntreprinderilor și întreprinderilor mici și mijlocii, inclusiv prin înființarea de spații de testare în materie de reglementare, de centre de securitate cibernetică și de acceleratoare pentru întreprinderile nou-înființate.

(70) Deoarece obiectivul prezentului regulament nu pot fi realizate în mod satisfăcător de către statele membre, dar, având în vedere efectele acțiunii, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este definit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este stabilit la același articol, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului respectiv.

(71) 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[32] și a emis un aviz la ***9 noiembrie 2022***[33].

(71a) Comisia ar trebui să modifice fișa financiară legislativă care însoțește prezentul regulament, punând la dispoziția ENISA nouă posturi suplimentare echivalent normă întreagă și credite suplimentare corespunzătoare pentru a-și îndeplini sarcinile suplimentare prevăzute în prezentul regulament,

---

[32] 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).

[33] ***JO C 452, 29.11.2022, p. 23.***

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiectul

Prezentul regulament stabilește:

(a) norme pentru ***punerea la dispoziție pe piață*** a produselor cu elemente digitale în vederea asigurării securității cibernetice a acestor produse;

(b) cerințe esențiale pentru proiectarea, dezvoltarea și producția de produse cu elemente digitale, precum și obligațiile operatorilor economici în legătură cu aceste produse în ceea ce privește securitatea cibernetică;

(c) cerințe esențiale pentru procesele de gestionare a vulnerabilităților instituite de producători pentru a asigura securitatea cibernetică a produselor cu elemente digitale pe parcursul întregului ciclu de viață, precum și obligațiile operatorilor economici în legătură cu aceste procese;

(d) norme privind ***monitorizarea,*** supravegherea pieței și asigurarea respectării normelor și cerințelor menționate mai sus.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică produselor cu elemente digitale ***puse la dispoziție pe piață care pot avea*** o conexiune de date ▌ directă sau indirectă la un dispozitiv sau la o rețea.

(2) Prezentul regulament nu se aplică produselor cu elemente digitale cărora li se aplică următoarele acte ***legislative*** ale Uniunii:

(a) Regulamentul (UE) 2017/745;

(b) Regulamentul (UE) 2017/746;

(c) Regulamentul (UE) 2019/2144.

(3) Prezentul regulament nu se aplică produselor cu elemente digitale care au fost certificate în conformitate cu Regulamentul (UE) 2018/1139.

(3a) Prezentul regulament se aplică software-ului liber și cu sursă deschisă numai în cazul în care un astfel de software este pus la dispoziție pe piață în cursul unei activități comerciale.

(4) Aplicarea prezentului regulament în cazul unor produse cu elemente digitale care fac obiectul altor norme ale Uniunii care stabilesc cerințe care abordează toate sau unele dintre riscurile acoperite de cerințele esențiale prevăzute în anexa I poate fi limitată sau exclusă dacă:

(a) această limitare sau excludere este în concordanță cu cadrul general de reglementare aplicabil produselor respective și dacă

(b) normele sectoriale asigură același nivel de protecție ca cel prevăzut de prezentul regulament.

Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a modifica prezentul regulament, specificând dacă o astfel de limitare sau excludere este necesară, produsele și normele în cauză, precum și domeniul de aplicare al limitării, dacă este cazul.

(4a) Prezentul regulament nu se aplică pieselor de schimb care sunt fabricate exclusiv pentru a înlocui piese identice și care sunt furnizate de producătorul produselor originale cu elemente digitale.

(5) Prezentul regulament nu se aplică produselor cu elemente digitale dezvoltate exclusiv în scopuri militare sau de securitate națională sau produselor proiectate în mod specific pentru prelucrarea informațiilor clasificate.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „produs cu elemente digitale” înseamnă orice produs software sau hardware și soluțiile sale de prelucrare de date la distanță, inclusiv componentele software sau hardware care urmează să fie introduse pe piață separat;

2. „prelucrare de date la distanță” înseamnă orice prelucrare de date la distanță pentru care software-ul este proiectat și dezvoltat de producător ***sau în numele*** producătorului și a cărei absență ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții;

3. „produs critic cu elemente digitale” înseamnă un produs cu elemente digitale care prezintă un risc de securitate cibernetică în conformitate cu criteriile prevăzute la articolul 6 alineatul (2) și a cărui funcționalitate de bază este prevăzută în anexa III;

4. „produs deosebit de critic cu elemente digitale” înseamnă un produs cu elemente digitale care prezintă un risc de securitate cibernetică în conformitate cu criteriile prevăzute la articolul 6 alineatul (5);

4a. „securitate cibernetică” înseamnă securitate cibernetică astfel cum este definită la articolul 2 punctul 1 din Regulamentul (UE) 2019/881;

5. „tehnologie operațională” înseamnă sisteme sau dispozitive digitale programabile care interacționează cu mediul fizic sau gestionează dispozitive care interacționează cu mediul fizic;

6. „software” înseamnă acea parte a unui sistem informatic electronic care constă într-un cod informatic;

7. „hardware” înseamnă un sistem informatic electronic fizic, sau anumite părți ale acestuia, capabil să prelucreze, să stocheze sau să transmită date digitale;

8. „componentă” înseamnă un software sau un hardware destinat integrării într-un sistem informatic electronic;

9. „sistem informatic electronic” înseamnă orice sistem, incluzând echipamentele electrice sau electronice, capabil să prelucreze, să stocheze sau să transmită date digitale;

10. „conexiune logică” înseamnă o reprezentare virtuală a unei conexiuni de date implementată printr-o interfață software;

11. „conexiune fizică” înseamnă orice conexiune între sisteme informatice electronice sau componente implementată prin mijloace fizice, inclusiv prin interfețe electrice sau mecanice, fire sau unde radio;

12. „conexiune indirectă” înseamnă o conexiune la un dispozitiv sau la o rețea care nu are loc direct, ci ca parte a unui sistem mai mare care este conectabil direct la un astfel de dispozitiv sau rețea;

13. „privilegiu” înseamnă un drept de acces acordat anumitor utilizatori sau programe pentru a efectua operațiuni relevante pentru securitate în cadrul unui sistem informatic electronic;

14. „privilegiu extins” înseamnă un drept de acces acordat anumitor utilizatori sau programe pentru a efectua un set extins de operațiuni relevante pentru securitate în cadrul unui sistem informatic electronic care, dacă este utilizat în mod necorespunzător sau este compromis, ar putea permite unui actor răuvoitor să obțină un acces mai larg la resursele unui sistem sau ale unei organizații;

15. „punct terminal” înseamnă orice dispozitiv care este conectat la o rețea și servește ca punct de intrare în rețeaua respectivă;

16. „resurse de rețea sau informatice” înseamnă funcționalități de date sau hardware sau software care sunt accesibile fie local, fie prin intermediul unei rețele sau al unui alt dispozitiv conectat;

17. „operator economic” înseamnă producătorul, reprezentantul autorizat, importatorul, distribuitorul sau orice altă persoană fizică sau juridică care face obiectul obligațiilor prevăzute în prezentul regulament;

18. „producător” înseamnă orice persoană fizică sau juridică care dezvoltă sau fabrică produse cu elemente digitale sau pentru care sunt proiectate, dezvoltate sau fabricate produsele cu elemente digitale și care le comercializează sub numele sau marca sa, contra cost***, pentru monetizare*** sau gratuit;

19. „reprezentant autorizat” înseamnă orice persoană fizică sau juridică stabilită în Uniune care a primit un mandat scris din partea unui producător pentru a acționa în numele acestuia în legătură cu sarcini specifice;

20. „importator” înseamnă orice persoană fizică sau juridică stabilită în Uniune care introduce pe piață un produs cu elemente digitale care poartă numele sau marca unei persoane fizice sau juridice stabilite în afara Uniunii;

21. „distribuitor” înseamnă orice persoană fizică sau juridică din lanțul de aprovizionare, alta decât producătorul sau importatorul, care pune la dispoziție un produs cu elemente digitale pe piața Uniunii fără a-i afecta proprietățile;

21a. „microîntreprinderi”, „întreprinderi mici” și „întreprinderi mijlocii” înseamnă microîntreprinderi, întreprinderi mici și întreprinderi mijlocii astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei[34];

21b. „consumator” înseamnă orice persoană fizică care, în circumstanțele prevăzute de prezentul regulament, acționează în scopuri care nu se încadrează în activitatea sa comercială, industrială, artizanală sau profesională;

21c. „perioadă de sprijin” înseamnă perioada în care producătorul se asigură că vulnerabilitățile produsului cu elemente digitale sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 2;

22. „introducere pe piață” înseamnă punerea la dispoziție pentru prima oară a unui produs cu elemente digitale pe piața Uniunii;

23. „punere la dispoziție pe piață” înseamnă orice furnizare a unui produs cu elemente digitale pentru distribuție sau utilizare pe piața Uniunii, în cadrul unei activități comerciale, contra cost sau gratuit;

24. „scop preconizat” înseamnă utilizarea care a fost preconizată de către producător a unui produs cu elemente digitale, inclusiv contextul și condițiile specifice de utilizare, astfel cum se specifică în informațiile oferite de furnizor în instrucțiunile de utilizare, în materialele și în declarațiile promoționale sau de vânzare, precum și în documentația tehnică;

25. „utilizare previzibilă în mod rezonabil” înseamnă o utilizare care nu este neapărat scopul preconizat specificat de producător în instrucțiunile de utilizare, în materialele și în declarațiile promoționale sau de vânzare, precum și în documentația tehnică, dar

---

34 ***Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii [notificată cu numărul C(2003) 1422] (JO L 124, 20.5.2003, p. 36).***

care este probabil să rezulte din comportamentul uman sau din operațiuni tehnice sau interacțiuni previzibile în mod rezonabil;

26. „utilizare necorespunzătoare previzibilă în mod rezonabil” înseamnă utilizarea unui produs cu elemente digitale într-un mod care nu este conform cu scopul său preconizat, dar care poate rezulta din comportamentul uman sau interacțiunea previzibilă în mod rezonabil cu alte sisteme;

27. „autoritate de notificare” înseamnă autoritatea națională responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora;

28. „evaluare a conformității” înseamnă procesul de verificare a îndeplinirii cerințelor esențiale prevăzute în anexa I;

29. „organism de evaluare a conformității” înseamnă un organism definit la articolul 2 alineatul (13) din Regulamentul (UE) nr. 765/2008;

30. „organism notificat” înseamnă un organism de evaluare a conformității desemnat în conformitate cu articolul 33 din prezentul regulament și cu alte acte relevante din legislația de armonizare a Uniunii;

31. „modificare substanțială” înseamnă o modificare a produsului cu elemente digitale în urma introducerii sale pe piață care afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 sau care are ca rezultat o modificare a utilizării preconizate pentru care a fost evaluat respectivul produs cu elemente digitale***, cu excepția actualizărilor necesare care vizează atenuarea vulnerabilităților***;

32. „marcaj CE” înseamnă un marcaj prin care un producător indică faptul că un produs cu elemente digitale și procesele instituite de producător sunt conforme cu cerințele esențiale prevăzute în anexa I și în alte acte legislative aplicabile ale Uniunii care armonizează condițiile de comercializare a produselor („legislația de armonizare a Uniunii”) care prevăd aplicarea acestuia;

33. „autoritate de supraveghere a pieței” înseamnă autoritatea definită la articolul 3 punctul 4 din Regulamentul (UE) 2019/1020;

34. „standard armonizat” înseamnă un standard armonizat astfel cum este definit la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012;

34a. „standard internațional” înseamnă un standard internațional astfel cum este definit la articolul 2 punctul 1 litera (a) din Regulamentul (UE) nr. 1025/2012;

35. „risc ▌ ” înseamnă un risc astfel cum este definit la articolul ***6 punctul 9*** din Directiva ***(UE) 2022/2555***;

36. „risc semnificativ în materie de securitate cibernetică” înseamnă un risc de securitate cibernetică despre care, pe baza caracteristicilor sale tehnice, se poate presupune că are o probabilitate ridicată de producere a unui incident care ar putea conduce la un impact negativ grav, inclusiv prin cauzarea unor perturbări sau a unor prejudicii materiale sau morale considerabile;

37. „listă a materialelor software” ***sau „SBOM”*** înseamnă o înregistrare oficială care conține detalii și relații din cadrul lanțului de aprovizionare ale componentelor incluse în elementele software ale unui produs cu elemente digitale;

38. „vulnerabilitate” înseamnă vulnerabilitate astfel cum este definită la articolul ***6 punctul 15*** din Directiva ***(UE) 2022/2555***;

39. „vulnerabilitate exploatată activ” înseamnă o vulnerabilitate pentru care există dovezi fiabile că executarea unui cod dăunător a fost efectuată de un actor pe un sistem fără permisiunea proprietarului sistemului;

39a. „incident” înseamnă un incident astfel cum este definit la articolul 6 punctul 6 din Directiva (UE) 2022/2555;

39b. „incident evitat la limită” înseamnă un incident evitat la limită astfel cum este definit la articolul 6 punctul 5 din Directiva (UE) 2022/2555;

39c. „amenințare cibernetică” înseamnă o amenințare cibernetică astfel cum este definită la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;40. „date cu caracter personal” înseamnă date cu caracter personal astfel cum sunt definite la articolul 4 ***punctul*** 1 din Regulamentul (UE) 2016/679;

Articolul 4

Libera circulație

(1) Statele membre nu împiedică, în ceea ce privește aspectele reglementate de prezentul regulament, punerea la dispoziție pe piață a produselor cu elemente digitale care sunt conforme cu prezentul regulament.

(2) Statele membre nu împiedică prezentarea și utilizarea unui produs ***prototip*** cu elemente digitale care nu este conform cu prezentul regulament***, cu condiția ca disponibilitatea acestui produs să fie limitată în timp și ca zonă geografică, iar acesta să fie furnizat exclusiv pentru testare și, dacă este posibil, să se indice în mod clar printr-un semn vizibil că produsul nu este conform.***

(3) Statele membre nu împiedică punerea la dispoziție ***în mod gratuit*** a unui software nefinalizat care nu este conform cu prezentul regulament, cu condiția ca software-ul respectiv să fie pus la dispoziție numai pentru o perioadă limitată necesară pentru testare și să se indice în mod clar printr-un un semn vizibil că acesta nu este conform cu prezentul regulament și nu va fi disponibil pe piață în alte scopuri decât testarea.

(3a) Statele membre, dacă este cazul cu sprijinul ENISA, pot stabili medii de testare controlate pentru produse inovatoare cu scopul de a facilita dezvoltarea lor. În acest context, se acordă un sprijin special microîntreprinderilor, întreprinderilor mici și mijlocii, inclusiv întreprinderilor nou-înființate.

Articolul 5

Cerințe pentru produsele cu elemente digitale

Produsele cu elemente digitale sunt puse la dispoziție pe piață numai în cazul în care:

1. îndeplinesc cerințele esențiale prevăzute în anexa I secțiunea 1, cu condiția să fie instalate, întreținute, utilizate în mod corespunzător pentru scopul preconizat sau în condiții care pot fi prevăzute în mod rezonabil și, după caz, ***dotate cu actualizările de securitate și de funcționalitate necesare*** și

2. procesele instituite de producător respectă cerințele esențiale prevăzute în anexa I secțiunea 2.

Articolul 6

Produsele critice cu elemente digitale

(1) Produsele cu elemente digitale care aparțin unei categorii enumerate în anexa III sunt considerate produse critice cu elemente digitale. Produsele care au funcționalitatea de bază a unei categorii enumerate în anexa III la prezentul regulament trebuie considerate ca făcând parte din categoria respectivă. Categoriile de produse critice cu elemente digitale se împart în clasele I și II, astfel cum sunt prevăzute în anexa III, în funcție de nivelul riscului de securitate cibernetică aferent acestor produse.

Integrarea unui produs cu o clasă de criticalitate superioară nu modifică nivelul de criticalitate al produsului în care este integrat.

(2) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a modifica anexa III prin includerea în lista categoriilor de produse critice cu elemente digitale a unei noi categorii sau prin retragerea unei categorii existente din lista respectivă. ***Primul astfel de act de delegat se adoptă nu mai devreme de doi ani de la data intrării în vigoare a prezentului regulament. Orice act delegat ulterior poate fi adoptat cel mai devreme după doi ani.*** Atunci când evaluează necesitatea de a modifica lista din anexa III, Comisia ține seama de nivelul de risc de securitate cibernetică aferent respectivei categorii de produse cu elemente digitale. La determinarea nivelului riscului de securitate cibernetică, se ține seama de unul sau mai multe dintre următoarele criterii:

(a) funcționalitatea legată de securitatea cibernetică a produsului cu elemente digitale și dacă produsul cu elemente digitale are cel puțin unul dintre următoarele atribute:

(i) este proiectat pentru a funcționa cu privilegii extinse sau pentru a gestiona privilegii;

(ii) are acces direct sau privilegiat la resurse de rețea sau informatice;

(iii) este proiectat pentru a controla accesul la tehnologia datelor sau la tehnologia operațională;

(iv) îndeplinește o funcție esențială pentru încredere, în special funcții de securitate, cum ar fi controlul rețelei, securitatea punctelor terminale și protecția rețelei;

(b) utilizarea preconizată în medii sensibile, inclusiv în medii industriale sau de către entități esențiale de tipul celor menționate ***la articolul 3 din*** Directiva ***(UE) 2022/2555***;

(c) utilizarea preconizată constând în îndeplinirea unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal;

(d) amploarea potențială a unui impact negativ, în special în ceea ce privește intensitatea și capacitatea sa de a afecta un număr mare de persoane;

(e) măsura în care utilizarea produselor cu elemente digitale a cauzat deja perturbări sau prejudicii materiale sau morale sau a generat preocupări semnificative în legătură cu materializarea unui impact negativ.

(3) Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea definițiilor categoriilor de produse din clasa I și clasa II, astfel cum sunt prevăzute în anexa III. Aceste acte delegate se adoptă până la... [▌ ***6*** de luni de la data intrării în vigoare a prezentului regulament].

(4) Produsele critice cu elemente digitale fac obiectul procedurilor de evaluare a conformității menționate la articolul 24 alineatele (2) și (3).

În cazul în care o nouă categorie de produse critice cu elemente digitale este adăugată la clasele I sau II din anexa III prin intermediul unui act delegat în temeiul alineatului (2) din prezentul articol, aceasta face obiectul procedurilor relevante de evaluare a conformității menționate la articolul 24 alineatul (2) și alineatul (3) din prezentul regulament în termen de 12 luni de la data adoptării actului delegat în cauză.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea categoriilor de produse deosebit de critice cu elemente digitale, pentru care producătorii au obligația de a obține un certificat european de securitate cibernetică în cadrul unui sistem european de certificare de securitate cibernetică ***la un nivel de asigurare „ridicat”*** în temeiul Regulamentului (UE) 2019/881 pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I sau cu anumite părți ale acestora. ***Obligația de a obține un certificat european de securitate cibernetică se aplică la 12 luni de la adoptarea***

actului delegat relevant. Atunci când stabilește aceste categorii de produse deosebit de critice cu elemente digitale, Comisia ține seama de nivelul de risc de securitate cibernetică aferent categoriei respective de produse cu elemente digitale, având în vedere unul sau mai multe dintre criteriile enumerate la alineatul (2), precum și evaluând dacă respectiva categorie de produse:

(a) este utilizată sau dacă se bazează pe ea entitățile esențiale de tipul celor menționate la articolul 3 din Directiva ▌(UE) 2022/2555 sau dacă aceasta va avea o potențială semnificație viitoare pentru activitățile entităților respective; sau

(b) este relevantă pentru reziliența întregului lanț de aprovizionare al produselor cu elemente digitale împotriva evenimentelor perturbatoare.

(5a) Comisia este împuternicită să adopte actele delegate menționate la alineatul (5) din prezentul articol nu mai devreme de 12 luni de la adoptarea sistemului european de certificare de securitate cibernetică relevant în temeiul Regulamentului (UE) 2019/881.

Articolul 6a

Grupul de experți privind reziliența cibernetică

(1) Până la ... [6 luni de la data intrării în vigoare a prezentului regulament], Comisia instituie un grup de experți privind reziliența cibernetică („Grupul de experți”). Grupul de experți este numit de Comisie pentru un mandat de trei ani, care poate fi reînnoit. Componența grupului de experți urmărește să fie echilibrată din punct de vedere geografic și din punctul de vedere al genului și include următoarele persoane:

(a) reprezentanți ai fiecăruia dintre următoarelor organisme:

(i) Agenția Uniunii Europene pentru Securitate Cibernetică;

(ia) Centrul european de competențe în materie de securitate cibernetică;

(ii) Comitetul european pentru protecția datelor;

(iii) Organismele europene de standardizare.

Dacă este necesar, pot fi invitați reprezentanți ai altor agenții ale Uniunii.

(b) experți care reprezintă operatorii economici relevanți, asigurând reprezentarea adecvată a microîntreprinderilor și a întreprinderilor mici și mijlocii;

(c) experți care reprezintă societatea civilă, inclusiv organizațiile de consumatori și comunitatea de programe informatice gratuite și cu sursă deschisă;

(d) experți numiți cu titlu personal care dețin cunoștințe și experiență dovedite în domeniile reglementate de prezentul regulament;

(e) experți care reprezintă mediul academic, inclusiv universitățile, institutele de cercetare și alte organizații științifice, inclusiv persoane care au competențe globale.

(2) Grupul de experți consiliază Comisia cu privire la următoarele aspecte:

(a) lista produselor critice cu elemente digitale prevăzute în anexa III, precum și eventuala necesitate de a actualiza lista respectivă;

(b) punerea în aplicare a sistemelor europene de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 și posibilitatea de a le face obligatorii pentru produsele extrem de critice cu elemente digitale;

(c) evaluări fără caracter obligatoriu ale produselor cu elemente digitale, la cererea unei autorități de supraveghere a pieței care efectuează o investigație în temeiul articolului 43;

(d) aplicarea conceptelor relevante ale noului cadru legislativ în cazul programelor informatice, în special al programelor informatice gratuite și cu sursă deschisă;

(e) elementele regulamentului care trebuie abordate în orientările menționate la articolul 17a;

(f) disponibilitatea și calitatea standardelor europene și internaționale, precum și posibilitatea de a le completa sau de a le înlocui cu specificații tehnice comune;

(g) disponibilitatea unor profesioniști calificați în domeniul securității cibernetice în întreaga Uniune, inclusiv a unui personal adecvat pentru a efectua evaluări ale conformității de către terți în temeiul prezentului regulament;

(h) eventuala necesitate de a modifica prezentul regulament.

Grupul de experți cartografiază, de asemenea, tendințele la nivelul Uniunii și al statelor membre în ceea ce privește vulnerabilitățile existente și remediate.

(3) Grupul de experți ține seama de opiniile unei game largi de părți interesate și își îndeplinește sarcinile la cel mai înalt nivel de profesionalism, independență, imparțialitate și obiectivitate.

(3a) Comisia consultă grupul de experți atunci când pregătește acte delegate sau de punere în aplicare în temeiul prezentului regulament.

(3b) Grupul de experți poate furniza autorităților de supraveghere a pieței evaluări fără caracter obligatoriu ale produselor cu elemente digitale pentru a facilita investigațiile în temeiul articolului 43.

(4) Grupul de experți este prezidat de Comisie și constituit în conformitate cu normele orizontale privind crearea și funcționarea grupurilor de experți ale Comisiei. În acest context, Comisia poate invita ad-hoc experți care dețin cunoștințe de specialitate specifice.

(5) Grupul de experți își îndeplinește sarcinile în conformitate cu principiul transparenței. Comisia publică componența grupului de experți, declarația de interese a membrilor săi, un rezumat al reuniunilor Grupului de experți și alte documente pertinente pe site-ul său.

Articolul 6b

Consolidarea competențelor într-un mediu digital rezilient din punct de vedere cibernetic

În sensul prezentului regulament și pentru a răspunde cererii de profesioniști capabili să asigure securitatea cibernetică a produselor cu elemente digitale, Comisia și statele membre, în cooperare cu ENISA, asigură punerea în aplicare a:

(a) programelor de educație și formare în domeniul securității cibernetice și parcursurile profesionale asociate acestora, contribuind la creșterea rezilienței și a incluziunii forței de muncă din domeniul securității cibernetice, inclusiv din punctul de vedere al genului și aliniate la nevoile întreprinderilor în cauză, în special în cazul în care aceste întreprinderi sunt microîntreprinderi, întreprinderi mici sau mijlocii, inclusiv întreprinderi nou-înființate, sau administrația publică;

(b) inițiativelor de intensificare a colaborării dintre sectorul privat, operatorii economici, inclusiv prin recalificarea sau perfecționarea profesională a angajaților producătorilor, consumatori, furnizorii de educație și formare, și statele membre, extinzând opțiunile pentru tineri de a avea acces la locuri de muncă în acest sector;

(c) strategiilor care vizează sporirea mobilității forței de muncă, dezvoltarea competențelor în materie de securitate cibernetică și crearea de instrumente organizaționale și tehnologice pentru a valorifica la maxim talentele existente în materie de securitate cibernetică.

Articolul 7

Siguranța generală a produselor

Prin derogare de la articolul 2 alineatul (1) al treilea paragraf litera (b) din Regulamentul ***(UE) 2023/988*** în care produsele respective nu fac obiectul unor cerințe specifice prevăzute de alte acte din legislația de armonizare a Uniunii în sensul articolului 3 punctul 25 din Regulamentul ***(UE) 2023/988***,capitolul III secțiunea 1, capitolele V și VII și capitolele IX-XI din Regulamentul ***(UE) 2023/988*** se aplică produselor respective în ceea ce privește riscurile în materie de siguranță care nu sunt acoperite de prezentul regulament.

Articolul 8

Sistemele de IA cu grad ridicat de risc

(1) Produsele cu elemente digitale clasificate drept sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament și care îndeplinesc cerințele esențiale prevăzute în secțiunea 1 din anexa I la prezentul regulament sunt considerate, în cazul în care procesele instituite de producător respectă cerințele esențiale prevăzute în secțiunea 2 din anexa I, conforme cu cerințele legate de securitatea cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], fără a aduce atingere celorlalte cerințe legate de acuratețe și robustețe incluse la articolul menționat anterior și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate a UE emisă în temeiul prezentului regulament.

(2) Pentru produsele și cerințele de securitate cibernetică menționate la alineatul (1), se aplică procedura relevantă de evaluare a conformității, astfel cum este prevăzută la articolul [articolul 43] din Regulamentul [Regulamentul privind inteligența artificială]. În scopul efectuării acestei evaluări, organismele ***relevante*** care au dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc în temeiul Regulamentului [Regulamentul privind inteligența artificială] au, de asemenea, dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc ***care intră*** în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în anexa I la prezentul regulament, cu condiția ca respectarea de către organismele notificate respective a cerințelor prevăzute la articolul 29 din prezentul regulament să fi fost evaluată în contextul procedurii de notificare în temeiul Regulamentului [Regulamentul privind inteligența artificială].

(3) Prin derogare de la alineatul (2), produsele critice cu elemente digitale enumerate în anexa III la prezentul regulament, care trebuie să aplice procedurile de evaluare a conformității menționate la articolul 24 alineatul (2) litera (a), la articolul 24 alineatul (2) litera (b) și la articolul 24 alineatul (3) literele (a) și (b) în temeiul prezentului regulament, care sunt clasificate, de asemenea, ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială] și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa [anexa VI] la Regulamentul [Regulamentul privind inteligența artificială] fac obiectul procedurilor de evaluare a conformității prevăzute de prezentul regulament în ceea ce privește cerințele esențiale ale prezentului regulament.

(3a) Producătorii de produse cu elemente digitale clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu alineatul (1) de la prezentul articol pot participa la spațiile de testare în materie de reglementare a IA menționate la articolul 53 din Regulamentul [Regulamentul privind IA].

Articolul 9

Produsele asimilate mașinilor

Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului ***(UE) 2023/1230*** care ***sunt produse cu elemente digitale sau*** produse cu elemente digitale ***finalizate***

parțial în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate UE pe baza prezentului regulament sunt considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în anexa [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul ***(UE) 2023/1230*** în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.

Articolul 9a

Achizițiile publice de produse cu elementele digitale

(1) Fără a aduce atingere Directivelor 2014/24/UE[35] și 2014/25/UE[36] ale Parlamentului European și ale Consiliului, statele membre asigură, atunci când achiziționează produse cu elemente digitale, un nivel ridicat de securitate cibernetică și o perioadă de asistență adecvată.

(2) Statele membre se asigură că producătorii remediază vulnerabilitățile care afectează produsele achiziționate public cu elemente digitale, inclusiv punând la dispoziție rapid actualizări de securitate.

CAPITOLUL II

OBLIGAȚIILE OPERATORILOR ECONOMICI

Articolul 10

Obligații ale fabricanților

(1) Atunci când introduc pe piață un produs cu elemente digitale, producătorii se asigură că acesta a fost proiectat, dezvoltat și produs în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 1.

---

35 Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE (JO L 94, 28.3.2014, p. 65).

36 Directiva 2014/25/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile efectuate de entitățile care își desfășoară activitatea în sectoarele apei, energiei, transporturilor și serviciilor poștale și de abrogare a Directivei 2004/17/CE (JO L 94, 28.3.2014, p. 243).

(2) În scopul respectării obligației prevăzute la alineatul (1), producătorii efectuează o evaluare a riscurilor de securitate cibernetică asociate cu un produs cu elemente digitale și iau în considerare rezultatul evaluării respective în cursul etapelor de planificare, proiectare, dezvoltare, producție, livrare și întreținere a produsului cu elemente digitale, cu scopul de a reduce la minimum riscurile de securitate cibernetică, de a preveni incidentele de securitate și de a reduce cât mai mult impactul unor astfel de incidente, inclusiv în ceea ce privește sănătatea și siguranța utilizatorilor.

(2a) Pe baza evaluării riscurilor în materie de securitate cibernetică, producătorii stabilesc modul în care cerințele esențiale prevăzute în anexa I secțiunea 1 sunt aplicabile produsului lor cu elemente digitale. Acestea includ evaluarea riscurilor în documentația tehnică, astfel cum se prevede la articolul 23.3. Atunci când introduce pe piață un produs cu elemente digitale, producătorul include o evaluare a riscurilor de securitate cibernetică în documentația tehnică prevăzută la articolul 23 și în anexa V. În cazul produselor cu elemente digitale menționate la articolul 8 și la articolul 24 alineatul (4) care fac, de asemenea, obiectul altor acte ale Uniunii, evaluarea riscurilor de securitate cibernetică poate face parte din evaluarea riscurilor impusă de respectivele acte ale Uniunii. În cazul în care anumite cerințe esențiale nu sunt aplicabile produsului cu elemente digitale comercializat, producătorul include o justificare clară în documentația respectivă.

(4) În scopul respectării obligației prevăzute la alineatul (1), producătorii exercită diligența necesară atunci când integrează în produsele cu elemente digitale componente obținute de la terți. ***Producătorul trebuie*** să se asigure că respectivele componente nu compromit securitatea produsului cu elemente digitale***, inclusiv la integrarea componentelor unui software gratuit și cu sursă deschisă care nu a fost pus la dispoziție pe piață în cadrul unei activități comerciale***.

La identificarea unei vulnerabilități a unei componente, inclusiv a unei componente libere și cu sursă deschisă, care este integrată în produsul cu elemente digitale, producătorii abordează și remediază vulnerabilitatea în conformitate cu cerințele de tratare a vulnerabilităților prevăzute în anexa I secțiunea 2 și comunică măsurile corective luate persoanei sau entității care asigură întreținerea componentei.

(4a) Producătorul componentelor furnizează producătorului produsului finit informațiile și documentația necesare pentru a se conforma cerințelor prezentului

regulament, atunci când le furnizează astfel de componente. Aceste informații sunt puse la dispoziție gratuit.

(5) Producătorul documentează în mod sistematic, într-un mod proporțional cu natura și cu riscurile de securitate cibernetică, aspectele de securitate cibernetică relevante ale produsului cu elemente digitale, inclusiv vulnerabilitățile de care ia cunoștință și orice informații relevante furnizate de terți, și, după caz, actualizează evaluarea riscurilor pentru produsul respectiv.

(6) Atunci când introduc pe piață un produs cu elemente digitale, ***producătorii stabilesc perioada de asistență în care*** vulnerabilitățile produsului respectiv sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 2. ***În acest sens, producătorul se asigură că perioada de asistență este proporțională cu durata de viață preconizată a produsului și în conformitate cu natura produsului și cu așteptările utilizatorilor, cu disponibilitatea mediului de operare și, dacă este cazul, cu perioada de asistență a principalelor componente integrate în produsul cu elemente digitale. În acest scop, producătorii pun la dispoziție, la cererea autorităților de supraveghere a pieței, informații privind durata de viață preconizată a produsului pe care au avut-o în vedere pentru a stabili durata perioadei de asistență pentru produsul pus la dispoziție pe piață. Autoritățile de supraveghere a pieței monitorizează produsele cu elemente digitale și se asigură în mod activ că producătorii au aplicat aceste criterii în mod corect, inclusiv o evaluare a informațiilor primite de la producători cu privire la durata de viață preconizată a produsului, atunci când stabilesc perioada de asistență.***

Dacă este cazul, perioada de asistență trebuie să fie indicată în mod clar pe produs sau pe ambalajul acestuia ori să fie inclusă în acordurile contractuale. ***În orice caz, utilizatorii finali sunt, de asemenea, informați înainte de cumpărare cu privire la durata perioadei de asistență.***

Producătorii trebuie să dispună de politici și proceduri adecvate, inclusiv de politici coordonate de divulgare a vulnerabilităților, menționate în anexa I secțiunea 2 punctul 5, pentru a prelucra și a remedia vulnerabilitățile potențiale ale produsului cu elemente digitale raportate din surse interne sau externe.

Dacă este cazul, pentru consumatorii de produse cu elemente digitale, procedurile respective includ actualizări automate de securitate implicite. Utilizatorii ar trebui

să aibă în continuare posibilitatea de a dezactiva respectivele actualizări automate de securitate.

Producătorii informează în mod activ utilizatorii atunci când produsul lor cu elemente digitale a ajuns la sfârșitul perioadei sale de asistență.

(6a) În cazul în care perioada de asistență este mai scurtă de cinci ani, iar gestionarea vulnerabilităților s-a încheiat, producătorii pot oferi acces la codul sursă al unui astfel de produs cu elemente digitale altor întreprinderi care se angajează să extindă furnizarea de servicii de gestionare a vulnerabilităților, în special actualizări de securitate. Accesul la aceste coduri sursă se acordă numai în cazul în care acest lucru este prevăzut într-un acord contractual. Aceste acorduri protejează proprietatea asupra produsului cu elemente digitale și împiedică diseminarea codului sursă către publicul larg, cu excepția cazului în care acest cod a fost deja furnizat pe baza unei licențe libere și cu sursă deschisă.

(7) Înainte de a introduce pe piață un produs cu elemente digitale, producătorii întocmesc documentația tehnică menționată la articolul 23.

Aceștia efectuează procedurile alese de evaluare a conformității menționate la articolul 24 sau dispun efectuarea acestora.

În cazul în care conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I secțiunea 2 a fost demonstrată prin respectiva procedură de evaluare a conformității, producătorii întocmesc declarația de conformitate UE în conformitate cu articolul 20 și aplică marcajul CE în conformitate cu articolul 22.

(8) Producătorii păstrează documentația tehnică și declarația de conformitate UE, ▌ la dispoziția autorităților de supraveghere a pieței timp de ***cel puțin*** zece ani sau pe durata ***perioadei de asistență***, oricare din ele este mai lungă, de la introducerea pe piață a produsului cu elemente digitale.

Autoritățile de supraveghere a pieței asigură confidențialitatea și protecția adecvată a informațiilor din documentația tehnică furnizată de producători în conformitate cu articolul 52.

(9) Producătorii se asigură că există proceduri care să garanteze conformitatea continuă a produselor cu elemente digitale care fac parte dintr-o producție în serie. Producătorul

ține seama în mod adecvat de modificările survenite în procesul de dezvoltare și de producție sau în proiectarea ori caracteristicile produsului cu elemente digitale și de modificările standardelor armonizate ***orizontale sau specifice sectorului***, ale sistemelor europene de certificare de securitate cibernetică sau ale specificațiilor comune menționate la articolul 19 în raport cu care se declară conformitatea produsului cu elemente digitale sau prin aplicarea cărora este verificată conformitatea acestuia.

(10) Producătorii se asigură că produsele cu elemente digitale sunt însoțite de informațiile și instrucțiunile prevăzute în anexa II, în format electronic sau fizic. Aceste informații și instrucțiuni trebuie să fie redactate într-o limbă ușor de înțeles de către utilizatori. Ele trebuie să fie clare, ușor de înțeles, inteligibile și lizibile. De asemenea, trebuie să permită instalarea, funcționarea și utilizarea în condiții de securitate a produselor cu elemente digitale.

În cazul în care aceste informații și instrucțiuni sunt furnizate în format electronic, producătorii:

(a) le prezintă într-un format ușor de utilizat, care să permită utilizatorului să le consulte online, să le descarce, să le salveze pe un dispozitiv electronic și să le imprime;

(b) se asigură că acestea sunt accesibile online cel puțin în perioada de asistență a produsului cu elemente digitale.

(11) Producătorii fie prezintă declarația de conformitate UE împreună cu produsul cu elemente digitale, fie includ în instrucțiunile și informațiile prevăzute în anexa II adresa de internet la care poate fi accesată declarația de conformitate UE.

(12) De la introducerea pe piață și ***cel puțin în perioada de asistență*** ▌, producătorii care știu sau au motive să creadă că produsul cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor producătorului, pentru a retrage sau a rechema produsul, după caz.

(13) În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, producătorii furnizează autorității respective, într-o limbă care poate fi ușor înțeleasă

de către aceasta, toate informațiile și documentația, pe suport de hârtie sau în format electronic, necesare pentru a demonstra conformitatea produsului cu elemente digitale și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I. Aceștia cooperează cu autoritatea respectivă, la cererea acesteia, cu privire la adoptarea oricăror măsuri pentru eliminarea riscurilor de securitate cibernetică prezentate de produsul cu elemente digitale pe care l-au introdus pe piață.

(14) Un producător care își încetează activitatea și, în consecință, nu este în măsură să respecte obligațiile prevăzute în prezentul regulament informează, înainte ca încetarea activității să producă efecte, autoritățile relevante de supraveghere a pieței cu privire la această situație, precum și, prin orice mijloace disponibile și în măsura posibilului, utilizatorii respectivelor produse cu elemente digitale introduse pe piață.

(15) Comisia***, după consultarea grupului de experți și ținând seama de standardele internaționale, este împuternicită să adopte acte delegate în conformitate cu articolul 50, specificând*** formatul și elementele listei materialelor software prevăzută în anexa I secțiunea 2 punctul (1). ▌

Articolul 11

Raportarea obligațiilor generale ale producătorilor

(1) Producătorul notifică ENISA ▌cu privire la orice vulnerabilitate exploatată activ conținută în produsul cu elemente digitale***, în conformitate cu alineatul (1a) din prezentul articol***. ▌ENISA transmite notificarea, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, către CSIRT desemnată în scopul divulgării coordonate a vulnerabilităților în conformitate cu articolul ***12*** din Directiva ***(UE) 2022/2555***din statele membre în cauză la primirea notificării și informează autoritatea de supraveghere a pieței cu privire la vulnerabilitatea notificată. ***În cazul în care pentru o vulnerabilitate notificată nu sunt disponibile măsuri corective sau de atenuare, ENISA se asigură că informațiile cu privire la vulnerabilitatea notificată sunt partajate în conformitate cu protocoale stricte de securitate și pe baza principiului necesității de a cunoaște.***

(1a) Notificările menționate la alineatul (1) se supun următoarei proceduri:

(a) o avertizare timpurie, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care producătorul a luat cunoștință că există o

vulnerabilitate exploatată în mod activ, inclusiv dacă sunt disponibile măsuri corective sau recomandate de atenuare a riscului cunoscute;

(b) o notificare a vulnerabilității, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la data la care producătorul a luat cunoștință de vulnerabilitatea exploatată în mod activ, care, după caz, actualizează informațiile generale menționate la litera (a), inclusiv orice măsuri corective sau de atenuare luate și indică o evaluare a amplorii vulnerabilității, inclusiv gravitatea și impactul acesteia;

(c) un raport final, în termen de o lună de la transmiterea notificării privind vulnerabilitatea în temeiul literei (b) sau când o măsură corectivă sau de atenuare este disponibilă, care să includă cel puțin următoarele elemente:

(i) o descriere a vulnerabilității, inclusiv a gravității și a impactului acesteia;

(ii) dacă sunt disponibile, informații privind orice actor care a exploatat sau care exploatează vulnerabilitatea;

(iii) detalii privind actualizarea securității sau alte măsuri corective care au fost puse la dispoziție pentru a remedia vulnerabilitatea.

(1b) După punerea la dispoziție a unei actualizări de securitate sau după punerea în aplicare a unei alte forme de măsuri corective sau de atenuare, ENISA adaugă vulnerabilitatea notificată în temeiul alineatului (1) de la prezentul articol în baza de date europeană a vulnerabilităților menționată la articolul 12 din Directiva (UE) 2022/2555.

(2) Producătorul notifică ENISA ▌ orice incident ***semnificativ*** care afectează securitatea produsului cu elemente digitale***, în conformitate cu alineatul (2b) din prezentul articol***. ENISA transmite notificările, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, punctului unic de contact desemnat în conformitate cu articolul ***8*** din Directiva ***(UE) 2022/2555*** din statele membre în cauză și informează autoritatea de supraveghere a pieței cu privire la incidentele semnificative notificate. ***Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite***.

(2a) Un incident este considerat semnificativ, astfel cum se menționează la alineatul (2), în cazul în care:

(a) a cauzat sau poate cauza perturbări operaționale grave ale producției sau ale serviciilor pentru producătorul în cauză, ceea ce ar avea un impact asupra securității unui produs; sau

(b) a afectat sau poate afecta alte persoane fizice sau juridice, cauzând prejudicii materiale sau morale considerabile.

(2b) Notificările menționate la alineatul (2) se supun următoarei proceduri:

(a) o avertizare timpurie, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care producătorul a luat cunoștință de incidentul semnificativ, care, după caz, indică dacă există suspiciuni că incidentul semnificativ este cauzat de acțiuni ilegale sau răuvoitoare sau ar putea avea un impact transfrontalier;

(b) o notificare a incidentului, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore din momentul în care producătorul a luat cunoștință de incidentul semnificativ, care, după caz, actualizează informațiile menționate la litera (a) și prezintă o evaluare inițială a incidentului semnificativ, a gravității și a impactului acestuia, precum și a indicatorilor de compromitere, dacă sunt disponibili;

(c) un raport final, în termen de o lună de la transmiterea notificării cu privire la incident în temeiul literei (b), care să includă cel puțin următoarele elemente:

(i) o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia;

(ii) tipul de amenințare sau de cauză principală care probabil că a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs;

(iv) dacă este cazul, impactul transfrontalier al incidentului;

în cazul unui incident în desfășurare la momentul prezentării raportului final menționat la litera (d) de la prezentul alineat, statele membre se asigură că

producătorul în cauză prezintă la momentul respectiv un raport privind progresele înregistrate și un raport final în termen de o lună de la gestionarea incidentului.

(2c) Producătorii care au notificat incidente semnificative în conformitate cu prezentul regulament și care sunt, de asemenea, identificați ca entități esențiale sau entități importante în temeiul Directivei (UE) 2022/2555 sunt considerați conformi cu cerințele prevăzute la articolul 23 din Directiva (UE) 2022/2555. ENISA transmite notificările primite în temeiul prezentului regulament către CSIRT responsabilă în conformitate cu Directiva (UE) 2022/2555. O entitate poate fi amendată o singură dată pentru nerespectarea unor cerințe care se suprapun.

(2d) Dacă este necesar, ENISA sau CSIRT relevantă poate solicita producătorilor să furnizeze un raport intermediar privind actualizările relevante ale situației cu privire la vulnerabilitatea exploatată activ sau la incidentul semnificativ.

(2e) Producătorii care se califică drept microîntreprinderi sau întreprinderi mici sau mijlocii sunt exceptați de la aplicarea alineatului (1a) litera (a) și a alineatului (2b) litera (a).

(3) ENISA transmite Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) instituită prin articolul ***16*** din Directiva ***(UE) 2022/2555*** informațiile notificate în temeiul alineatelor (1) și (2) dacă aceste informații sunt relevante pentru gestionarea coordonată la nivel operațional a incidentelor și crizelor de securitate cibernetică de mare amploare.

(4) Producătorul informează, fără întârzieri nejustificate și după ce a luat cunoștință de acesta, utilizatorii ***afectați ai*** produsului cu elemente digitale ***și, după caz, toți utilizatorii*** cu privire la ***incidentul semnificativ*** și, dacă este necesar, cu privire la măsurile ***de atenuare a riscurilor și cu privire la orice măsuri*** corective pe care utilizatorul le poate aplica pentru a atenua impactul incidentului ***semnificativ***.

(4a) ENISA se asigură că notificările în temeiul alineatelor (1) și (2) sunt transmise prin canale de comunicare și stocate pe servere care asigură cel mai înalt nivel posibil de securitate cibernetică și de protecție împotriva actorilor răuvoitori.

(4b) În cazul în care sensibilizarea publicului este necesară pentru a preveni un incident semnificativ sau pentru a gestiona un incident semnificativ în curs sau în cazul în care divulgarea incidentului semnificativ este în alt mod în interesul public, ENISA

și, după caz, echipele de intervenție în caz de incidente de securitate informatică sau autoritățile competente ale statelor membre în cauză pot, după consultarea producătorului în cauză, să informeze publicul cu privire la incidentul semnificativ sau să solicite producătorului să facă acest lucru.

(5) Comisia ***adoptă acte delegate în conformitate cu articolul 50, pentru a completa prezentul regulament prin specificarea mai detaliată a formatului*** notificărilor și ***a procedurii*** de efectuare a notificărilor transmise în temeiul alineatelor (1) și (2). ***Aceste acte delegate*** se adoptă ***până la ... [12 luni de la data intrării în vigoare a prezentului regulament].***

(6) Pe baza notificărilor primite în temeiul alineatelor (1) și (2), ENISA pregătește un raport tehnic bienal referitor la tendințele emergente în ceea ce privește riscurile de securitate cibernetică ale produselor cu elemente digitale și îl transmite grupului de cooperare menționat la articolul ***14*** din Directiva ***(UE) 2022/2555***. Primul raport de acest tip se prezintă în termen de 24 de luni de la data la care încep să se aplice obligațiile prevăzute la alineatele (1) și (2). ***ENISA include informații relevante din rapoartele sale tehnice în raportul său privind situația securității cibernetice în Uniune în temeiul articolului 18 din Directiva (UE) 2022/2555.***

(6a) ENISA instituie un mecanism securizat de raportare digitală, după consultarea Grupului de experți, pentru a simplifica obligațiile de raportare ale producătorilor. Acest mecanism servește drept punct de intrare unic pentru obligațiile de raportare stabilite în temeiul prezentului regulament și, dacă este posibil, în temeiul altor acte legislative ale Uniunii.

Articolul 11a

Notificarea voluntară

(1) În plus față de obligațiile de notificare prevăzute la articolul 11, notificările pot fi transmise ENISA în mod voluntar de către:

(a) producători, în ceea ce privește incidentele, amenințările cibernetice și incidentele evitate la limită;

(b) alte entități decât cele menționate la litera (a), indiferent dacă intră în domeniul de aplicare al prezentului regulament sau nu, cu privire la incidente

semnificative și nesemnificative, amenințări cibernetice și incidente evitate la limită;

(c) orice actor în ceea ce privește vulnerabilitățile care pot fi incluse în baza de date europeană a vulnerabilităților menționată la articolul 12 din Directiva (UE) 2022/2555.

(2) ENISA prelucrează notificările menționate la alineatul (1) litera (a) de la prezentul articol în conformitate cu procedura prevăzută la articolul 11. ENISA poate trata notificările obligatorii cu prioritate față de notificările voluntare.

(3) Pentru a simplifica notificările voluntare, este posibil ca acestea să fie notificate prin intermediul mecanismului de raportare digitală securizat menționat la articolul 11 alineatul (6a).

(4) După caz, ENISA asigură confidențialitatea și protecția adecvată a informațiilor furnizate de entitatea notificatoare. Fără a aduce atingere prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, raportarea voluntară nu impune entității notificatoare nicio obligație suplimentară care nu i-ar fi revenit dacă nu ar fi transmis notificarea.

Articolul 11b

Punct unic de contact pentru utilizatori

(1) Pentru a facilita raportarea cu privire la securitatea produselor, producătorii desemnează un punct unic de contact care să permită utilizatorilor să comunice direct și rapid cu aceștia, după caz, prin mijloace electronice și într-un mod ușor de utilizat, inclusiv permițând utilizatorilor produsului să aleagă mijloacele de comunicare prevăzute la punctul 1 din anexa II, care nu se bazează exclusiv pe instrumente automatizate.

(2) Pe lângă obligațiile prevăzute în Directiva 2000/31/CE a Parlamentului European și a Consiliului[37], producătorii publică informațiile necesare pentru ca utilizatorii

---

[37] Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (JO L 178, 17.7.2000, p. 1).

finali să poată identifica și comunica cu ușurință cu punctele lor unice de contact. Informațiile respective sunt ușor accesibile și se actualizează.

Articolul 12

Reprezentanți autorizați

(1) Un producător poate numi un reprezentant autorizat printr-un mandat scris.

(2) Obligațiile stabilite la articolul 10 alineatul (1) până la alineatul (7) prima liniuță și la articolul 10 alineatul (9) nu fac parte din mandatul reprezentantului autorizat.

(3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la producător. ***La cerere, acesta furnizează autorităților de supraveghere a pieței o copie a mandatului.*** Mandatul permite reprezentantului autorizat să îndeplinească cel puțin următoarele:

(a) să păstreze declarația de conformitate UE menționată la articolul 20 și documentația tehnică menționată la articolul 23 la dispoziția autorităților de supraveghere a pieței timp de zece ani de la introducerea pe piață a produsului cu elemente digitale;

(aa) în cazul în care reprezentantul autorizat are motive să creadă că un produs cu elemente digitale în cauză prezintă un risc de securitate cibernetică, informează producătorul;

(b) în urma unei cereri motivate din partea unei autorități de supraveghere a pieței, să furnizeze autorității respective toate informațiile și documentația necesare pentru a demonstra conformitatea produsului cu elemente digitale;

(c) să coopereze cu autoritățile de supraveghere a pieței, la cererea acestora, cu privire la orice acțiune întreprinsă pentru eliminarea ***efectivă a*** riscurilor reprezentate de produsul cu elemente digitale acoperit de mandatul reprezentantului autorizat.

Articolul 13

Obligațiile importatorilor

(1) Importatorii introduc pe piață numai produse cu elemente digitale care respectă cerințele esențiale prevăzute în anexa I secțiunea 1 și în cazul cărora procesele instituite de producător respectă cerințele esențiale prevăzute în anexa I secțiunea 2.

(2) Înainte de a introduce pe piață un produs cu elemente digitale, importatorii se asigură că:

(a) producătorul a efectuat procedurile adecvate de evaluare a conformității menționate la articolul 24;

(b) producătorul a întocmit documentația tehnică;

(c) produsul cu elemente digitale poartă marcajul CE menționat la articolul 22***, declarația de conformitate UE este disponibilă*** și ***produsul*** este însoțit de informațiile și instrucțiunile de utilizare prevăzute în anexa II***;***

(ca) toate documentele care demonstrează îndeplinirea cerințelor prevăzute la prezentul articol au fost primite de la producător.

(3) În cazul în care un importator consideră sau are motive să creadă că un produs cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I, importatorul nu introduce produsul pe piață până când produsul respectiv sau procesele instituite de producător nu au fost aduse în conformitate cu cerințele esențiale prevăzute în anexa I. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, importatorul informează producătorul și autoritățile de supraveghere a pieței în acest sens.

Pe baza recomandărilor specifice primite de autoritățile de supraveghere a pieței sau de Comisie în conformitate cu articolele 43 și 45, importatorul aplică aceste recomandări, inclusiv retragerea sau rechemarea produsului. În plus, în cazul în care un importator consideră sau are motive să creadă că un produs cu elemente digitale poate prezenta un risc de securitate cibernetică având în vedere factori de risc netehnici, acesta retrage sau recheamă produsul respectiv. Importatorii informează autoritățile de supraveghere a pieței și Comisia în acest sens.

(4) Importatorii indică pe produsul cu elemente digitale sau ▌ pe ambalaj sau într-un document care însoțește respectivul produs, numele, denumirea lor comercială înregistrată sau marca lor înregistrată, adresa poștală și adresa de e-mail***, și, după caz, site-ul web*** la care pot fi contactați. Datele de contact trebuie să fie prezentate într-o limbă ușor de înțeles pentru utilizatori și pentru autoritățile de supraveghere a pieței.

(5) Importatorii se asigură că produsul cu elemente digitale este însoțit de instrucțiunile și informațiile prevăzute în anexa II, redactate într-o limbă care poate fi ușor înțeleasă de către utilizatori.

(6) Importatorii care știu sau au motive să creadă că un produs cu elemente digitale pe care l-au introdus pe piață sau procesele instituite de producătorul acestuia nu sunt conforme cu cerințele esențiale prevăzute în anexa I ***îi solicită*** imediat ***producătorului să ia*** măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor instituite de producătorul acestuia cu cerințele esențiale prevăzute în anexa I sau pentru a retrage sau a rechema produsul, după caz.

(6a) După ***ce au luat cunoștință de o vulnerabilitate*** a produsului cu elemente digitale, importatorii informează producătorul fără întârzieri nejustificate cu privire la vulnerabilitatea respectivă. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, importatorii informează imediat în acest sens autoritățile de supraveghere a pieței din statele membre în care au pus la dispoziție pe piață respectivul produs cu elemente digitale, oferind detalii, în special cu privire la neconformitate și la eventualele măsuri corective adoptate.

(7) Importatorii păstrează o copie a declarației de conformitate UE la dispoziția autorităților de supraveghere a pieței timp de zece ani de la introducerea pe piață a produsului și se asigură că documentația tehnică poate fi pusă la dispoziția acestor autorități, la cerere.

(8) În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, importatorii furnizează autorității respective, într-o limbă care poate fi ușor înțeleasă de către aceasta, toate informațiile și documentația, pe suport de hârtie sau în format electronic, necesare pentru a demonstra conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I secțiunea 2. Importatorii

cooperează cu autoritatea respectivă, la cererea acesteia, cu privire la orice acțiune întreprinsă pentru eliminarea riscurilor prezentate de produsele cu elemente digitale pe care aceștia le-au introdus pe piață.

(9) Atunci când importatorul unui produs cu elemente digitale constată că producătorul produsului respectiv și-a încetat activitatea și, în consecință, nu este în măsură să respecte obligațiile prevăzute în prezentul regulament, importatorul informează autoritățile relevante de supraveghere a pieței cu privire la această situație, precum și, prin orice mijloace disponibile și în măsura posibilului, utilizatorii produselor cu elemente digitale introduse pe piață.

Articolul 14

Obligațiile distribuitorilor

(1) În cazul în care pun la dispoziție pe piață un produs cu elemente digitale, distribuitorii acordă o atenție deosebită cerințelor prezentului regulament.

(2) Înainte de a pune la dispoziție pe piață un produs cu elemente digitale, distribuitorii verifică dacă:

(a) respectivul produs cu elemente digitale poartă marcajul CE;

(b) producătorul și importatorul au respectat cerințele prevăzute la articolul 10 alineatele (10) și (11) și la articolul 13 alineatul (4) ***și au comunicat distribuitorului toate documentele relevante;***

(3) În cazul în care un distribuitor consideră sau are motive să creadă***, pe baza informațiilor pe care le deține,*** că un produs cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I, distribuitorul nu pune produsul la dispoziție pe piață până când produsul respectiv sau procesele instituite de producător nu au fost aduse la nivel de conformitate. În plus, atunci când produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, distribuitorul informează producătorul și autoritățile de supraveghere a pieței în acest sens.

(4) Distribuitorii care știu sau au motive să creadă***, pe baza informațiilor pe care le dețin,*** că un produs cu elemente digitale pe care l-au pus la dispoziție pe piață sau procesele instituite de producătorul acestuia nu sunt conforme cu cerințele esențiale prevăzute în

anexa I ***solicită producătorului să ia*** măsurile corective necesare pentru a aduce produsul cu elemente digitale sau procesele instituite de producătorul acestuia la nivel de conformitate sau pentru a retrage sau a rechema produsul, după caz.

(4a) După ***ce au luat cunoștință de o vulnerabilitate*** a produsului cu elemente digitale, distribuitorii informează producătorul fără întârzieri nejustificate cu privire la vulnerabilitatea respectivă. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, distribuitorii informează imediat în acest sens autoritățile de supraveghere a pieței din statele membre în care au pus la dispoziție pe piață respectivul produs cu elemente digitale, oferind detalii, în special cu privire la neconformitate și la eventualele măsuri corective adoptate.

(5) În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, distribuitorii furnizează autorității respective, într-o limbă care poate fi ușor înțeleasă de către aceasta, toate informațiile și documentația, pe suport de hârtie sau în format electronic, necesare pentru a demonstra conformitatea produsului cu elemente digitale și a proceselor instituite de producătorul acestuia cu cerințele esențiale prevăzute în anexa I. Distribuitorii cooperează cu autoritatea respectivă, la cererea acesteia, cu privire la orice acțiune întreprinsă pentru eliminarea riscurilor prezentate de produsele cu elemente digitale pe care aceștia le-au pus la dispoziție pe piață.

(6) ***Pe baza informațiilor pe care le deține,*** atunci când distribuitorul unui produs cu elemente digitale constată că producătorul produsului respectiv și-a încetat activitatea și, în consecință, nu este în măsură să respecte obligațiile prevăzute în prezentul regulament, distribuitorul informează autoritățile relevante de supraveghere a pieței cu privire la această situație, precum și, prin orice mijloace disponibile și în măsura posibilului, utilizatorii produselor cu elemente digitale introduse pe piață.

Articolul 15

Situațiile în care obligațiile producătorilor se aplică importatorilor și distribuitorilor

Importatorul sau distribuitorul este considerat producător în sensul prezentului regulament și i se aplică obligațiile care îi revin producătorului prevăzute la articolul 10 și la articolul 11 alineatele (1), (2), (4) și (7) atunci când respectivul importator sau distribuitor introduce pe piață

un produs cu elemente digitale sub numele sau marca sa ori efectuează o modificare substanțială a produsului cu elemente digitale deja introdus pe piață.

Articolul 16

Alte cazuri în care se aplică obligațiile producătorilor

O persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul, care efectuează o modificare substanțială a produsului cu elemente digitale ***și îl pune la dispoziție pe piață*** este considerată producător în sensul prezentului regulament.

Persoana respectivă este supusă obligațiilor producătorului prevăzute la articolul 10 și la articolul 11 alineatele (1), (2), (4) și (7) pentru partea produsului care este afectată de modificarea substanțială sau, dacă modificarea substanțială are un impact asupra securității cibernetice a produsului cu elemente digitale în ansamblul său, pentru întregul produs.

Articolul 17

Identificarea operatorilor economici

(1) Operatorii economici furnizează autorităților de supraveghere a pieței, la cerere ▌, următoarele informații:

(a) denumirea și adresa oricărui operator economic care le-a furnizat acestora un produs cu elemente digitale;

(b) denumirea și adresa oricărui operator economic căruia aceștia i-au furnizat un produs cu elemente digitale.

(2) Operatorii economici trebuie să fie în măsură să prezinte informațiile menționate la alineatul (1) timp de zece ani de la data la care le-a fost furnizat produsul cu elemente digitale și timp de zece ani de la data la care aceștia au furnizat produsul, după caz.

Articolul 17a

Orientări

(1) Pentru a asigura claritate, certitudine și coerență între practicile operatorilor economici, Comisia elaborează și emite orientări pentru operatorii economici, în care explică modul de aplicare a prezentului regulament, acordând o atenție

deosebită modalităților de facilitare a conformării de către microîntreprinderi și întreprinderile mici și mijlocii.

(2) Orientările se publică până la ... [12 luni de la data intrării în vigoare a prezentului regulament] și se actualizează după caz, în special având în vedere eventualele modificări ale listei de produse critice prevăzute în anexa III. Acestea includ cel puțin următoarele elemente:

(a) o explicație detaliată a domeniului de aplicare al prezentului regulament, cu un accent deosebit pe soluțiile de prelucrare a datelor la distanță și pe software-ul liber și cu sursă deschisă;

(b) criteriile detaliate utilizate pentru a determina modul în care produsele critice cu elemente digitale sunt încadrate în clasele I sau II, astfel cum se prevede în anexa III;

(c) interacțiunea dintre prezentul regulament și alte acte legislative ale Uniunii, în special în ceea ce privește prezumțiile de conformitate și evaluările conformității;

(d) orientări pentru producători cu privire la modul de efectuare a evaluării riscurilor în materie de securitate cibernetică menționate la articolul 10 alineatul (2) și la aplicabilitatea cerințelor esențiale, inclusiv, dacă sunt disponibile, a celor mai bune practici;

(e) orientări pentru producători cu privire la modul de determinare corespunzătoare a perioadei de sprijin pentru diferite categorii de produse, în conformitate cu articolul 10 alineatul (6);

(f) o explicație a modului de gestionare a cerințelor de raportare în temeiul prezentului regulament sau al altor acte legislative ale Uniunii;

(g) o listă a actelor delegate și de punere în aplicare publicate de Comisie în temeiul prezentului regulament;

(h) orientări pentru statele membre cu privire la neurmărirea penală a cercetătorilor în domeniul securității informațiilor;

(i) orientări cu privire la ceea ce constituie modificări substanțiale.

(3) La elaborarea orientărilor în temeiul prezentului articol, Comisia consultă Grupul

de experți.

CAPITOLUL III

CONFORMITATEA PRODUSULUI CU ELEMENTE DIGITALE

Articolul 18

Prezumția de conformitate

(1) Produsele cu elemente digitale și procesele instituite de producător care sunt conforme cu standardele armonizate sau cu anumite părți ale acestora ale căror referințe au fost publicate în Jurnalul Oficial al Uniunii Europene sunt considerate a fi conforme cu cerințele esențiale prevăzute în anexa I, vizate de respectivele standarde sau părți ale acestora.

Comisia solicită, în conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații europene de standardizare să elaboreze standarde armonizate pentru cerințele esențiale prevăzute în anexa I la prezentul regulament. Atunci când elaborează cererea de standardizare pentru prezentul regulament, Comisia depune eforturi pentru a ține seama de standardele internaționale existente sau iminente în materie de securitate cibernetică, pentru a simplifica elaborarea de standarde armonizate.

(2) Produsele cu elemente digitale și procesele instituite de producător care sunt conforme cu specificațiile comune menționate la articolul 19 sunt considerate a fi conforme cu cerințele esențiale prevăzute în anexa I, în măsura în care specificațiile comune respective acoperă aceste cerințe.

(3) Produsele cu elemente digitale și procesele instituite de producător pentru care s-a emis o declarație de conformitate UE sau un certificat în cadrul unui sistem european de certificare de securitate cibernetică adoptat în conformitate cu Regulamentul (UE) 2019/881 și specificat în conformitate cu alineatul (4) sunt considerate a fi conforme cu cerințele esențiale prevăzute în anexa I în măsura în care declarația de conformitate UE sau certificatul de securitate cibernetică sau părți ale acestora acoperă cerințele respective.

(4) Comisia este împuternicită să ***adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea sistemelor*** europene de

certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea ***produselor cu elemente digitale*** cu cerințele esențiale sau cu anumite părți ale acestora, astfel cum sunt prevăzute în anexa I. În plus, ***emiterea unui*** certificat de securitate cibernetică emis în cadrul unor astfel de sisteme***, la un nivel de asigurare „substanțial” sau „ridicat”,*** elimină obligația unui producător de a efectua o evaluare a conformității de către terți pentru cerințele corespunzătoare, astfel cum se prevede la articolul 24 alineatul (2) literele (a) și (b) și la articolul 24 alineatul (3) literele (a) și (b). ▌

Articolul 19

Specificațiile comune

(1) ▌ Comisia este împuternicită să adopte ▌ acte ***delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin stabilirea unor*** specificații comune ***care acoperă*** cerințele ***tehnice care oferă un mijloc de respectare a cerințelor*** prevăzute în anexa I ***pentru produsele care intră în domeniul de aplicare al prezentului regulament, în cazul în care au fost îndeplinite următoarele condiții:***

(a) Comisia a solicitat, în temeiul articolului 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații de standardizare europene să elaboreze un standard armonizat pentru cerințele esențiale prevăzute în anexa I, iar cererea nu a fost acceptată sau documentele de standardizare europeană care răspund cererii respective nu sunt livrate în termenul stabilit în conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012 sau documentele de standardizare europeană nu se conformează solicitării; și dacă

(b) nu este publicată în Jurnalul Oficial al Uniunii Europene nicio trimitere la standardele armonizate care acoperă cerințele esențiale prevăzute în anexa I la prezentul regulament, în conformitate cu Regulamentul (UE) nr. 1025/2012, și nu se preconizează publicarea niciunei astfel de trimiteri într-un termen rezonabil.

(2) Înainte de pregătirea actului delegat, Comisia informează Grupul de experți că consideră că sunt îndeplinite condițiile de la alineatul (1). La pregătirea actelor delegate, Comisia ține seama de avizele Grupului de experți.

(3) În cazul în care un standard armonizat este adoptat de o organizație de standardizare europeană și este propus Comisiei pentru ca referința sa să fie publicată în Jurnalul Oficial al Uniunii Europene, Comisia evaluează standardul armonizat în conformitate cu Regulamentul (UE) nr. 1025/2012. Atunci când referința unui standard armonizat este publicată în Jurnalul Oficial al Uniunii Europene, Comisia abrogă actele delegate relevante menționate la alineatul (1) sau acele părți ale lor care vizează aceleași cerințe esențiale menționate la anexa I la prezentul regulament.

Articolul 20

Declarația de conformitate UE

(1) Declarația de conformitate UE este întocmită de producători în conformitate cu articolul 10 alineatul (7) și prevede faptul că îndeplinirea cerințelor esențiale aplicabile prevăzute în anexa I a fost demonstrată.

(2) Declarația de conformitate UE trebuie să fie structurată după modelul prevăzut în anexa IV și să conțină elementele specificate în procedurile relevante de evaluare a conformității stabilite în anexa VI. O astfel de declarație trebuie actualizată ***după caz***. Aceasta trebuie pusă la dispoziție în limba sau limbile solicitate de statul membru în care produsul cu elemente digitale este introdus pe piață sau pus la dispoziție.

(3) În cazul în care un produs cu elemente digitale face obiectul mai multor acte ale Uniunii care impun o declarație de conformitate UE, se întocmește o singură declarație de conformitate UE în temeiul tuturor acestor acte ale Uniunii. Declarația respectivă conține elementele de identificare a actelor în cauză ale Uniunii, inclusiv referințele de publicare ale acestora.

(4) Prin întocmirea declarației de conformitate UE, producătorul își asumă responsabilitatea pentru conformitatea produsului.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin adăugarea de elemente la conținutul minim al declarației de conformitate UE prevăzute în anexa IV, pentru a ține seama de evoluțiile tehnologice.

Articolul 21

Principii generale ale marcajului CE

Marcajul CE, astfel cum este definit la articolul 3 punctul (32), este supus principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.

Articolul 22

Reguli și condiții privind aplicarea marcajului CE

(1) Marcajul CE se aplică în mod vizibil, lizibil și indelebil pe produsul cu elemente digitale. În cazul în care acest lucru nu este posibil sau nu este justificat din cauza naturii produsului cu elemente digitale, marcajul se aplică pe ambalaj și pe declarația de conformitate UE menționată la articolul 20 care însoțește produsul cu elemente digitale. Pentru produsele cu elemente digitale care sunt sub formă de software, marcajul CE se aplică fie pe declarația de conformitate UE menționată la articolul 20, fie pe site-ul care însoțește produsul software. ***În această ultimă situație, secțiunea relevantă a site-ului trebuie să fie accesibilă cu ușurință și în mod direct pentru consumatori.***

(2) În funcție de natura produsului cu elemente digitale, înălțimea marcajului CE aplicat pe produsul respectiv poate fi mai mică de 5 mm, cu condiția ca acesta să rămână vizibil și lizibil.

(3) Marcajul CE se aplică înainte ca produsul cu elemente digitale să fie introdus pe piață. Acesta poate fi urmat de o pictogramă sau de orice alt marcaj care indică un risc special sau o utilizare specială prevăzut(ă) în actele de punere în aplicare menționate la alineatul (6).

(4) Marcajul CE este urmat de numărul de identificare al organismului notificat, în cazul în care organismul respectiv este implicat în procedura de evaluare a conformității bazată pe asigurarea totală a calității (pe baza modulului H) menționată la articolul 24.

Numărul de identificare al organismului notificat se aplică chiar de către organismul notificat sau, la instrucțiunile acestuia, de către producător sau de către reprezentantul autorizat al acestuia.

(5) Statele membre se bazează pe mecanismele existente pentru a asigura aplicarea corectă a regimului aplicabil marcajului CE și întreprind acțiuni corespunzătoare în cazul

utilizării inadecvate a respectivului marcaj. În cazul în care produsul cu elemente digitale face obiectul altor acte legislative ale Uniunii care prevăd și aplicarea marcajului CE, marcajul indică faptul că produsul îndeplinește și cerințele celorlalte acte legislative.

(6) ***După consultarea grupului de experți, a grupului specific de cooperare administrativă (ADCO) și, dacă este cazul, a altor părți interesate,*** Comisia poate stabili, prin intermediul unor acte delegate, specificații tehnice pentru ***sistemele de etichetare, inclusiv etichete armonizate***, pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale, ***perioada de sprijin*** și mecanisme de promovare a utilizării acestora ***în rândul întreprinderilor și al consumatorilor și pentru a îmbunătăți conștientizarea în rândul publicului cu privire la securitatea produselor cu elemente digitale.*** Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Articolul 23

Documentația tehnică

(1) Documentația tehnică conține toate datele sau detaliile relevante referitoare la mijloacele utilizate de producător pentru a se asigura că produsul cu elemente digitale și procesele instituite de producător respectă cerințele esențiale prevăzute în anexa I. Aceasta conține cel puțin elementele prevăzute în anexa V.

(2) Documentația tehnică se întocmește înainte de introducerea pe piață a produsului cu elemente digitale și se actualizează în permanență, după caz, ***cel puțin pe durata perioadei de sprijin***.

(3) Pentru produsele cu elemente digitale menționate la articolul 8 și la articolul 24 alineatul (4) care fac, de asemenea, obiectul altor acte ale Uniunii, se întocmește o singură documentație tehnică care conține informațiile menționate în anexa V la prezentul regulament și informațiile prevăzute în respectivele acte ale Uniunii.

(4) Documentația tehnică și corespondența referitoare la orice procedură de evaluare a conformității se întocmesc în una dintre limbile oficiale ale statului membru în care este stabilit organismul notificat sau într-o limbă acceptată de acesta.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament cu elementele care trebuie incluse în documentația tehnică prevăzută în anexa V, pentru a ține seama de evoluțiile tehnologice, precum și de situațiile întâlnite în procesul de punere în aplicare a prezentului regulament. ***Comisia se asigură că sarcina administrativă pentru microîntreprinderi și întreprinderile mici și mijlocii are un caracter proporționat.***

Articolul 24

Proceduri de evaluare a conformității pentru produsele cu elemente digitale

(1) Producătorul efectuează o evaluare a conformității produsului cu elemente digitale și a proceselor instituite de producător pentru a stabili dacă sunt îndeplinite cerințele esențiale prevăzute în anexa I. Producătorul sau reprezentantul autorizat al producătorului demonstrează conformitatea cu cerințele esențiale utilizând una dintre procedurile următoare:

(a) procedura controlului intern (pe baza modulului A) prevăzută în anexa VI sau

(b) procedura examinării UE de tip (pe baza modulului B) prevăzută în anexa VI, urmată de conformitatea cu tipul UE bazată pe controlul intern al producției (pe baza modulului C) prevăzută în anexa VI sau

(c) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VI;

(ca) un sistem european de certificare a securității cibernetice, adoptat în temeiul Regulamentului (UE) 2019/881, în conformitate cu articolul 18 alineatul (4).

(2) În cazul în care, la evaluarea conformității produsului critic cu elemente digitale din clasa I prevăzută în anexa III și a proceselor instituite de producătorul său cu cerințele esențiale prevăzute în anexa I, producătorul sau reprezentantul autorizat al producătorului nu a aplicat sau a aplicat doar parțial standardele armonizate, specificațiile comune sau sistemele europene de certificare de securitate cibernetică ***cu nivelul de asigurare „substanțial” sau „ridicat”*** menționate la articolul 18 sau în cazul în care nu există astfel de standarde armonizate, specificații comune sau sisteme europene de certificare de securitate cibernetică, produsul cu elemente digitale și

procesele instituite de producător sunt supuse, în ceea ce privește cerințele esențiale respective, uneia dintre procedurile următoare:

(a) procedura examinării UE de tip (pe baza modulului B), prevăzută în anexa VI, urmată de conformitatea cu tipul UE bazată pe controlul intern al producției (pe baza modulului C), prevăzută în anexa VI sau

(b) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VI.

(2a) Standardele armonizate, specificațiile comune sau sistemele europene de certificare de securitate cibernetică sunt în vigoare cu șase luni înainte de aplicarea procedurii de evaluare a conformității menționate la alineatul (2) de la prezentul articol. În cele șase luni anterioare aplicării alineatului (2) de la prezentul articol sau în cazul în care nu există standarde armonizate, specificații comune sau sisteme europene de certificare de securitate cibernetică, producătorii demonstrează conformitatea produsului esențial cu elementele digitale din clasa I, astfel cum se prevede în anexa III, prin intermediul procedurii menționate la alineatul (1) de la prezentul articol.

(3) În cazul în care produsul este un produs critic cu elemente digitale din clasa II prevăzută în anexa III, producătorul sau reprezentantul autorizat al producătorului demonstrează conformitatea cu cerințele esențiale prevăzute în anexa I utilizând una dintre procedurile următoare:

(-a) un certificat european de securitate cibernetică, emis conform unui sistem european de certificare a securității cibernetice, cu nivelul de asigurare „substanțial” sau „ridicat”, în temeiul Regulamentului (UE) 2019/881.

(a) procedura examinării UE de tip (pe baza modulului B) prevăzută în anexa VI, urmată de conformitatea cu tipul UE bazată pe controlul intern al producției (pe baza modulului C) prevăzută în anexa VI sau

(b) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VI.

(3a) Comisia solicită ENISA să pregătească propunerile de sisteme care lipsesc în conformitate cu articolul 48 din Regulamentul (UE) 2019/881.

(4) Producătorii de produse cu elemente digitale care sunt clasificate drept sisteme DES și ***sunt vizate de*** Regulamentul [Regulamentul privind spațiul european al datelor privind sănătatea] demonstrează conformitatea cu cerințele esențiale prevăzute în anexa I la prezentul regulament utilizând procedura relevantă de evaluare a conformității impusă de Regulamentul [capitolul III din Regulamentul privind spațiul european al datelor privind sănătatea].

(5) Atunci când stabilesc taxele pentru procedurile de evaluare a conformității, organismele notificate țin seama de interesele și nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii ▌ și reduc taxele respective în mod proporțional cu interesele și nevoile specifice ale acestora. ***Comisia asigură un sprijin financiar adecvat în cadrul de reglementare al programelor existente ale Uniunii, în special pentru a ușura sarcina financiară a microîntreprinderilor și a întreprinderilor mici și mijlocii.***

Articolul 24a

Acorduri de recunoaștere reciprocă

Pentru a promova comerțul internațional, Comisia depune eforturi pentru a încheia acorduri de recunoaștere reciprocă (ARR) cu țări terțe. Uniunea încheie ARR numai cu țările terțe care beneficiază de un nivel de dezvoltare tehnică comparabil și care au o abordare compatibilă privind evaluarea conformității. Acordurile asigură același nivel de protecție ca cel prevăzut de prezentul regulament.

CAPITOLUL IV

NOTIFICAREA ORGANISMELOR DE EVALUARE A CONFORMITĂȚII

Articolul 25

Notificare

Statele membre notifică Comisiei și celorlalte state membre organismele de evaluare a conformității autorizate să efectueze evaluări ale conformității în conformitate cu prezentul regulament.

Articolul 26

Autoritățile de notificare

(1) Statele membre desemnează o autoritate de notificare care este responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea și notificarea organismelor de evaluare a conformității și cu monitorizarea organismelor notificate, incluzând conformitatea cu dispozițiile de la articolul 31.

(2) Statele membre pot decide ca evaluarea și monitorizarea menționate la alineatul (1) să fie efectuate de un organism național de acreditare în sensul și în conformitate cu Regulamentul (CE) nr. 765/2008.

Articolul 27

Cerințe privind autoritățile de notificare

(1) Autoritatea de notificare trebuie să fie instituită astfel încât să nu existe conflicte de interese cu organismele de evaluare a conformității.

(2) Autoritatea de notificare trebuie să fie organizată și să funcționeze astfel încât să se garanteze obiectivitatea și imparțialitatea activităților sale.

(3) Autoritatea de notificare trebuie să fie organizată astfel încât fiecare decizie cu privire la notificarea organismului de evaluare a conformității să fie luată de persoanele competente, altele decât cele care au efectuat evaluarea.

(4) Autoritatea de notificare nu oferă și nu prestează activități pe care le desfășoară organismele de evaluare a conformității sau servicii de consultanță în condiții comerciale sau concurențiale.

(5) Autoritatea de notificare garantează confidențialitatea informațiilor obținute.

(6) Autoritatea de notificare trebuie să dispună de personal competent suficient pentru a-și îndeplini sarcinile în mod corespunzător.

(6a) Autoritatea de notificare reduce la minimum sarcinile administrative și taxele impuse îndeosebi microîntreprinderilor și întreprinderilor mici și mijlocii.

Articolul 28

Obligația de informare a autorităților de notificare

(1) Statele membre informează Comisia în legătură cu procedurile lor de evaluare și notificare a organismelor de evaluare a conformității și de monitorizare a organismelor notificate, precum și în legătură cu orice modificări ale acestora.

(1a) În termen de ... [24 de luni de la intrarea în vigoare a prezentului regulament], statele membre se asigură că în Uniune există un număr suficient de organisme notificate pentru efectuarea evaluări ale conformității, pentru a evita blocajele și obstacolele în calea accesului pe piață.

(2) Comisia pune la dispoziția publicului informațiile respective.

Articolul 29

Cerințele în materie de organisme notificate

(1) Pentru a fi notificat, un organism de evaluare a conformității trebuie să îndeplinească cerințele prevăzute la alineatele (2)-(12).

(2) Organismul de evaluare a conformității trebuie să fie înființat în temeiul dreptului intern și să aibă personalitate juridică.

(3) Organismul de evaluare a conformității trebuie să fie un organism terț, independent de organizația sau de produsul pe care îl evaluează.

Un organism care aparține unei asociații de afaceri sau unei federații profesionale care reprezintă întreprinderile implicate în proiectarea, dezvoltarea, producția, furnizarea, asamblarea, utilizarea sau întreținerea produselor cu elemente digitale pe care le evaluează poate fi considerat a fi un astfel de organism, cu condiția să se demonstreze că este independent și că nu există conflicte de interese.

(4) Organismul de evaluare a conformității, personalul de conducere și personalul responsabil cu îndeplinirea sarcinilor de evaluare a conformității nu trebuie să aibă calitatea de proiectant, dezvoltator, producător, furnizor, instalator, cumpărător, proprietar, utilizator sau operator de întreținere al produselor pe care le evaluează, și nici de reprezentant autorizat al vreuneia dintre părțile menționate. Acest lucru nu împiedică utilizarea produselor evaluate care sunt necesare pentru operațiunile

organismului de evaluare a conformității sau utilizarea produselor respective în scopuri personale.

Un organism de evaluare a conformității, personalul de conducere și personalul responsabil cu îndeplinirea sarcinilor de evaluare a conformității nu trebuie să aibă o implicare directă în proiectarea, dezvoltarea, producția, comercializarea, instalarea, utilizarea sau întreținerea produselor respective, și nici să reprezinte părțile angajate în activitățile menționate. Aceștia nu se implică în activități care le-ar putea afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității pentru care sunt notificați. Aceste dispoziții se aplică în special serviciilor de consultanță.

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

(5) Organismele de evaluare a conformității și personalul acestora îndeplinesc activitățile de evaluare a conformității la cel mai înalt grad de integritate profesională și cu competența tehnică necesară în domeniul respectiv și trebuie să fie libere de orice presiune și stimulent, îndeosebi financiare, care le-ar putea influența aprecierea sau ar putea influența rezultatele activităților lor de evaluare a conformității, în special din partea persoanelor sau a grupurilor de persoane care au un interes față de rezultatele activităților respective.

(6) Organismul de evaluare a conformității trebuie să poată să îndeplinească toate sarcinile de evaluare a conformității care sunt menționate în anexa VI și pentru care a fost notificat, indiferent dacă atribuțiile respective sunt îndeplinite chiar de organismul de evaluare a conformității sau în numele și sub responsabilitatea acestuia.

În orice moment și pentru fiecare procedură de evaluare a conformității și pentru fiecare tip sau categorie de produse pentru care este notificat, organismul de evaluare a conformității trebuie să aibă la dispoziție:

(a) personalul necesar, având cunoștințele tehnice necesare și experiență suficientă și corespunzătoare pentru a îndeplini sarcinile de evaluare a conformității;

(b) descrierile necesare ale procedurilor în conformitate cu care se realizează evaluarea conformității, asigurându-se transparența și posibilitatea de a

reproduce procedurile în cauză. Organismul de evaluare a conformității trebuie să dispună de politici și proceduri adecvate, care să facă o distincție clară între sarcinile îndeplinite ca organism notificat și orice alte activități;

(c) procedurile necesare pentru a-și desfășura activitatea ținând seama în mod corespunzător de dimensiunea unei întreprinderi, de domeniul de activitate și de structura acesteia, de gradul de complexitate al tehnologiei utilizate pentru produse, precum și de caracterul de serie sau de masă al procesului de producție.

Organismul de evaluare a conformității trebuie să dispună de mijloacele necesare pentru a îndeplini sarcinile tehnice și administrative legate de activitățile de evaluare a conformității în mod corespunzător și să aibă acces la toate echipamentele și facilitățile necesare.

(7) Personalul responsabil de îndeplinirea activităților de evaluare a conformității trebuie să posede următoarele:

(a) o pregătire tehnică și profesională solidă care să acopere toate activitățile de evaluare a conformității pentru care organismul de evaluare a conformității a fost notificat;

(b) cunoștințe satisfăcătoare cu privire la cerințele evaluărilor pe care le realizează și autoritatea necesară pentru realizarea acestor evaluări;

(c) cunoștințe și o înțelegere corespunzătoare a cerințelor esențiale ***stabilite în anexa I***, a standardelor armonizate aplicabile și a dispozițiilor relevante din legislația de armonizare a Uniunii și din actele de punere în aplicare a acesteia;

(d) capacitatea de a întocmi certificate, procese-verbale și rapoarte care să demonstreze că evaluările au fost efectuate.

(7a) Statele membre și Comisia instituie măsuri adecvate pentru a asigura o disponibilitate suficientă a profesioniștilor calificați, în vederea reducerii la minimum a blocajelor în activitățile organismelor de evaluare a conformității și a facilitării respectării prezentului regulament de către operatorii economici.

(8) Imparțialitatea organismelor de evaluare a conformității, a personalului de conducere și a personalului de evaluare al acestora trebuie să fie garantată.

Remunerația personalului de conducere și a personalului de evaluare al organismului de evaluare a conformității nu trebuie să depindă de numărul de evaluări realizate sau de rezultatele acestor evaluări.

(9) Organismele de evaluare a conformității încheie o asigurare de răspundere dacă răspunderea nu este asumată de stat în conformitate cu dreptul intern sau dacă statul membru respectiv nu este direct responsabil pentru evaluarea conformității.

(10) Personalul organismului de evaluare a conformității păstrează secretul profesional referitor la toate informațiile obținute în îndeplinirea sarcinilor sale în temeiul anexei VI sau al oricărei dispoziții din legislația națională de punere în aplicare a acesteia, excepție făcând relația cu autoritățile de supraveghere a pieței ale statului membru în care își desfășoară activitățile. Drepturile de autor sunt protejate ***în conformitate cu articolul 52***. Organismul de evaluare a conformității trebuie să dispună de proceduri documentate care să asigure conformitatea cu prezentul alineat.

(11) Organismele de evaluare a conformității trebuie să participe la activitățile de standardizare relevante și la activitățile grupului de coordonare a organismelor notificate înființat în temeiul articolului 40 sau să se asigure că personalul lor de evaluare este informat cu privire la aceste activități și trebuie să pună în aplicare ca orientare generală deciziile și documentele administrative produse ca rezultat al activității grupului respectiv.

(12) Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termene și condiții coerente, echitabile și rezonabile, ***în conformitate cu articolul 37 alineatul (2),*** ținând seama în mod special de interesele ***microîntreprinderilor și ale întreprinderilor mici și mijlocii*** în ceea ce privește taxele.

Articolul 30

Prezumția de conformitate a organismelor notificate

În cazul în care un organism de evaluare a conformității își demonstrează conformitatea cu criteriile prevăzute în standardele armonizate relevante sau în anumite părți din acestea, ale căror referințe au fost publicate în Jurnalul Oficial al Uniunii Europene, se consideră că acesta este conform cu cerințele prevăzute la articolul 29, în măsura în care standardele armonizate aplicabile acoperă aceste cerințe.

Articolul 31

Filialele organismelor notificate și subcontractarea de către organismele notificate

(1) În cazul în care subcontractează anumite sarcini legate de evaluarea conformității sau recurge la o filială, organismul notificat se asigură că subcontractantul sau filiala îndeplinește cerințele prevăzute la articolul 29 și informează autoritatea de notificare în acest sens.

(2) Organismele notificate își asumă întreaga responsabilitate pentru sarcinile îndeplinite de subcontractanți sau de filiale, indiferent de locul în care sunt stabiliți (stabilite) aceștia (acestea).

(3) Activitățile pot fi subcontractate sau realizate de o filială doar cu acordul producătorului.

(4) Organismele notificate pun la dispoziția autorității de notificare documentele relevante privind evaluarea calificărilor subcontractantului sau ale filialei și privind activitățile îndeplinite de acesta (aceasta) în temeiul prezentului regulament.

Articolul 32

Cererea de notificare

(1) Organismul de evaluare a conformității depune o cerere de notificare către autoritatea de notificare a statului membru în care este stabilit.

(2) Această cerere este însoțită de o descriere a activităților de evaluare a conformității, a procedurii sau procedurilor de evaluare a conformității și a produsului sau produselor pentru care organismul se consideră a fi competent, precum și de un certificat de acreditare, în cazul în care acesta există, eliberat de un organism național de acreditare, care să ateste că organismul de evaluare a conformității îndeplinește cerințele prevăzute la articolul 29.

(3) În cazul în care organismul de evaluare a conformității în cauză nu poate prezenta un certificat de acreditare, acesta prezintă autorității de notificare toate documentele justificative necesare pentru verificarea, recunoașterea și monitorizarea periodică a conformității sale cu cerințele prevăzute la articolul 29.

Articolul 33

Procedura de notificare

(1) Autoritățile de notificare pot notifica numai organismele de evaluare a conformității care au îndeplinit cerințele prevăzute la articolul 29.

(2) Autoritatea de notificare notifică Comisia și celelalte state membre utilizând sistemul informațional NANDO (New Approach Notified and Designated Organisations – Noua abordare privind organizațiile notificate și desemnate), dezvoltat și gestionat de Comisie.

(3) Notificarea include detalii complete despre activitățile de evaluare a conformității, despre modulul sau modulele de evaluare a conformității și despre produsul sau produsele în cauză, precum și atestarea relevantă a competenței.

(4) În cazul în care notificarea nu se bazează pe certificatul de acreditare menționat la articolul 32 alineatul (2), autoritatea de notificare prezintă Comisiei și celorlalte state membre documente justificative care atestă competența organismului de evaluare a conformității și măsurile adoptate pentru a se asigura că organismul respectiv va fi monitorizat periodic și că va îndeplini în continuare cerințele prevăzute la articolul 29.

(5) Organismul în cauză poate efectua activitățile unui organism notificat numai în cazul în care Comisia sau celelalte state membre nu au ridicat obiecții în termen de două săptămâni de la notificare, atunci când se utilizează un certificat de acreditare, sau în termen de două luni de la notificare, atunci când nu se utilizează acreditarea.

Numai un astfel de organism este considerat organism notificat în sensul prezentului regulament.

(6) Comisia și celelalte state membre sunt înștiințate cu privire la orice modificări relevante ulterioare aduse notificării.

Articolul 34

Numerele de identificare și listele cu organismele notificate

(1) Comisia atribuie organismului notificat un număr de identificare.

Comisia atribuie un singur număr de identificare organismului notificat, chiar dacă acesta este notificat în temeiul mai multor acte ale Uniunii.

(2) Comisia pune la dispoziția publicului lista organismelor notificate în baza prezentului regulament, inclusiv numerele de identificare care le-au fost alocate și activitățile pentru care au fost notificate.

Comisia se asigură că această listă este actualizată.

Articolul 35

Modificări ale notificărilor

(1) În cazul în care o autoritate de notificare a constatat sau a fost informată că un organism notificat nu mai îndeplinește cerințele prevăzute la articolul 29 sau că acesta nu își îndeplinește obligațiile, autoritatea de notificare restricționează, suspendă sau retrage notificarea, după caz, în funcție de gravitatea încălcării cerințelor sau a neîndeplinirii obligațiilor. Aceasta informează imediat Comisia și celelalte state membre în consecință.

(2) În caz de restricționare, suspendare sau retragere a notificării sau în cazul în care organismul notificat și-a încetat activitatea, statul membru notificator ia măsurile adecvate pentru a se asigura că dosarele organismului respectiv fie sunt prelucrate de un alt organism notificat, fie sunt puse la dispoziția autorităților de notificare și de supraveghere a pieței responsabile, la cererea acestora.

Articolul 36

Contestarea competenței organismelor notificate

(1) Comisia investighează toate cazurile în care are îndoieli sau i se aduc la cunoștință îndoieli privind competența unui organism notificat sau continuitatea îndeplinirii de către un organism notificat a cerințelor și a responsabilităților care îi revin.

(2) Statul membru notificator prezintă Comisiei, la cerere, toate informațiile referitoare la baza notificării sau la menținerea competenței organismului în cauză.

(3) Comisia se asigură că toate informațiile sensibile obținute pe parcursul investigațiilor sale sunt tratate în mod confidențial.

(4) În cazul în care constată că un organism notificat nu satisface sau nu mai satisface cerințele pentru a fi notificat, Comisia informează statul membru notificator în

consecință și solicită acestuia să ia măsurile corective necesare, inclusiv anularea notificării, dacă este necesar.

Articolul 37

Obligații operaționale pentru organismele notificate

(1) Organismele notificate efectuează evaluări ale conformității în conformitate cu procedurile de evaluare a conformității prevăzute la articolul 24 și în anexa VI.

(2) Evaluarea conformității se efectuează în mod proporțional, evitând sarcinile inutile pentru operatorii economici, ***ținând cont de interesele microîntreprinderilor și ale întreprinderilor mici și mijlocii***. Organismul de evaluare a conformității își desfășoară activitatea ținând seama în mod corespunzător de dimensiunea întreprinderii, de domeniul de activitate și structura acesteia, de gradul de complexitate ***și de expunerea la risc a tipului*** de produs și a tehnologiei utilizate pentru produse, precum și de caracterul de serie sau de masă al procesului de producție.

(3) Cu toate acestea, organismele notificate respectă gradul de precizie și nivelul de protecție necesare pentru conformitatea produsului cu dispozițiile regulamentului.

(4) În cazul în care un organism notificat constată că cerințele prevăzute în anexa I sau în standardele armonizate corespunzătoare sau în specificațiile tehnice menționate la articolul 19 nu au fost îndeplinite de către un producător, acesta solicită producătorului să ia măsurile corective adecvate și nu emite certificatul de conformitate.

(5) Atunci când pe parcursul monitorizării conformității efectuate după eliberarea certificatului organismul notificat constată că un produs nu mai este conform cu cerințele prevăzute în prezentul regulament, acesta solicită producătorului să ia măsurile corective adecvate și suspendă sau retrage certificatul, dacă este necesar.

(6) În cazul în care nu se iau măsuri corective sau acestea nu au efectul necesar, organismul notificat restricționează, suspendă sau retrage certificatele, după caz.

Articolul 38

Obligații de informare în sarcina organismelor notificate

(1) Organismele notificate informează autoritatea de notificare în legătură cu:

(a) orice refuzare, restricționare, suspendare sau retragere a unui certificat;

(b) orice circumstanțe care afectează domeniul de aplicare și condițiile notificării;

(c) orice cerere de informare cu privire la activitățile de evaluare a conformității desfășurate, primită de la autoritățile de supraveghere a pieței;

(d) la cerere, activitățile de evaluare a conformității realizate în limita domeniului de aplicare al notificării și orice altă activitate realizată, inclusiv activitățile transfrontaliere și subcontractările.

(2) Organismele notificate furnizează celorlalte organisme notificate în temeiul prezentului regulament care desfășoară activități similare de evaluare a conformității referitoare la aceleași produse informații relevante privind aspecte legate de rezultatele negative și, la cerere, de rezultatele pozitive ale evaluării conformității.

Articolul 39

Schimbul de experiență

Comisia asigură organizarea unui schimb de experiență între autoritățile naționale ale statelor membre responsabile de politica privind notificarea.

Articolul 40

Coordonarea organismelor notificate

(1) Comisia se asigură că între organismele notificate există o coordonare și o cooperare adecvată***, ținând seama și de necesitatea de a reduce sarcina administrativă și taxele,*** care funcționează în cadrul unui grup transsectorial al organismelor notificate.

(2) Statele membre se asigură că organismele notificate de ele participă la activitatea grupului respectiv, în mod direct sau prin intermediul unor reprezentanți desemnați.

CAPITOLUL V

SUPRAVEGHEREA PIEȚEI ȘI ASIGURAREA RESPECTĂRII LEGISLAȚIEI

Articolul 41

Supravegherea pieței și controlul produselor cu elemente digitale pe piața Uniunii

(1) Regulamentul (UE) 2019/1020 se aplică produselor cu elemente digitale care intră în domeniul de aplicare al prezentului regulament.

(2) Fiecare stat membru desemnează una sau mai multe autorități de supraveghere a pieței cu scopul de a asigura punerea în aplicare eficace a prezentului regulament. Statele membre pot desemna o autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței pentru prezentul regulament.

(3) Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu autoritățile naționale de certificare a securității cibernetice desemnate în temeiul articolului 58 din Regulamentul (UE) 2019/881***, cu autoritățile competente și cu CSIRT desemnate în temeiul Directivei (UE) 2022/2555*** și fac schimb de informații în mod regulat. ▌

(3a) În ceea ce privește supravegherea punerii în aplicare a obligațiilor de raportare în temeiul articolului 11 din prezentul regulament, autoritățile de supraveghere a pieței desemnate cooperează cu ENISA. Autoritățile de supraveghere a pieței pot solicita ENISA să furnizeze consiliere tehnică pe teme legate de punerea în aplicare și asigurarea respectării prezentului regulament. Atunci când efectuează o investigație în temeiul articolului 43, autoritățile de supraveghere a pieței pot solicita ENISA să ofere evaluări fără caracter obligatoriu în ceea ce privește conformitatea produselor cu elemente digitale.

(4) Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu alte autorități de supraveghere a pieței desemnate în temeiul altor acte din legislația de armonizare a Uniunii pentru alte produse și fac schimb de informații în mod regulat.

(5) Autoritățile de supraveghere a pieței cooperează, după caz, cu autoritățile care supraveghează legislația Uniunii în domeniul protecției datelor. O astfel de cooperare include informarea acestor autorități cu privire la orice constatare relevantă pentru îndeplinirea competențelor lor, inclusiv atunci când se emit orientări și recomandări în temeiul alineatului (8) din prezentul articol, în cazul în care aceste orientări și recomandări se referă la prelucrarea datelor cu caracter personal.

Autoritățile care supraveghează legislația Uniunii în domeniul protecției datelor au competența de a solicita și de a accesa orice documentație creată sau păstrată în temeiul prezentului regulament atunci când accesul la documentația respectivă este necesar pentru îndeplinirea sarcinilor lor. Acestea informează autoritățile de supraveghere a pieței desemnate din statul membru în cauză cu privire la orice astfel de solicitare.

(6) Statele membre se asigură că autoritățile naționale competente dispun de resurse financiare și umane adecvate***, cu competențe corespunzătoare în materie de securitate cibernetică,*** pentru a-și îndeplini sarcinile care le revin în temeiul prezentului regulament.

(7) Comisia facilitează schimbul de experiență ***periodic și structurat*** între autoritățile de supraveghere a pieței desemnate.

(8) Autoritățile de supraveghere a pieței pot oferi orientări și recomandări operatorilor economici cu privire la punerea în aplicare a prezentului regulament***, precum și în ceea ce privește factorii de risc fără caracter tehnic,*** cu sprijinul ***CSIRT, al ENISA și al*** Comisiei.

(8a) Autoritățile de supraveghere a pieței sunt în măsură să primească plângeri din partea consumatorilor în conformitate cu articolul 11 din Regulamentul 2019/1020, inclusiv prin stabilirea unor mecanisme clare și accesibile pentru facilitarea raportării vulnerabilităților, incidentelor și amenințărilor cibernetice.

(9) Autoritățile de supraveghere a pieței raportează anual Comisiei rezultatele activităților relevante de supraveghere a pieței. Autoritățile de supraveghere a pieței desemnate raportează fără întârziere Comisiei și autorităților naționale de concurență relevante toate informațiile identificate în cursul activităților de supraveghere a pieței care ar putea prezenta interes pentru aplicarea legislației Uniunii în domeniul concurenței.

Autoritățile de supraveghere a pieței furnizează Comisiei date cu privire la perioada de asistență medie stabilită de producători, precum și cu privire la durata de viață preconizată a produsului, atunci când aceasta este disponibilă, defalcate pe categorii de produse cu elemente digitale. Comisia analizează aceste informații și le publică într-o bază de date accesibilă publicului și ușor de utilizat.

(9a) Comisia evaluează datele raportate, inclusiv în temeiul alineatului (9) de la prezentul articol, în scopul rapoartelor menționate la articolul 56. În cazul în care datele raportate sugerează un nivel crescut de neconformitate pentru anumite categorii de produse, Comisia, după consultarea grupului de experți și a ADCO, poate recomanda ca autoritățile de supraveghere să se concentreze îndeaproape asupra categoriilor de produse vizate.

(10) Pentru produsele cu elemente digitale care intră în domeniul de aplicare al prezentului regulament și care sunt clasificate drept sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială], autoritățile de supraveghere a pieței desemnate în sensul Regulamentului [Regulamentul privind inteligența artificială] sunt autoritățile responsabile cu activitățile de supraveghere a pieței necesare în temeiul prezentului regulament. Autoritățile de supraveghere a pieței desemnate în temeiul Regulamentului [Regulamentul privind inteligența artificială] cooperează, după caz, cu autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament și, în ceea ce privește supravegherea punerii în aplicare a obligațiilor de raportare în temeiul articolului 11, cu ENISA. Autoritățile de supraveghere a pieței desemnate în temeiul Regulamentului [Regulamentul privind inteligența artificială] informează în special autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament cu privire la orice constatare relevantă pentru îndeplinirea sarcinilor lor legate de punerea în aplicare a prezentului regulament.

(11) Se instituie un ▌ADCO ***pentru reziliența cibernetică a produselor cu elemente digitale,*** pentru aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO trebuie să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate și, dacă este cazul, din reprezentanți ai birourilor unice de legătură. ***În special, acest ADCO face schimb de bune practici și, atunci când este relevant, cooperează cu grupul de experți și cu ENISA, precum și cu grupul de cooperare și cu rețeaua CSIRT menționată în Directiva (UE) 2022/2555.***

(11a) Autoritățile de supraveghere a pieței facilitează implicarea părților interesate, inclusiv a organizațiilor științifice, de cercetare și a organizațiilor de consumatori, în activitățile lor.

Articolul 42

Accesul la date și la documentație

În cazul în care este necesar pentru a evalua conformitatea produselor cu elemente digitale și a proceselor instituite de producătorii lor cu cerințele esențiale prevăzute în anexa I și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă acces la datele necesare

pentru a evalua proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților acestor produse, inclusiv la documentația internă aferentă a operatorului economic respectiv.

Articolul 43

Procedura la nivel național privind produsele cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică

(1) În cazul în care autoritatea de supraveghere a pieței dintr-un stat membru are motive suficiente să considere că un produs cu elemente digitale, inclusiv gestionarea vulnerabilităților sale, prezintă un risc semnificativ în materie de securitate cibernetică, aceasta efectuează***, fără întârzieri nejustificate și, după caz, în cooperare cu CSIRT,*** o evaluare a respectivului produs cu elemente digitale în ceea ce privește conformitatea sa cu toate cerințele prevăzute în prezentul regulament. Operatorii economici relevanți cooperează cu autoritatea de supraveghere a pieței în funcție de necesități.

În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că produsul cu elemente digitale nu respectă cerințele prevăzute în prezentul regulament, aceasta solicită fără întârziere operatorului ***economic*** relevant să întreprindă toate acțiunile corective adecvate pentru a aduce produsul în conformitate cu cerințele sau pentru a retrage produsul de pe piață ori pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului și stabilit de autoritatea respectivă.

Autoritatea de supraveghere a pieței informează organismul notificat relevant în consecință. Articolul 18 din Regulamentul (UE) 2019/1020 se aplică acțiunilor corective adecvate.

(1a) În cazul în care autoritatea de supraveghere a pieței dintr-un stat membru are motive suficiente să considere că un produs cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică sau amenințări semnificative la adresa securității naționale în lumina unor factori de risc netehnici, aceasta adresează recomandări specifice operatorilor economici, cu scopul de a se asigura că sunt puse în aplicare acțiuni corective adecvate.

(2) În cazul în care autoritatea de supraveghere a pieței consideră că neconformitatea nu se limitează la teritoriul său național, aceasta informează Comisia și celelalte state membre cu privire la rezultatele evaluării și la acțiunile pe care le-a impus operatorului.

(3) Producătorul se asigură că sunt întreprinse toate acțiunile corective adecvate pentru toate produsele cu elemente digitale în cauză pe care acesta le-a pus la dispoziție pe piață în întreaga Uniune.

(4) În cazul în care producătorul unui produs cu elemente digitale nu întreprinde acțiuni corective adecvate în termenul menționat la alineatul (1) al doilea paragraf, autoritatea de supraveghere a pieței ia toate măsurile provizorii adecvate pentru a interzice sau a restricționa punerea la dispoziție a produsului respectiv pe piața sa națională, pentru a-l retrage de pe piață sau pentru a-l rechema.

Autoritatea respectivă informează Comisia și celelalte state membre, fără întârziere, cu privire la aceste măsuri.

(5) Informațiile menționate la alineatul (4) trebuie să cuprindă toate detaliile disponibile, în special datele necesare pentru identificarea produselor cu elemente digitale care sunt neconforme, originea produsului cu elemente digitale, natura neconformității invocate și riscul pe care aceasta îl implică, natura și durata măsurilor naționale adoptate, precum și argumentele prezentate de operatorul relevant. În special, autoritatea de supraveghere a pieței indică dacă neconformitatea se datorează unuia sau mai multora dintre motivele următoare:

(a) nerespectarea de către produs sau de către procesele instituite de producător a cerințelor esențiale prevăzute în anexa I;

(b) deficiențe ale standardelor armonizate, ale sistemelor de certificare de securitate cibernetică sau ale specificațiilor comune menționate la articolul 18.

(6) Autoritățile de supraveghere a pieței din statele membre, altele decât autoritatea de supraveghere a pieței din statul membru care a inițiat procedura, informează fără întârziere Comisia și celelalte state membre cu privire la toate măsurile adoptate și la toate informațiile suplimentare deținute referitoare la neconformitatea produsului în cauză și, în cazul în care nu sunt de acord cu privire la măsura națională notificată, cu privire la obiecțiile lor.

(7) În cazul în care, în termen de trei luni de la primirea informațiilor menționate la alineatul (4), niciun stat membru și nici Comisia nu ridică vreo obiecție cu privire la o măsură provizorie luată de un stat membru, măsura respectivă este considerată justificată. Acest lucru nu aduce atingere drepturilor procedurale care îi

revin operatorului în cauză în conformitate cu articolul 18 din Regulamentul (UE) 2019/1020.

(8) Autoritățile de supraveghere a pieței din toate statele membre se asigură că se iau măsuri restrictive adecvate în ceea ce privește produsul în cauză, cum ar fi retragerea fără întârziere a produsului de pe piețele lor.

Articolul 44

Procedura de salvgardare a Uniunii

(1) Dacă în termen de trei luni de la primirea notificării menționate la articolul 43 alineatul (4) un stat membru ridică obiecții împotriva unei măsuri adoptate de un alt stat membru sau în cazul în care Comisia consideră că măsura este contrară legislației Uniunii, Comisia inițiază fără întârziere consultări cu statul membru relevant și cu operatorul sau operatorii economici în cauză și evaluează măsura națională. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura națională este justificată sau nu în termen de nouă luni de la notificarea menționată la articolul 43 alineatul (4) și notifică această decizie statului membru în cauză.

(2) În cazul în care măsura națională este considerată justificată, toate statele membre iau măsurile necesare pentru a garanta că produsul cu elemente digitale considerat neconform este retras de pe piețele lor și informează Comisia în consecință. În cazul în care măsura națională este considerată nejustificată, statul membru în cauză retrage măsura.

(3) În cazul în care măsura națională este considerată justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale standardelor armonizate, Comisia aplică procedura prevăzută la articolul 10 din Regulamentul (UE) nr. 1025/2012.

(4) În cazul în care măsura națională este considerată justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale unui sistem european de certificare de securitate cibernetică menționat la articolul 18, Comisia analizează dacă este oportun să modifice sau să abroge actul de punere în aplicare menționat la articolul 18 alineatul (4) care precizează prezumția de conformitate în ceea ce privește sistemul de certificare respectiv.

(5) În cazul în care măsura națională este considerată justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale specificațiilor comune menționate la articolul 19, Comisia analizează dacă este oportun să modifice sau să abroge actul de punere în aplicare menționat la articolul 19 care stabilește specificațiile comune respective.

Articolul 45

Procedura la nivelul UE privind produsele cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică

(1) În cazul în care Comisia are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică nu respectă cerințele prevăzute în prezentul regulament, aceasta ***solicită*** autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43.

(1a) În cazul în care Comisia are motive suficiente să considere că un produs cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică în lumina unor factori de risc netehnici, aceasta informează autoritățile relevante de supraveghere a pieței și adresează recomandări specifice operatorilor economici, cu scopul de a se asigura că sunt puse în aplicare acțiuni corective adecvate.

(2) În circumstanțe ▌care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive suficiente să considere că produsul menționat la alineatul (1) continuă să nu respecte cerințele prevăzute în prezentul regulament, iar autoritățile relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia ***solicită*** ENISA să efectueze o evaluare a conformității. Comisia informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.

(3) Pe baza evaluării realizate de ENISA, Comisia poate decide că este necesară o măsură corectivă sau restrictivă la nivelul Uniunii. În acest scop, Comisia consultă fără întârziere statele membre în cauză și operatorul sau operatorii economici relevanți.

(4) Pe baza consultării menționate la alineatul (3), Comisia poate adopta acte de punere în aplicare pentru a decide cu privire la eventuale măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea, într-un termen rezonabil, proporțional cu natura riscului. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

(5) Comisia comunică imediat decizia menționată la alineatul (4) operatorului sau operatorilor economici relevanți. Statele membre pun în aplicare fără întârziere actele menționate la alineatul (4) și informează Comisia în consecință.

(6) Alineatele (2)-(5) se aplică pe durata situației excepționale care a justificat intervenția Comisiei și atât timp cât produsul respectiv nu este adus în conformitate cu prezentul regulament.

Articolul 46

Produse cu elemente digitale care sunt conforme, dar care prezintă un risc semnificativ în materie de securitate cibernetică

(1) În cazul în care, în urma efectuării unei evaluări în temeiul articolului 43, autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un produs cu elemente digitale și procesele instituite de producător sunt conforme cu prezentul regulament, acestea prezintă un risc semnificativ în materie de securitate cibernetică și, în plus, prezintă un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin intermediul unui sistem informatic electronic de tipul celor menționate ***la articolul 3 din*** Directiva ***(UE) 2022/2555*** sau în ceea ce privește alte aspecte ale protecției interesului public, aceasta impune operatorului ***economic*** relevant să ia toate măsurile adecvate pentru a se asigura că respectivul produs cu elemente digitale și procesele instituite de producătorul în cauză nu mai prezintă riscul respectiv la introducerea pe piață, pentru a retrage produsul cu elemente digitale de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului.

(2) Producătorul sau alți operatori ***economici*** relevanți se asigură că sunt întreprinse acțiuni corective cu privire la produsele cu elemente digitale în cauză pe care aceștia le-au pus la dispoziție pe piață în întreaga Uniune, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).

(3) Statul membru informează imediat Comisia și celelalte state membre cu privire la măsurile luate în temeiul alineatului (1). Informațiile respective includ toate detaliile disponibile, în special datele necesare pentru identificarea respectivelor produse cu elemente digitale, originea și lanțul de aprovizionare aferente acestor produse, natura riscului implicat, precum și natura și durata măsurilor naționale adoptate.

(4) Comisia inițiază fără întârziere consultări cu statele membre și cu operatorul economic relevant și evaluează măsurile naționale adoptate. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura este justificată sau nu și, dacă este cazul, propune măsuri adecvate.

(5) Comisia comunică decizia sa celorlalte state membre.

(6) În cazul în care are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale, deși este conform cu prezentul regulament, prezintă riscurile menționate la alineatul (1), Comisia poate solicita autorității sau autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43 și la alineatele (1), (2) și (3) din prezentul articol.

(7) În circumstanțe ▌care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive suficiente să considere că produsul menționat la alineatul (6) continuă să prezinte riscurile prevăzute la alineatul (1), iar autoritățile naționale relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia poate solicita ENISA să efectueze o evaluare a riscurilor prezentate de produs și informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.

(8) Pe baza evaluării realizate de ENISA, menționată la alineatul (7), Comisia ***stabilește*** ▌o acțiune corectivă sau restrictivă la nivelul Uniunii***, dacă este necesar***. În acest scop,

Comisia consultă fără întârziere statele membre în cauză și operatorul sau operatorii relevanți.

(9) Pe baza consultării menționate la alineatul (8), Comisia poate adopta acte de punere în aplicare pentru a decide cu privire la eventuale măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea, într-un termen rezonabil, proporțional cu natura riscului. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

(10) Comisia comunică imediat decizia menționată la alineatul (9) operatorului sau operatorilor relevanți. Statele membre pun în aplicare fără întârziere aceste acte și informează Comisia în consecință.

(11) Alineatele (6)-(10) se aplică pe durata situației excepționale care a justificat intervenția Comisiei și atât timp cât produsul respectiv continuă să prezinte riscurile menționate la alineatul (1).

Articolul 47

Neconformitatea formală

(1) Autoritatea de supraveghere a pieței dintr-un stat membru solicită producătorului relevant să pună capăt neconformității în cauză, atunci când constată una dintre situațiile următoare:

(a) marcajul de conformitate a fost aplicat cu încălcarea articolului 21 și a articolului 22;

(b) marcajul de conformitate nu a fost aplicat;

(c) declarația de conformitate UE nu a fost întocmită;

(d) declarația de conformitate UE nu a fost întocmită corect;

(e) numărul de identificare al organismului notificat, care este implicat în procedura de evaluare a conformității, în cazurile aplicabile, nu a fost aplicat;

(f) documentația tehnică nu este disponibilă sau este incompletă.

(2) În cazul în care neconformitatea menționată la alineatul (1) persistă, statul membru în cauză ia toate măsurile corespunzătoare pentru a restricționa sau a interzice punerea la

dispoziție pe piață a produsului cu elemente digitale sau pentru a se asigura că acesta este rechemat sau retras de pe piață.

Articolul 48

Activități comune ale autorităților de supraveghere a pieței

(1) Autoritățile de supraveghere a pieței ***desfășoară*** activități comune menite să asigure securitatea cibernetică și protecția consumatorilor în ceea ce privește anumite produse cu elemente digitale introduse sau puse la dispoziție pe piață, în special produsele despre care se constată adesea că prezintă riscuri de securitate cibernetică.

(2) Comisia sau ENISA ***propune*** desfășurarea de activități comune de verificare a conformității cu prezentul regulament de către autoritățile de supraveghere a pieței pe baza unor indicii sau informații privind o potențială neconformitate în mai multe state membre a unor produse care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în acesta.

(3) Autoritățile de supraveghere a pieței și Comisia, după caz, se asigură că acordul privind desfășurarea de activități comune nu duce la o concurență neloială între operatorii economici și nu afectează obiectivitatea, independența și imparțialitatea părților la acord.

(4) O autoritate de supraveghere a pieței poate utiliza orice informație rezultată în urma activităților desfășurate în cadrul oricărei investigații pe care o efectuează.

(5) Respectiva autoritate de supraveghere a pieței și Comisia, după caz, pun la dispoziția publicului acordul privind activitățile comune, inclusiv numele părților implicate.

Articolul 49

Acțiuni de verificare

(1) Autoritățile de supraveghere a pieței ***desfășoară regulat*** acțiuni de control coordonate simultane („acțiuni de verificare”) pentru anumite produse cu elemente digitale sau pentru anumite categorii de astfel de produse, în scopul de a verifica respectarea prezentului regulament sau de a detecta încălcările acestuia. ***Aceste acțiuni includ inspecții ale produselor achiziționate sub o identitate falsă și urmăresc să verifice conformitatea produselor respective cu prezentul regulament.***

(2) Cu excepția cazului în care autoritățile de supraveghere a pieței în cauză convin altfel, acțiunile de verificare sunt coordonate de Comisie. Coordonatorul acțiunii de verificare ***pune*** la dispoziția publicului rezultatele agregate.

(3) ENISA ***identifică***, în îndeplinirea sarcinilor sale, inclusiv pe baza notificărilor primite în conformitate cu articolul 11 alineatele (1) și (2), categoriile de produse pentru care ***se organizează*** acțiuni de verificare. Propunerea de acțiuni de verificare este prezentată coordonatorului potențial menționat la alineatul (2) pentru a fi examinată de autoritățile de supraveghere a pieței.

(4) Atunci când desfășoară acțiuni de verificare, autoritățile de supraveghere a pieței implicate pot utiliza competențele de investigare prevăzute la articolele 41-47 și orice alte competențe care le sunt conferite de dreptul intern.

(5) Autoritățile de supraveghere a pieței ***invită*** funcționari ai Comisiei și alte persoane însoțitoare autorizate de Comisie să participe la acțiunile de verificare.

CAPITOLUL VI

COMPETENȚELE DELEGATE ȘI PROCEDURA COMITETULUI

Articolul 50

Exercitarea delegării

(1) Comisiei i se conferă competența de a adopta acte delegate sub rezerva condițiilor prevăzute la prezentul articol.

(2) Comisiei i se conferă competența de a adopta acte delegate menționată la articolul 2 alineatul (4), la articolul 6 alineatele (2), (3) și (5), ***la articolul 10 alineatul (15), la articolul 11 alineatul (5), la articolul 18 alineatul (4), la articolul 19 alineatul (1),*** la articolul 20 alineatul (5) și la articolul 23 alineatul (5).

(3) Delegarea de competențe menționată la articolul 2 alineatul (4), la articolul 6 alineatele (2), (3) și (5), ***la articolul 10 alineatul (15), la articolul 11 alineatul (5), la articolul 18 alineatul (4), la articolul 19 alineatul (1),*** la articolul 20 alineatul (5) și la articolul 23 alineatul (5) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia

în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu afectează valabilitatea actelor delegate care sunt deja în vigoare.

(4) Înainte de a adopta un act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile stabilite 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 2 alineatul (4), al articolului 6 alineatul (2), (3) sau (5), ***al articolului 10 alineatul (15), al articolului 11 alineatul (5), al articolului 18 alineatul (4), al articolului 19 alineatul (1),*** al articolului 20 alineatul (5) ***sau*** al articolului 23 alineatul (5) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, atât Parlamentul European, cât și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 51

Procedura comitetului

(1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

(2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

(3) În cazul în care avizul comitetului trebuie obținut prin procedură scrisă, această procedură se încheie fără rezultat dacă, înainte de expirarea termenului de transmitere a avizului, acest lucru este hotărât de președintele comitetului sau solicitat un membru al comitetului.

CAPITOLUL VII

CONFIDENȚIALITATE ȘI SANCȚIUNI

Articolul 52

Confidențialitate

(1) Toate părțile implicate în aplicarea prezentului regulament respectă confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și a activităților lor într-un mod care să protejeze în special:

(a) drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale ale unei persoane fizice sau juridice, inclusiv codul sursă, cu excepția cazurilor menționate la articolul 5 din Directiva 2016/943 a Parlamentului European și a Consiliului[38];

(b) punerea efectivă în aplicare a prezentului regulament, în special în scopul inspecțiilor, investigațiilor sau auditurilor;

(c) interesele securității publice și naționale;

(d) integritatea procedurilor penale sau administrative.

(2) Fără a aduce atingere alineatului (1), informațiile transmise în mod confidențial între autoritățile de supraveghere a pieței, precum și între autoritățile de supraveghere a pieței și Comisie nu trebuie divulgate fără acordul prealabil al autorității de supraveghere a pieței care le-a emis.

(3) Alineatele (1) și (2) nu aduc atingere drepturilor și obligațiilor care revin Comisiei, statelor membre și organismelor notificate cu privire la schimbul de informații și la difuzarea avertizărilor, și nici obligațiilor persoanelor în cauză de a furniza informații în temeiul dreptului penal al statelor membre.

(4) Atunci când este necesar, Comisia și statele membre pot face schimb de informații sensibile cu autoritățile relevante din țări terțe cu care au încheiat acorduri de

---

38 Directiva (UE) 2016/943 a Parlamentului European și a Consiliului din 8 iunie 2016 privind protecția know-how-ului și a informațiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării și divulgării ilegale (JO L 157, 15.6.2016, p. 1).

confidențialitate bilaterale sau multilaterale care garantează un nivel adecvat de protecție.

Articolul 53

Sancțiuni

(1) Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor prezentului regulament de către operatorii economici și iau toate măsurile necesare asigurării punerii în aplicare a acestora. Sancțiunile trebuie să fie eficace, proporționale și disuasive. ***Statele membre se asigură că normele respective țin seama de capacitățile financiare ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.***

(2) Statele membre notifică fără întârziere normele respective Comisiei și îi comunică acesteia, fără întârziere, orice modificare ulterioară privind aceste norme. ***Comisia se asigură că normele și măsurile respective sunt aplicate în mod uniform și consecvent în întreaga Uniune.***

(3) Nerespectarea cerințelor esențiale de securitate cibernetică prevăzute în anexa I și a obligațiilor prevăzute la articolele 10 și 11 face obiectul unor amenzi administrative de până la 15 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 2,5 % din cifra sa de afaceri anuală totală la nivel mondial pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

(4) Nerespectarea altor obligații în temeiul prezentului regulament face obiectul unor amenzi administrative de până la 10 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 2 % din cifra sa de afaceri anuală totală la nivel mondial pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

(5) Furnizarea de informații incorecte, incomplete sau înșelătoare organismelor notificate și autorităților de supraveghere a pieței ca răspuns la o cerere face obiectul unor amenzi administrative de până la 5 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 1 % din cifra sa de afaceri anuală totală la nivel mondial pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

(6) Atunci când se ia o decizie cu privire la cuantumul amenzii administrative în fiecare caz în parte, se iau în considerare toate circumstanțele relevante ale situației specifice și se acordă atenția cuvenită următoarelor aspecte:

(a) natura, gravitatea și durata încălcării și a consecințelor acesteia;

(aa) dacă încălcarea este neintenționată;

(b) dacă ***aceleași sau*** alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator pentru o încălcare similară;

(c) dimensiunea***, în special în ceea ce privește microîntreprinderile, întreprinderile mici și mijlocii, inclusiv întreprinderile nou-înființate,*** și cota de piață ale operatorului care a săvârșit încălcarea.

(7) Autoritățile de supraveghere a pieței care aplică amenzi administrative comunică aceste informații autorităților de supraveghere a pieței din alte state membre prin intermediul sistemului de informații și comunicare menționat la articolul 34 din Regulamentul (UE) 2019/1020.

(8) Fiecare stat membru stabilește norme pentru a stabili dacă și în ce măsură pot fi impuse amenzi administrative autorităților și organismelor publice stabilite în statul membru respectiv.

(9) În funcție de sistemul juridic al statelor membre, normele privind amenzile administrative pot fi aplicate de așa manieră încât amenzile să fie impuse de instanțele naționale competente sau de alte organisme, potrivit competențelor stabilite la nivel național în statele membre respective. Aplicarea unor astfel de norme în statele membre respective are un efect echivalent.

(10) Pot fi impuse amenzi administrative, în funcție de circumstanțele fiecărui caz în parte, în plus față de orice alte măsuri corective sau restrictive aplicate de autoritățile de supraveghere a pieței pentru aceeași încălcare.

Articolul 53a

Alocarea veniturilor provenite din sancțiuni

Statele membre alocă veniturile provenite din sancțiunile menționate la articolul 53 alineatul (1) proiectelor de creștere a nivelului de securitate cibernetică în cadrul Uniunii. Aceste proiecte vizează cel puțin una dintre următoarele:

(a) creșterea numărului de profesioniști calificați în domeniul securității cibernetice, îndeosebi femei;

(b) mărirea capacităților microîntreprinderilor și ale întreprinderilor mici și mijlocii, pentru a le înlesni acestora respectarea prezentului regulament;

(c) creșterea sensibilizării publicului cu privire la amenințările cibernetice, în special în ceea ce privește prevenirea și gestionarea acestora;

(d) dezvoltarea de instrumente pentru a mări reziliența întreprinderilor Uniunii la furtul de proprietate intelectuală facilitat prin mijloace informatice.

CAPITOLUL VIII

DISPOZIȚII TRANZITORII ȘI FINALE

Articolul 54

Modificare adusă Regulamentului (UE) 2019/1020

În anexa I la Regulamentul (UE) 2019/1020 se adaugă următorul punct:

„(71) [Regulamentul XXX] [Actul european privind reziliența cibernetică]”.

Articolul 54a

Modificare adusă Directivei (UE) 2020/1828

În anexa I la Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului[39], se adaugă următorul punct:

---

[39] Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului din 25 noiembrie 2020 privind acțiunile în reprezentare pentru protecția intereselor colective ale consumatorilor și de abrogare a Directivei 2009/22/CE (JO L 409, 4.12.2020, p. 1).

„(67) [Regulamentul XXX] [Actul european privind reziliența cibernetică]”.

Articolul 55

Dispoziții tranzitorii

(1) Certificatele de examinare UE de tip și deciziile de aprobare emise în ceea ce privește cerințele de securitate cibernetică pentru produsele cu elemente digitale care fac obiectul altor acte din legislația de armonizare a Uniunii rămân valabile până la [42 de luni de la data intrării în vigoare a prezentului regulament], cu excepția cazului în care expiră înainte de data respectivă sau cu excepția cazului în care se prevede altfel în alte acte legislative ale Uniunii, caz în care rămân valabile, astfel cum se menționează în legislația respectivă a Uniunii.

(2) Produsele cu elemente digitale care au fost introduse pe piață înainte de [data aplicării prezentului regulament menționată la articolul 57] fac obiectul cerințelor prezentului regulament numai dacă, de la acea dată, produsele respective fac obiectul unor modificări substanțiale în ceea ce privește proiectarea sau scopul lor preconizat.

(3) Prin derogare de la alineatul (2), obligațiile prevăzute la articolul 11 se aplică tuturor produselor cu elemente digitale care intră în domeniul de aplicare al prezentului regulament și care au fost introduse pe piață înainte de [data aplicării prezentului regulament menționată la articolul 57].

(3a) Până la data de la care se aplică prezentul regulament, producătorii pot respecta cerințele prezentului regulament în mod voluntar. În cazul în care producătorii respectă prezentul regulament în ceea ce privește produsele lor cu elemente digitale, se consideră că aceștia respectă și Regulamentul delegat (UE) 2022/30.

Comisia abrogă Regulamentul delegat (UE) 2022/30 la aceeași dată de aplicare a prezentului regulament.

Articolul 56

Evaluare și reexaminare

(1) Până la [36 de luni de la data de la care se aplică prezentul regulament] și, ulterior, la fiecare patru ani, Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament. Rapoartele se fac publice.

(2) În fiecare an, atunci când prezintă proiectul de buget pentru anul următor, Comisia prezintă o evaluare detaliată a sarcinilor ENISA în temeiul prezentului regulament, astfel cum se prevede în anexa VIa și în alte acte legislative relevante ale Uniunii, și detaliază resursele financiare și umane necesare pentru îndeplinirea sarcinilor respective.

Articolul 57

Intrarea în vigoare și aplicarea

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

Se aplică de la [***36*** de luni de la data intrării în vigoare a prezentului regulament]. Cu toate acestea, articolul 11 se aplică de la [***18*** luni de la data intrării în vigoare a prezentului regulament].

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*

ANEXA I

CERINȚE ESENȚIALE DE SECURITATE CIBERNETICĂ

1. CERINȚE DE SECURITATE REFERITOARE LA PROPRIETĂȚILE PRODUSELOR CU ELEMENTE DIGITALE

(1) Produsele cu elemente digitale sunt proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri;

▌

(3) Pe baza evaluării riscurilor ***în materie de securitate cibernetică*** menționate la articolul 10 alineatul (2) și după caz, produsele cu elemente digitale trebuie:

(-a) să fie puse la dispoziție fără vulnerabilități exploatabile cunoscute;

(a) să fie ***puse la dispoziție*** cu o configurație securizată implicită, ***cu excepția cazului în care părțile au convenit altfel în contextul relațiilor dintre întreprinderi,*** inclusiv cu posibilitatea de a reseta produsul la starea sa inițială***, păstrând totodată toate actualizările de securitate instalate***;

(aa) în cazul în care acest lucru este fezabil din punct de vedere tehnic, să fie puse la dispoziție pe piață cu separarea funcțională a actualizărilor de securitate de actualizarea funcționalității;

(ab) să asigure actualizări automate de securitate cu un mecanism de neparticipare clar și ușor de utilizat și notificarea utilizatorilor cu privire la actualizările disponibile;

(b) să asigure protecția împotriva accesului neautorizat prin mecanisme de control adecvate, inclusiv, dar fără a se limita la sistemele de autentificare, de gestionare a identității sau a accesului;

(c) să protejeze confidențialitatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, de exemplu prin criptarea datelor relevante în repaus sau în tranzit prin mecanisme de ultimă generație ***și prin utilizarea altor mijloace tehnice***;

(d) să protejeze integritatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, a comenzilor, a programelor și a configurației împotriva oricărei manipulări sau modificări neautorizate de către utilizator, și să raporteze cu privire la fișierele corupte ***sau la un posibil acces neautorizat***;

(e) să prelucreze numai date, cu caracter personal sau de altă natură, care sunt adecvate, relevante și limitate la ceea ce este necesar în legătură cu utilizarea preconizată a produsului („reducerea la minimum a datelor”);

(f) să protejeze disponibilitatea funcțiilor esențiale ***și de bază, și după un incident***, inclusiv ***prin gestionarea de rezervă, precum și măsurile de reziliență și de atenuare*** împotriva atacurilor vizând blocarea accesului la servicii;

(g) să își reducă la minimum propriul impact negativ asupra disponibilității serviciilor furnizate de alte dispozitive sau rețele;

(h) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se limiteze suprafețele de atac, inclusiv interfețele externe;

(i) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se reducă impactul unui incident prin utilizarea de mecanisme și tehnici adecvate de prevenire a exploatării vulnerabilităților;

(j) să furnizeze informații legate de securitate prin ***capacități de înregistrare*** și/sau ***monitorizare a*** activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora***, cu un mecanism de neparticipare pentru utilizator***;

▌

(ka) să le permită utilizatorilor să își retragă și să își elimine în mod permanent datele în condiții de siguranță.

2. CERINȚE PRIVIND GESTIONAREA VULNERABILITĂȚILOR

Producătorii de produse cu elemente digitale trebuie:

(1) să identifice și să documenteze vulnerabilitățile și componentele produsului, inclusiv prin întocmirea unei liste a materialelor software într-un format folosit în mod curent și care poate fi citit automat, care să acopere cel puțin dependențele de nivel superior ale produsului;

(2) în ceea ce privește riscurile pe care le prezintă produsele cu elemente digitale, să abordeze și să remedieze fără întârziere vulnerabilitățile, inclusiv prin furnizarea de actualizări de securitate ***instalate automat, după caz, în conformitate cu secțiunea I***;

(3) să aplice teste și reexaminări eficace și periodice ale securității produsului cu elemente digitale;

(4) după punerea la dispoziție a unei actualizări de securitate, ***să partajeze și*** să publice informații cu privire la vulnerabilitățile remediate ***într-o manieră controlată***, inclusiv o descriere a vulnerabilităților, informații care să permită utilizatorilor să identifice produsul cu elemente digitale afectat, impactul vulnerabilităților, gravitatea acestora și informații ***clare și accesibile*** care să ajute utilizatorii să remedieze vulnerabilitățile;

(5) să instituie și să pună în aplicare o politică privind divulgarea coordonată a vulnerabilităților;

(6) să ia măsuri pentru a facilita schimbul de informații cu privire la potențialele vulnerabilități ale produsului lor cu elemente digitale, precum și cu privire la componentele terților conținute în produsul respectiv, inclusiv prin furnizarea unei adrese de contact pentru raportarea vulnerabilităților descoperite în produsul cu elemente digitale;

(7) să prevadă mecanisme de distribuire securizată a actualizărilor ***de securitate*** pentru produsele cu elemente digitale, pentru a se asigura că vulnerabilitățile exploatabile sunt remediate sau atenuate în timp util;

(8) să se asigure că, în cazul în care sunt disponibile corecții de securitate sau actualizări pentru abordarea problemelor de securitate identificate, acestea sunt difuzate fără întârziere și***, cu excepția cazului în care părțile au convenit altfel în contextul relațiilor dintre întreprinderi,*** gratuit, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse;

(8a) dacă este posibil și aplicabil, să înștiințeze utilizatorul cu privire la sfârșitul perioadei de sprijin.

ANEXA II

INFORMAȚII ȘI INSTRUCȚIUNI PENTRU UTILIZATOR

Produsul cu elemente digitale trebuie să fie însoțit cel puțin de:

1. numele, denumirea comercială înregistrată sau marca înregistrată a producătorului, precum și adresa poștală, adresa de e-mail și***, dacă este disponibil, site-ul web*** la care poate fi contactat producătorul, pe produs sau ▌ pe ambalaj sau într-un document care însoțește produsul;

2. punctul ***unic*** de contact unde pot fi raportate și primite informații cu privire la vulnerabilitățile în materie de securitate cibernetică ale produsului, ***precum și politica producătorului privind vulnerabilitățile coordonate și locul în care acestea pot fi găsite***;

3. identificarea corectă a tipului, lotului, versiunii sau numărului de serie sau a altui element care permite identificarea produsului, precum și instrucțiunile și informațiile de utilizare corespunzătoare;

4. utilizarea preconizată, inclusiv mediul de securitate furnizat de producător, precum și funcționalitățile esențiale ale produsului și informații cu privire la proprietățile de securitate;

5. orice circumstanță cunoscută sau previzibilă legată de utilizarea produsului cu elemente digitale în conformitate cu scopul preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil care poate conduce la riscuri semnificative de securitate cibernetică;

6. dacă și, după caz, unde poate fi accesată lista materialelor software ***de către autoritățile competente în conformitate cu condițiile de nedivulgare prevăzute la articolul 52***;

7. dacă este cazul, adresa de internet la care poate fi accesată declarația de conformitate UE;

8. tipul de asistență tehnică de securitate oferită de producător și ***perioada de sprijin în*** care utilizatorii se pot aștepta ***să fie gestionate vulnerabilitățile și*** să primească actualizări de securitate;

9. instrucțiuni detaliate sau o adresă de internet la care să se găsească astfel de instrucțiuni detaliate și informații privind:

   (a) măsurile necesare în timpul punerii în funcțiune inițiale și pe toată durata de viață a produsului pentru a se asigura o utilizare securizată a acestuia;

   (b) modul în care modificările aduse produsului pot afecta securitatea datelor;

   (c) modul în care pot fi instalate actualizările relevante pentru securitate;

   (d) dezafectarea securizată a produsului, inclusiv informații privind modul în care datele utilizatorilor pot fi eliminate în mod securizat.

ANEXA III

PRODUSELE CRITICE CU ELEMENTE DIGITALE

Clasa I

1. Software pentru sisteme de gestionare a identității și software de gestionare a accesului privilegiat;
2. Browsere autonome și încorporate;
3. Manageri de parole;

3a. Cititoare biometrice;

4. Software care caută, elimină sau plasează în carantină programe informatice malware;
5. Produse cu elemente digitale cu funcție de rețea privată virtuală (VPN);
6. Sisteme de administrare a rețelei;
7. Instrumente de gestionare a configurației rețelei;
8. Sisteme de monitorizare a traficului în rețea;
9. Gestionarea resurselor rețelei;
10. Sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM);
11. Gestionarea actualizărilor/corecțiilor, inclusiv managerii de boot;
12. Sisteme de gestionare a configurațiilor aplicațiilor;
13. Software de accesare ▌ de la distanță;
14. Software de gestionare a dispozitivelor mobile;
15. Interfețe fizice ***și virtuale*** de rețea;
16. Sisteme de operare neincluse în clasa II;
17. Firewall-uri, sisteme de detectare și/sau prevenire a intruziunilor care nu sunt incluse în clasa II;

19. ***Microprocesoare de uz general și*** microprocesoare neincluse în clasa II;

20. Microcontrolere;
21. Circuite integrate specifice aplicațiilor (ASIC) și rețele de porți programabile de utilizator (FPGA) destinate utilizării de către entități esențiale de tipul celor menționate ***la articolul 3 din*** Directiva ***(UE) 2022/2555***;
22. Sisteme de control pentru automatizări industriale (IACS) neincluse în clasa II, cum ar fi controlerele logice programabile (PLC), sistemele de control distribuit (SCD), controlerele numerice computerizate pentru mașini-unelte (CNC)***, roboții industriali și sistemele lor de control*** și sistemele de control de supraveghere și de achiziție de date (SCADA);
23. Internetul industrial al obiectelor neinclus în clasa II***;***

23a. Sisteme de automatizare la domiciliu, inclusiv servere pentru locuințe inteligente și asistenți virtuali;

23b. Dispozitive de securitate, inclusiv încuietori inteligente pentru uși, camere de luat vederi și sisteme de alarmă;

23c. Jucării inteligente;

23d. Aparate medicale personale și dispozitive portabile.

Clasa II

1. Sisteme de operare pentru servere, calculatoare de tip desktop și dispozitive mobile;
2. Hipervizoare și sisteme de runtime a containerelor care sprijină executarea virtualizată a sistemelor de operare și a mediilor similare;
3. Infrastructuri de chei publice și emitenți de certificate digitale;
4. Firewall-uri, sisteme de detectare și/sau prevenire a intruziunilor destinate utilizării industriale;

▌

6. Microprocesoare destinate integrării în controlere logice programabile și în elemente securizate;
7. Routere, modemuri destinate conectării la internet și comutatoare ▌;
8. Elemente securizate;
9. Module de securitate hardware (HSM);
10. Criptoprocesoare securizate;
11. Carduri inteligente, cititoare și tokenuri pentru carduri inteligente;
12. Sisteme de control pentru automatizări industriale (IACS) destinate utilizării de către entități esențiale de tipul celor menționate ***la articolul 3 din*** Directiva ***(UE) 2022/2555***, cum ar fi controlerele logice programabile (PLC), sistemele de control distribuit (SCD), controlerele numerice computerizate pentru mașini-unelte (CNC) și sistemele de control de supraveghere și de achiziție de date (SCADA);
13. Dispozitive pentru internetul industrial al obiectelor destinate utilizării de către entități esențiale de tipul celor menționate ***la articolul 3 din*** Directiva ***(UE) 2022/2555***;

▌

15. Contoare inteligente.

ANEXA IV

DECLARAȚIA DE CONFORMITATE UE

Declarația de conformitate UE menționată la articolul 20 trebuie să conțină toate informațiile următoare:

1. Denumirea și tipul și orice informații suplimentare care permit identificarea unică a produsului cu elemente digitale;
2. Denumirea și adresa producătorului sau a reprezentantului său autorizat;
3. O declarație potrivit căreia declarația de conformitate UE este emisă pe răspunderea exclusivă a furnizorului;
4. Obiectul declarației (identificarea produsului care să permită trasabilitatea. Poate include și o fotografie, după caz.);
5. O declarație potrivit căreia obiectul declarației descris mai sus este conform cu legislația de armonizare relevantă a Uniunii;
6. Menționarea tuturor standardelor armonizate relevante utilizate sau a oricărei alte specificații comune sau certificări de securitate cibernetică în legătură cu care se declară conformitatea;
7. După caz, denumirea și numărul organismului notificat, o descriere a procedurii de evaluare a conformității efectuate și identificarea certificatului emis;
8. Informații suplimentare:

Semnat pentru și în numele: ……

(locul și data emiterii):

(numele, funcția) (semnătura):

ANEXA V

CONȚINUTUL DOCUMENTAȚIEI TEHNICE

Documentația tehnică menționată la articolul 23 trebuie să conțină cel puțin următoarele informații, aplicabile produsului cu elemente digitale relevant:

1. o descriere generală a produsului cu elemente digitale, inclusiv:
   (a) scopul preconizat al acestuia;
   (b) versiunile de software care afectează conformitatea cu cerințele esențiale;
   (c) în cazul în care produsul cu elemente digitale este un produs hardware, fotografii sau ilustrații care să prezinte caracteristicile externe, marcajul și dispunerea internă;
   (d) informațiile și instrucțiunile pentru utilizatori prevăzute în anexa II;
2. o descriere a proiectării, dezvoltării și producției produsului și a proceselor de gestionare a vulnerabilităților, inclusiv:
   (a) informații complete privind proiectarea și dezvoltarea produsului cu elemente digitale, inclusiv, dacă este cazul, desene și scheme și/sau o descriere a arhitecturii sistemului, care să explice modul în care componentele software se bazează unele pe altele sau se alimentează reciproc și se integrează în prelucrarea generală;
   (b) informații și specificații complete privind procesele de gestionare a vulnerabilităților instituite de producător, inclusiv lista materialelor software, politica coordonată de divulgare a vulnerabilităților, dovezi ale furnizării unei adrese de contact pentru raportarea vulnerabilităților și o descriere a soluțiilor tehnice alese pentru distribuirea securizată a actualizărilor;
   (c) informații și specificații complete privind procesele de producție și de monitorizare a produsului cu elemente digitale și validarea acestor procese;
3. o evaluare a riscurilor de securitate cibernetică împotriva cărora este proiectat, dezvoltat, fabricat, livrat și întreținut produsul cu elemente digitale, astfel cum se prevede la articolul 10 din prezentul regulament***, inclusiv modul în care sunt aplicabile cerințele esențiale prevăzute în anexa I, secțiunea 1***;
4. o listă cuprinzând standardele armonizate aplicate integral sau parțial, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, specificațiile comune prevăzute la articolul 19 din prezentul regulament sau sistemele de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 în conformitate cu articolul 18 alineatul (3) și, în cazul în care aceste standarde armonizate, specificații comune sau sisteme de certificare de securitate cibernetică nu au fost aplicate, descrieri ale soluțiilor adoptate pentru a îndeplini cerințele esențiale prevăzute în anexa I secțiunile 1 și 2, inclusiv o listă a altor specificații tehnice relevante aplicate. În cazul unor standarde armonizate, specificații comune sau certificări de securitate cibernetică aplicate parțial, documentația tehnică trebuie să precizeze părțile care au fost aplicate;
5. rapoarte privind testele efectuate pentru verificarea conformității produsului și a proceselor de gestionare a vulnerabilităților cu cerințele esențiale aplicabile, prevăzute în anexa I secțiunile 1 și 2;

6. o copie a declarației de conformitate UE;

7. după caz, lista materialelor software, astfel cum este definită la articolul 3 punctul (36), furnizată în urma unei cereri motivate din partea unei autorități de supraveghere a pieței, cu condiția ca aceasta să fie necesară pentru ca autoritatea respectivă să poată verifica conformitatea cu cerințele esențiale prevăzute în anexa I.

ANEXA VI

PROCEDURI DE EVALUARE A CONFORMITĂȚII

Procedura de evaluare a conformității bazată pe control intern (pe baza modulului A)

1. Controlul intern este procedura de evaluare a conformității prin care producătorul îndeplinește obligațiile prevăzute la punctele 2, 3 și 4 și garantează și declară pe răspunderea sa exclusivă că produsele cu elemente digitale îndeplinesc toate cerințele esențiale prevăzute în anexa I secțiunea 1 și că producătorul îndeplinește cerințele esențiale prevăzute în anexa I secțiunea 2.

2. Producătorul întocmește documentația tehnică descrisă în anexa V.

3. Proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților produselor cu elemente digitale

   Producătorul ia toate măsurile necesare pentru ca procesele de proiectare, dezvoltare, producție și gestionare a vulnerabilităților, precum și monitorizarea acestora să asigure conformitatea produselor cu elementele digitale care sunt fabricate sau dezvoltate și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I secțiunile 1 și 2.

4. Marcajul de conformitate și declarația de conformitate

4.1. Producătorul aplică marcajul CE pe fiecare produs cu elemente digitale în parte care îndeplinește cerințele aplicabile prevăzute în prezentul regulament.

4.2. Producătorul întocmește o declarație de conformitate UE în scris pentru fiecare produs cu elemente digitale în conformitate cu articolul 20 și o păstrează, împreună cu documentația tehnică, la dispoziția autorităților naționale timp de zece ani de la introducerea pe piață a produsului cu elemente digitale ***sau pe durata de sprijin, oricare dintre ele este mai lungă***. Declarația de conformitate UE trebuie să identifice tipul de produs pentru care a fost întocmită. O copie a declarației de conformitate UE trebuie să fie pusă la dispoziția autorităților relevante, la cerere.

5. Reprezentanți autorizați

   Obligațiile producătorului prevăzute la punctul 4 pot fi îndeplinite de către reprezentantul său autorizat, în numele său și pe răspunderea sa, cu condiția ca acestea să fie menționate în mandat.

Examinarea UE de tip (pe baza modulului B)

1. Examinarea UE de tip este acea parte a procedurii de evaluare a conformității prin care un organism notificat examinează proiectarea și dezvoltarea tehnică ale unui produs și procesele de gestionare a vulnerabilităților instituite de producător și atestă că un produs cu elemente digitale îndeplinește cerințele esențiale prevăzute în anexa I secțiunea 1 și că producătorul îndeplinește cerințele esențiale prevăzute în anexa I secțiunea 2.

2. Examinarea UE de tip se efectuează prin evaluarea caracterului adecvat al proiectării și dezvoltării tehnice a produsului prin examinarea documentației tehnice și a documentelor justificative menționate la punctul 3, la care se adaugă examinarea unor

exemplare ale uneia sau mai multor părți critice ale produsului (combinație de tip de producție și tip de proiectare).

3. Producătorul trebuie să înainteze o cerere de examinare UE de tip către un singur organism notificat, la alegerea sa.

Cererea trebuie să cuprindă:

– denumirea și adresa producătorului, iar dacă cererea este depusă de reprezentantul autorizat, se precizează și numele și adresa acestuia;

– o declarație scrisă care să precizeze că nu a fost depusă o cerere identică la un alt organism notificat;

– documentația tehnică, care trebuie să permită evaluarea conformității produsului cu cerințele esențiale aplicabile prevăzute în anexa I secțiunea 1 și a proceselor de gestionare a vulnerabilităților ale producătorului cu cerințele esențiale aplicabile prevăzute în anexa I secțiunea 2 și să includă o analiză și o evaluare adecvată a riscului (riscurilor). Documentația tehnică trebuie să specifice cerințele aplicabile și să acopere, în măsura în care acest lucru este relevant pentru evaluare, proiectarea, fabricarea și exploatarea produsului. Documentația tehnică trebuie să cuprindă, ori de câte ori este necesar, elementele menționate în anexa V;

– documentele justificative pentru caracterul adecvat al soluțiilor de proiectare și dezvoltare tehnică și al proceselor de gestionare a vulnerabilităților. Aceste documente justificative trebuie să menționeze orice document care a fost utilizat, în special atunci când standardele relevante armonizate și/sau specificațiile tehnice relevante nu au fost aplicate în întregime. Documentele justificative includ, în cazul în care este necesar, rezultatele testelor efectuate în numele său ori pe răspunderea sa de laboratorul corespunzător al producătorului sau de un alt laborator de testare.

4. Organismul de certificare notificat:

4.1. examinează documentația tehnică și documentele justificative pentru a evalua dacă proiectarea și dezvoltarea tehnică a produsului sunt adecvate în raport cu cerințele esențiale prevăzute în anexa I secțiunea 1 și dacă procesele de gestionare a vulnerabilităților instituite de producător sunt adecvate în raport cu cerințele esențiale prevăzute în anexa I secțiunea 2;

4.2. verifică dacă exemplarul (exemplarele) a(u) fost dezvoltat(e) sau produs(e) în conformitate cu documentația tehnică și identifică elementele care au fost proiectate și dezvoltate în conformitate cu dispozițiile aplicabile din standardele armonizate și/sau specificațiile tehnice relevante, precum și elementele care au fost proiectate și dezvoltate fără a se aplica dispozițiile relevante ale acestor standarde;

4.3. efectuează examinările și testele corespunzătoare sau dispune efectuarea acestora pentru a verifica, în cazul în care producătorul a ales să aplice soluțiile din standardele armonizate și/sau specificațiile tehnice relevante pentru cerințele prevăzute în anexa I, dacă acestea au fost aplicate corect;

4.4. efectuează examinările și testele corespunzătoare sau dispune efectuarea acestora pentru a verifica, în cazul în care nu au fost aplicate soluțiile din standardele armonizate și/sau specificațiile tehnice relevante pentru cerințele prevăzute în anexa I,

dacă soluțiile adoptate de către producător îndeplinesc cerințele esențiale corespunzătoare;

4.5. stabilește de comun acord cu producătorul locul în care vor fi efectuate examinările și testele.

5. Organismul notificat întocmește un raport de evaluare care evidențiază activitățile întreprinse, conform punctului 4, precum și rezultatele acestora. Fără a aduce atingere obligațiilor sale față de autoritățile de notificare, organismul notificat nu divulgă conținutul acestui raport, în întregime sau parțial, decât cu acordul producătorului.

6. În cazul în care tipul și procesele de gestionare a vulnerabilităților îndeplinesc cerințele esențiale prevăzute în anexa I, organismul notificat eliberează producătorului un certificat de examinare UE de tip. Certificatul trebuie să conțină denumirea și adresa producătorului, concluziile examinării, condițiile (dacă există) pentru valabilitatea certificatului și datele necesare pentru identificarea tipului aprobat și a proceselor de gestionare a vulnerabilităților. Certificatul poate avea una sau mai multe anexe.

Certificatul și anexele acestuia trebuie să conțină toate informațiile relevante care să permită evaluarea conformității cu tipul examinat a produselor fabricate sau dezvoltate și a proceselor de gestionare a vulnerabilităților și care permit controlul în utilizare.

În cazul în care tipul și procesele de gestionare a vulnerabilităților nu îndeplinesc cerințele esențiale aplicabile prevăzute în anexa I, organismul notificat refuză emiterea unui certificat de examinare UE de tip și informează solicitantul în consecință, precizând în detaliu motivele refuzului.

7. Organismul notificat se informează în permanență cu privire la orice modificări ale stadiului actual al tehnologiei general recunoscut, care indică posibilitatea ca tipul aprobat și procesele de gestionare a vulnerabilităților să nu mai îndeplinească cerințele esențiale aplicabile prevăzute în anexa I la prezentul regulament și stabilește dacă aceste modificări necesită investigații suplimentare. În acest caz, organismul notificat informează producătorul în consecință.

Producătorul informează organismul notificat care deține documentația tehnică referitoare la certificatul de examinare UE de tip cu privire la toate modificările tipului aprobat și ale proceselor de gestionare a vulnerabilităților care pot influența conformitatea cu cerințele esențiale prevăzute în anexa I sau cu condițiile de valabilitate ale certificatului respectiv. Aceste modificări necesită o aprobare suplimentară sub forma unui supliment la certificatul inițial de examinare UE de tip.

8. Fiecare organism notificat își informează autoritățile de notificare în legătură cu certificatele de examinare UE de tip și/sau eventualele suplimente la acestea pe care le-a emis sau retras și, în mod periodic sau la cerere, pune la dispoziția autorităților sale de notificare lista certificatelor și/sau a eventualelor suplimente la acestea care au fost refuzate, suspendate sau restricționate în alt mod.

Fiecare organism notificat informează celelalte organisme notificate în legătură cu certificatele de examinare UE de tip și/sau eventualele suplimente la acestea pe care le-a refuzat, retras, suspendat sau restricționat în alt mod și, la cerere, în legătură cu certificatele și/sau suplimentele la acestea pe care le-a emis.

Comisia, statele membre și celelalte organisme notificate pot obține, la cerere, o copie a certificatelor de examinare UE de tip și/sau a suplimentelor la acestea. Pe baza unei cereri, Comisia și statele membre pot obține o copie a documentației tehnice și a

rezultatelor examinărilor efectuate de organismul notificat. Organismul notificat păstrează un exemplar al certificatului de examinare UE de tip, al anexelor și suplimentelor acestuia, precum și dosarul tehnic incluzând documentația depusă de producător, până la expirarea valabilității certificatului.

9. Producătorul păstrează la dispoziția autorităților naționale o copie a certificatului de examinare UE de tip, a anexelor și a suplimentelor acestuia, împreună cu documentația tehnică, timp de zece ani de la introducerea pe piață a produsului ***sau pentru perioada de sprijin***.

10. Reprezentantul autorizat al producătorului poate depune cererea menționată la punctul 3 și poate îndeplini obligațiile prevăzute la punctele 7 și 9, cu condiția ca acestea să fie menționate în mandat.

Conformitatea cu tipul bazată pe controlul intern al producției (pe baza modulului C)

1. Conformitatea cu tipul bazată pe controlul intern al producției este acea parte a procedurii de evaluare a conformității prin care producătorul îndeplinește obligațiile prevăzute la punctele 2 și 3 și garantează și declară că produsele în cauză sunt conforme cu tipul descris în certificatul de examinare UE de tip și respectă cerințele esențiale prevăzute în anexa I secțiunea 1.

2. Producția

2.1. Producătorul ia toate măsurile necesare pentru ca procesul de producție și monitorizarea acestuia să asigure conformitatea produselor fabricate cu tipul aprobat descris în certificatul de examinare UE de tip și cu cerințele esențiale prevăzute în anexa I secțiunea 1.

3. Marcajul de conformitate și declarația de conformitate

3.1. Producătorul aplică marcajul CE pe fiecare produs în parte care este conform cu tipul descris în certificatul de examinare UE de tip și care îndeplinește cerințele aplicabile ale instrumentului legislativ.

3.2. Producătorul întocmește o declarație de conformitate scrisă pentru un model de produs și o păstrează la dispoziția autorităților naționale pe o perioadă de 10 ani după introducerea pe piață a produsului ***sau pentru perioada de sprijin***. Declarația de conformitate trebuie să identifice modelul produsului pentru care a fost întocmită. O copie a declarației de conformitate trebuie să fie pusă la dispoziția autorităților relevante, la cerere.

4. Reprezentantul autorizat

Obligațiile producătorului prevăzute la punctul 3 pot fi îndeplinite de către reprezentantul său autorizat, în numele său și pe răspunderea sa, cu condiția ca acestea să fie menționate în mandat.

Conformitatea bazată pe asigurarea totală a calității (pe baza modulului H)

1. Conformitatea bazată pe asigurarea totală a calității este procedura de evaluare a conformității prin care producătorul îndeplinește obligațiile prevăzute la punctele 2 și 5 și garantează și declară pe răspunderea sa exclusivă că produsele (sau categoriile de produse) în cauză îndeplinesc cerințele esențiale prevăzute în anexa I secțiunea 1 și că

procesele de gestionare a vulnerabilităților instituite de producător îndeplinesc cerințele prevăzute în anexa I secțiunea 2.

2. Proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților produselor cu elemente digitale

Producătorul utilizează un sistem de calitate aprobat, astfel cum se specifică la punctul 3, pentru proiectarea, dezvoltarea și fabricarea produselor în cauză și pentru gestionarea vulnerabilităților, menține eficacitatea acestuia pe parcursul întregului ciclu de viață al produselor în cauză și este supus supravegherii specificate la punctul 4.

3. Sistemul de calitate

3.1. Producătorul înaintează o cerere de evaluare a sistemului de calitate către un organism notificat la alegerea sa, pentru produsele în cauză.

Cererea trebuie să cuprindă:

– denumirea și adresa producătorului, iar dacă cererea este depusă de reprezentantul autorizat, se precizează și numele și adresa acestuia;

– documentația tehnică pentru un singur model din fiecare categorie de produse care urmează a fi fabricate sau dezvoltate. Documentația tehnică trebuie să cuprindă, oricând este cazul, elementele menționate în anexa V;

– documentația referitoare la sistemul de calitate; și dacă

– o declarație scrisă care să precizeze că nu fost depusă o cerere identică la un alt organism notificat.

3.2. Sistemul de calitate asigură conformitatea produselor cu cerințele esențiale prevăzute în anexa I secțiunea 1 și conformitatea proceselor de gestionare a vulnerabilităților instituite de producător cu cerințele prevăzute în anexa I secțiunea 2.

Toate elementele, cerințele și dispozițiile adoptate de către producător trebuie să fie consemnate în documente în mod sistematic și ordonat sub formă de politici, proceduri și instrucțiuni scrise. Documentația sistemului de calitate trebuie să permită o interpretare consecventă a programelor, planurilor, manualelor și înregistrărilor privind calitatea.

Documentația trebuie să cuprindă în special o descriere adecvată:

– a obiectivelor referitoare la calitate și a structurii organizatorice, a responsabilităților și a competențelor personalului de conducere cu privire la proiectarea, dezvoltarea și calitatea produselor și la gestionarea vulnerabilităților;

– a specificațiilor privind proiectarea și dezvoltarea tehnică, inclusiv a standardelor, care vor fi aplicate și, în cazul în care standardele armonizate și/sau specificațiile tehnice relevante nu vor fi aplicate în totalitate, a mijloacelor care vor fi folosite pentru a asigura respectarea cerințelor esențiale prevăzute în anexa I secțiunea 1 care se aplică produselor respective;

– a specificațiilor privind procedurile, inclusiv a standardelor, care vor fi aplicate, și, în cazul în care standardele armonizate și/sau specificațiile tehnice relevante nu vor fi aplicate în totalitate, a mijloacelor care vor fi

folosite pentru a asigura respectarea cerințelor esențiale prevăzute în anexa I secțiunea 2 care se aplică producătorului respectiv;

– a tehnicilor de control al proiectării și dezvoltării, precum și a tehnicilor de verificare a proiectării și dezvoltării, a proceselor și a acțiunilor sistematice care vor fi utilizate la proiectarea și dezvoltarea produselor ce aparțin categoriei de produse vizate;

– a tehnicilor corespunzătoare de producție, de control al calității și de asigurare a calității, a proceselor și a acțiunilor sistematice care vor fi utilizate;

– a examinărilor și a testelor care vor fi efectuate înaintea, în cursul și în urma producției, precum și a frecvenței cu care vor fi efectuate;

– a înregistrărilor referitoare la calitate, cum ar fi rapoarte de inspecție și informații referitoare la teste, precum și date privind etalonarea, rapoarte referitoare la calificarea personalului implicat etc.;

– a mijloacelor de monitorizare privind atingerea calității cerute a proiectului și a produsului și funcționarea eficace a sistemului de calitate.

3.3. Organismul notificat evaluează sistemul de calitate pentru a stabili dacă acesta îndeplinește cerințele menționate la punctul 3.2.

Acesta prezumă conformitatea cu cerințele respective pentru elementele sistemului de calitate care sunt conforme cu specificațiile corespunzătoare ale standardului național care pune în aplicare standardul armonizat și/sau specificațiile tehnice relevante.

Pe lângă experiența în sisteme de management al calității, echipa de audit trebuie să aibă cel puțin un membru cu experiență de evaluator în domeniul produsului relevant și al tehnologiei produsului în cauză și să cunoască cerințele aplicabile prevăzute în prezentul regulament. Auditul trebuie să includă o vizită de evaluare la sediul producătorului, în cazul în care există un astfel de sediu. Echipa de audit analizează documentația tehnică menționată la punctul 3.1 a doua liniuță în vederea verificării capacității producătorului de a identifica cerințele aplicabile prevăzute în prezentul regulament și a efectuării examinărilor necesare cu scopul de a asigura conformitatea produsului cu aceste cerințe.

Decizia este notificată producătorului sau reprezentantului autorizat al acestuia.

Notificarea trebuie să cuprindă concluziile procesului de audit și decizia motivată referitoare la evaluare.

3.4. Producătorul se angajează să îndeplinească obligațiile care decurg din sistemul de calitate astfel cum a fost aprobat și să îl mențină astfel încât acesta să rămână adecvat și eficace.

3.5. Producătorul informează în permanență organismul notificat care a aprobat sistemul de calitate în legătură cu orice intenție de modificare a sistemului de calitate.

Organismul notificat evaluează modificările propuse și decide dacă sistemul de calitate modificat va continua să îndeplinească cerințele menționate la punctul 3.2 sau dacă este necesară o reevaluare.

Organismul notificat notifică decizia sa producătorului. Notificarea trebuie să cuprindă concluziile examinării și decizia motivată referitoare la evaluare.

4. Supravegherea care intră în sfera de responsabilitate a organismului notificat

4.1. Scopul supravegherii este acela de a asigura îndeplinirea corespunzătoare de către producător a obligațiilor ce decurg din sistemul de calitate aprobat.

4.2. Producătorul autorizează accesul organismului notificat, în scopul evaluării, la spațiile de proiectare, dezvoltare, producție, inspecție, testare și depozitare și îi furnizează orice informație necesară, în special:

– documentația privind sistemul de calitate;

– înregistrările referitoare la calitate, astfel cum sunt prevăzute în partea sistemului de calitate destinată proiectării, de exemplu rezultatele analizelor, calculelor, testelor etc.;

– înregistrările referitoare la calitate, astfel cum sunt prevăzute în partea sistemului de calitate destinată fabricării, de exemplu rapoarte de inspecție și date privind testele, date privind etalonarea, rapoarte privind calificarea personalului în cauză etc.

4.3. Organismul notificat efectuează misiuni de audit periodice pentru a se asigura că producătorul menține și aplică sistemul de calitate și prezintă producătorului un raport de audit.

5. Marcajul de conformitate și declarația de conformitate

5.1. Producătorul aplică marcajul CE și, sub responsabilitatea organismului notificat menționat la punctul 3.1, numărul de identificare al acestuia pe fiecare produs în parte care îndeplinește cerințele prevăzute în secțiunea 1 din anexa I la prezentul regulament.

5.2. Producătorul întocmește o declarație de conformitate scrisă pentru fiecare model de produs și o păstrează la dispoziția autorităților naționale pe o perioadă de 10 ani după introducerea pe piață a produsului ***sau pentru perioada de sprijin***. Declarația de conformitate trebuie să identifice modelul produsului pentru care a fost întocmită.

O copie a declarației de conformitate trebuie să fie pusă la dispoziția autorităților relevante, la cerere.

6. Pe o perioadă de cel puțin zece ani de la introducerea pe piață a produsului ***sau pentru perioada de sprijin sau perioada în care sunt tratate vulnerabilitățile***, producătorul menține la dispoziția autorităților naționale:

– documentația tehnică menționată la punctul 3.1;

– documentația privind sistemul de calitate prevăzută la punctul 3.1;

– modificarea menționată la punctul 3.5, astfel cum a fost aprobată;

– deciziile și rapoartele organismului notificat menționate la punctele 3.5, 4.3 și 4.4.

7. Fiecare organism notificat își informează autoritățile de notificare în legătură cu aprobările sistemului de calitate care au fost emise sau retrase și, în mod periodic sau la cerere, pune la dispoziția autorităților sale de notificare lista aprobărilor sistemelor de calitate care au fost refuzate, suspendate sau restricționate în alt mod.

Fiecare organism notificat informează celelalte organisme notificate în legătură cu aprobările sistemelor de calitate pe care le-a refuzat, suspendat sau retras și, la cerere, în legătură cu aprobările sistemelor de calitate pe care le-a emis.

8. Reprezentantul autorizat

Obligațiile producătorului menționate la punctele 3.1, 3.5, 5 și 6 pot fi îndeplinite de către reprezentantul său autorizat, în numele său și pe răspunderea sa, cu condiția ca acestea să fie menționate în mandat.

ANEXA VIa

NEVOILE ÎN MATERIE DE CAPACITATE ALE AGENȚIEI UNIUNII EUROPENE PENTRU SECURITATE ENERGETICĂ (ENISA)

Pentru a-și îndeplini obligațiile care îi revin în temeiul prezentului regulament și pentru a nu compromite obligațiile existente ale Agenției în temeiul altor acte legislative ale Uniunii, se asigură personal și finanțare adecvate pentru ENISA. Prin urmare, sarcinile suplimentare ale ENISA în temeiul prezentului regulament sunt însoțite de resurse umane și financiare suplimentare. Vor fi necesare nouă posturi suplimentare în echivalent normă întreagă și creditele suplimentare corespunzătoare pentru a acoperi sarcinile suplimentare în temeiul prezentului regulament.

EXPUNERE DE MOTIVE

Raportorul salută călduros propunerea Comisiei de a aborda deficiențele de securitate cibernetică ale produselor hardware și software. În 2021, costul global al criminalității informatice a ajuns la o sumă record de 5,5 mii de miliarde EUR. Acest fenomen, împreună cu tendința ascendentă a digitalizării, invită legiuitorii să se asigure că sunt instituite măsuri adecvate de securitate cibernetică pentru a proteja atât interesele consumatorilor, cât și pe cele ale industriei.

În acest sens, raportorul salută prezentarea de către Comisie a unei propuneri ambițioase, care va crește nivelul general de securitate cibernetică în statele membre și funcționarea pieței interne. Este necesar un cadru de reglementare armonizat pentru ca întreprinderile care își desfășoară activitatea pe piața unică să poată beneficia de claritate juridică, precum și pentru a se asigura că Uniunea poate juca un rol de lider în definirea normelor privind securitatea cibernetică pe scena mondială.

În ceea ce privește domeniul de aplicare, raportorul este de acord cu propunerea Comisiei de a include toate produsele cu elemente digitale. Această abordare cuprinzătoare ar asigura conformitatea în materie de securitate cibernetică de-a lungul întregului lanț valoric, îmbunătățind competitivitatea și atractivitatea produselor fabricate în Uniune. Cu toate acestea, este necesar să se simplifice formularea actuală și să se facă referire la produsele care pot fi conectate direct și indirect, excluzând, în același timp, piesele de schimb concepute exclusiv pentru procesul de reparare, care au fost pe piață înainte de punerea în aplicare a prezentului regulament. În ceea ce privește software-ul cu sursă deschisă, raportorul este conștient de necesitatea de a proteja această sursă importantă de inovare și, prin urmare, a prezentat un amendament pentru a se asigura că dezvoltatorii nu ar trebui să respecte prezentul regulament dacă nu primesc venituri financiare pentru proiectele lor. Cu toate acestea, software-ul cu sursă deschisă furnizat în cadrul unei activități comerciale ar trebui să fie acoperit, pentru a asigura securitatea cibernetică a ecosistemului Uniunii.

Deși marea majoritate a produselor cu elemente digitale vor trebui să fie supuse doar autoevaluării, produsele critice în temeiul articolului 6 vor face obiectul unei evaluări de către o parte terță. În această privință, raportorul consideră că regulamentul ar trebui îmbunătățit, oferind mai multă claritate cu privire la frecvența cu care poate fi modificată lista prevăzută în anexa III, precum și cu privire la procedurile care trebuie urmate după adăugarea unui produs pe această listă. Aceasta din urmă este deosebit de importantă pentru a oferi întreprinderilor suficient timp pentru a se adapta. Cu toate acestea, raportorul consideră că sistemele de automatizare la domiciliu și produsele care măresc securitatea privată, cum ar fi camerele de luat vederi și încuietorile inteligente, ar trebui să constituie produse esențiale din clasa I. Acest lucru se datorează faptului că integritatea acestor produse este esențială pentru siguranța și viața privată a cetățenilor.

În plus, proiectul de raport prevede o mai mare implicare a părților interesate prin crearea Grupului de experți privind reziliența cibernetică. Acest organism ar trebui să aibă sarcina de a consilia Comisia și de a-și asuma un rol activ în pregătirea actelor delegate menționate în prezentul regulament. Astfel, pentru a exprima pe deplin interesele tuturor părților, Grupul de experți ar trebui să fie format din instituții, industrie, societatea civilă, mediul academic și experți individuali.

Pe lângă subiectul menționat anterior, proiectul de raport subliniază necesitatea ca statele membre să țină seama cu fermitate de securitatea cibernetică atunci când achiziționează public produse cu elemente digitale și să se asigure că vulnerabilitățile sunt abordate cu promptitudine.
În ceea ce privește obligațiile producătorilor, raportorul consideră că stabilirea unei date pentru durata de viață preconizată a produsului nu este adecvată pentru o reglementare orizontală, care intenționează să acopere o gamă largă de produse, de la software la telefoane și mașini industriale. Din acest motiv, raportorul consideră că este mai adecvat ca producătorii să determine durata de viață a produselor lor, cu condiția ca durata sugerată să fie compatibilă cu așteptările rezonabile ale consumatorilor. O durată flexibilă ar permite, de asemenea, producătorilor să își prezinte produsele și să aibă o durată de viață îndelungată ca element al competitivității. Prin urmare, pentru a sensibiliza consumatorii cu privire la această chestiune specifică, regulamentul ar trebui, de asemenea, să oblige producătorii să indice în mod clar durata de viață preconizată a produsului pe ambalajul acestuia sau să o includă în acordurile contractuale și să informeze consumatorii atunci când durata de viață este pe punctul de a se încheia. În plus, proiectul de raport dorește să pună un accent deosebit pe siguranță. Prin urmare, raportorul consideră că producătorii ar trebui, de asemenea, să fie obligați să actualizeze automat, atunci când este posibil, elementele de siguranță ale produsului lor. În cazul în care un producător a definit o durată de viață preconizată mai mică de cinci ani, acesta ar trebui să fie pregătit să încheie acorduri contractuale cu întreprinderi care doresc să furnizeze servicii care prelungesc durata de viață a unui produs și să le comunice codul sursă. Această posibilitate nu ar trebui să implice un transfer de proprietate sau publicarea codului sursă.

În ceea ce privește obligațiile de raportare în temeiul articolului 11, raportorul dorește să alinieze calendarul la NIS2, astfel încât să existe mai multă coerență și securitate juridică pentru părțile interesate. În acest sens, raportorul sugerează raportarea incidentelor semnificative (mai degrabă decât a tuturor incidentelor), precum și exploatarea activă a vulnerabilităților, cu condiția să existe protocoale clare privind modul de gestionare în condiții de siguranță a acestor notificări, pentru a se evita răspândirea informațiilor privind vulnerabilitățile neremediate. Raportorul introduce, de asemenea, un mecanism de raportare voluntară a altor incidente, incidente evitate la limită și amenințări cibernetice.

Cu toate acestea, pentru a maximiza efectul raportării, este important să existe o entitate unică, inclusiv pentru a simplifica cerințele de raportare pentru producătorii din întreaga Uniune. În această privință, raportorul consideră că cea mai bună instituție care poate juca acest rol este ENISA. Prin urmare, având în vedere creșterea sarcinilor și a competențelor conferite ENISA, Comisia ar trebui să modifice fișa financiară legislativă care însoțește prezentul regulament, punând la dispoziția Agenției Uniunii Europene pentru Securitate Cibernetică posturi suplimentare și credite suplimentare corespunzătoare pentru a îndeplini sarcinile suplimentare ale agenției prevăzute în prezentul regulament.

În plus, un aspect fundamental pentru raportor este acela de a se asigura că există un sprijin suficient pentru ca întreprinderile să pună în aplicare cerințele prezentului regulament. Acest lucru este valabil în special pentru microîntreprinderi și întreprinderile mici și mijlocii, care, având în vedere capacitățile lor limitate, pot întâmpina unele provocări în ceea ce privește asigurarea conformității cu agențiile de rating de credit. Prin urmare, raportorul consideră că este esențial să se prelungească la 40 de luni data de la care regulamentul se aplică. În această

perioadă de tranziție, ar trebui să fie posibil ca producătorii să respecte CRA în mod voluntar, pentru a obține o prezumție de conformitate cu Regulamentul delegat referitor la Directiva privind echipamentele radio și pentru a se adapta la prezentul regulament înainte de punerea sa oficială în aplicare. În plus, raportorul dorește să sublinieze că este important ca Uniunea să ofere sprijin pentru perfecționarea și recalificarea lucrătorilor și să asigure disponibilitatea profesioniștilor din domeniul securității cibernetice, un element-cheie pentru succesul prezentului regulament.

În plus, ca abordare generală pentru a ajuta toate părțile interesate, raportorul solicită orientări din partea Comisiei pentru a oferi mai multe precizări cu privire la etapa efectivă de punere în aplicare, oferind astfel mai multă claritate tuturor părților implicate.

O altă problemă la fel de presantă pentru raportor este comerțul internațional. Din acest motiv, proiectul de raport solicită Comisiei să ia în considerare acorduri de recunoaștere reciprocă cu țări terțe care împărtășesc aceeași viziune, în cazul în care acestea au un nivel comparabil de dezvoltare tehnică și au o abordare compatibilă în ceea ce privește evaluarea conformității, asigurând același nivel de protecție ca cel prevăzut de prezentul regulament. Cu toate acestea, este esențial să se asigure o monitorizare adecvată a produselor care provin din țări riscante, care pot conține uși secrete sau alte vulnerabilități: ENISA ar trebui să se coordoneze cu autoritățile de supraveghere a pieței și să efectueze verificările necesare cu privire la vânzătorii care ar putea prezenta un profil de risc mai ridicat.

În cele din urmă, raportorul consideră că veniturile generate de sancțiuni ar trebui să fie alocate proiectelor, ceea ce va crește nivelul general de securitate cibernetică în întreaga Uniune și, prin urmare, să fie alocate programului Europa digitală, sprijinind proiecte care vizează, printre altele, recalificarea și perfecționarea forței de muncă actuale.

ANEXĂ: LISTA ENTITĂȚILOR SAU PERSOANELOR DE LA CARE RAPORTORUL A PRIMIT CONTRIBUȚII

Următoarea listă este întocmită în mod absolut voluntar, sub responsabilitatea exclusivă a raportorului. Raportorul a primit contribuții de la următoarele entități sau persoane în pregătirea raportului, până la adoptarea acestuia în comisie:

Entitatea și/sau persoana
ISC/2
ACEM
Airlines4Europe
Alliance for IoT and Edge Computing Innovation
Amazon
Camera de Comerț Americană
ANEC
Apple
APPLiA
Associazione Italiana Internet Provider
BDI
Beuc
Bitkom
BritCham
Broadcom
BSA - Alianța producătorilor de software
Business Europe
Card Payment Sweden
CEMA
Centrum für Europäische Politik
CNH
Confederația Industriilor Daneze (DI)
Confindustria
Coaliția pentru securitate cibernetică
DEKRA
Deutsche Telekom
Developers Alliance
Europa digitală
Enedis
Engineering
Ericsson
ESMIG
ETNO
ETRMA
Organizația Europeană de Securitate Cibernetică
European Materials Handling Federation (Federația Europeană de Manipulare a Materialelor) (FEM)

Eurosmart
Federunacoma
Free Software Foundation Europe
Asociația asiguratorilor din Germania
Giesecke+Devrient
GitHub
Google
GSMA
Hanbury Strategy
Huawei
IBM
Independent Retail Europe (Asociația europeană a grupurilor de detailiști independenți)
Information Technology Industry Council (Consiliul pentru Industria Tehnologiei Informatice)
Leaseurope
Lenovo
Mechanical Engineering Industry Association (Asociația industriei ingineriei mecanice) (VDMA)
MedTechEurope
Microsoft
Okta
Open Forum Europe
Orange
Orgalim
Reprezentanța permanentă a Belgiei
Reprezentanța permanentă a Italiei
Reprezentanța permanentă a Țărilor de Jos
Piaggio
Privacy International
SAP
Schneider Electric
Siemens
SME United
Splunk
Industriile tehnologice din Finlanda
Telefonica
Consiliul TIC
Trellix
Twillio
Unife
Grupul Vodafone
Wikimedia
Worldr
Xiaomi
Zoom

30.6.2023

AVIZ AL COMISIEI PENTRU PIAȚA INTERNĂ ȘI PROTECȚIA CONSUMATORILOR

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020
(COM(2022)0454 – C9-0308/2022 – 2022/0272(COD))

Raportor pentru aviz (*): Morten Løkkegaard

(*) Procedura comisiei asociate – articolul 57 din Regulamentul de procedură

JUSTIFICARE SUCCINTĂ

În calitate de fost raportor pentru aviz în cadrul Comisiei IMCO pentru Directiva NIS2, raportorul consideră că Actul privind reziliența cibernetică constituie un pas esențial și natural pentru îmbunătățirea securității cibernetice a Uniunii Europene. Având în vedere faptul că, prin definiție, securitatea cibernetică nu va fi niciodată completă 100 %, raportorul este de părere că este important să facem tot ce ne stă în putință pentru a reduce numărul verigilor slabe din Uniunea noastră și, în acest sens, Actul privind reziliența cibernetică este un pas binevenit. Trebuie să sporim securitatea cibernetică a produselor cu elemente digitale și a altor produse noi, cum ar fi dispozitivele IoT, devenite elemente naturale ale vieții de zi cu zi a consumatorilor și a întreprinderilor europene.

Întrucât Comisia IMCO este responsabilă de funcționarea și punerea în aplicare a pieței unice, inclusiv a pieței unice digitale, și de normele privind protecția consumatorilor, raportorul a încercat să introducă amendamente care vizează îmbunătățirea funcționării pieței interne, asigurând, în același timp, un nivel ridicat de protecție a consumatorilor în domeniul de aplicare al propunerii, în special în ceea ce privește cerințele de securitate cibernetică pentru produsele cu elemente digitale.

În plus, raportorul este de părere că trebuie îmbunătățite anumite aspecte ale propunerii de regulament, pentru a asigura claritatea juridică și coerența între dispozițiile relevante ale propunerii de regulament și a altor instrumente juridice. Acest lucru se referă în special la Directiva NIS2, la Regulamentul recent adoptat privind siguranța generală a produselor, la Regulamentul privind inteligența artificială și la Regulamentul privind echipamentele tehnice, precum și la o serie de acte delegate și de punere în aplicare relevante. Prin urmare, raportorul a propus amendamente care vizează îmbunătățirea clarității juridice și contribuie la asigurarea unei interpretări și aplicări coerente, eficace și consecvente a legislațiilor menționate.

În plus, întrucât microîntreprinderile și întreprinderile mici și mijlocii sunt actori economici esențiali pe piața digitală, raportorul a introdus o serie de amendamente pentru a simplifica procedurile administrative și a limita sarcina administrativă pentru întreprinderile mici, fără a

scădea nivelul de siguranță. În plus, raportorul a introdus amendamente care asigură faptul că microîntreprinderilor și IMM-urilor li se vor oferi orientări și consiliere specifice în ceea ce privește respectarea cerințelor din Actul privind reziliența cibernetică.

În cele din urmă, raportorul a introdus amendamente cu scopul de a asigura o comunicare mai eficientă cu autoritățile competente (autoritățile naționale de supraveghere a pieței, ENISA), precum și de a consolida dispozițiile privind obligațiile și competențele autorităților relevante în ceea ce privește plângerile, inspecțiile și activitățile comune. În plus, unele amendamente ale raportorului se axează pe îmbunătățirea cerințelor de securitate cibernetică pentru componentele integrate în produsele finale cu elemente digitale, specificând obligațiile operatorilor economici, cum ar fi producătorii și reprezentanții autorizați.

Raportorul reiterează poziția potrivit căreia introducerea Actului privind reziliența cibernetică este un pas imediat și natural pentru a înăspri impactul amenințărilor la adresa securității cibernetice în Uniunea noastră. Prin amendamentele propuse, raportorul a încercat să găsească echilibrul adecvat între asigurarea unui nivel sporit de securitate cibernetică în beneficiul consumatorilor europeni, cu o sarcină proporțională pentru comunitatea de afaceri. Ambiția raportorului este ca securitatea cibernetică să devină un parametru natural al concurenței pe piața internă. În acest sens, raportorul a încercat să adapteze propunerea.

AMENDAMENTE

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

Amendamentul 1

Propunere de regulament
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) Este necesar să se îmbunătățească funcționarea pieței interne prin stabilirea unui cadru juridic uniform pentru cerințele esențiale de securitate cibernetică pentru introducerea produselor cu elemente digitale pe piața Uniunii. Ar trebui abordate două probleme majore care generează costuri suplimentare pentru utilizatori și pentru societate: nivelul scăzut de securitate cibernetică a produselor cu elemente digitale, care se reflectă în răspândirea pe scară largă a vulnerabilităților și în furnizarea insuficientă și inconsecventă de actualizări de securitate pentru abordarea acestora, și accesul insuficient și înțelegerea insuficientă a informațiilor din partea utilizatorilor, ceea ce îi împiedică să aleagă produse cu caracteristici adecvate de securitate cibernetică sau să le utilizeze în mod securizat.	(1) Este necesar să se îmbunătățească funcționarea pieței interne***, asigurând în același timp un nivel ridicat de protecție a consumatorilor și de securitate cibernetică,*** prin stabilirea unui cadru juridic uniform pentru cerințele esențiale de securitate cibernetică pentru introducerea produselor cu elemente digitale pe piața Uniunii. Ar trebui abordate două probleme majore care generează costuri suplimentare pentru utilizatori și pentru societate: nivelul scăzut de securitate cibernetică a produselor cu elemente digitale, care se reflectă în răspândirea pe scară largă a vulnerabilităților și în furnizarea insuficientă și inconsecventă de actualizări de securitate pentru abordarea acestora, și accesul insuficient și înțelegerea insuficientă a informațiilor din partea utilizatorilor, ceea ce îi împiedică să aleagă produse cu caracteristici adecvate de securitate cibernetică sau să le utilizeze în mod securizat.

Amendamentul 2

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) În anumite condiții, toate produsele cu elemente digitale integrate într-un	(7) În anumite condiții, toate produsele cu elemente digitale integrate într-un

sistem electronic de informații mai mare sau conectate la un astfel de sistem pot servi drept vector de atac pentru actorii rău-intenționați. În consecință, chiar și hardware-ul și software-ul considerate mai puțin critice pot facilita compromiterea inițială a unui dispozitiv sau a unei rețele, permițând actorilor rău-intenționați să obțină un acces privilegiat la un sistem sau să se deplaseze lateral între sisteme. Prin urmare, producătorii ar trebui să se asigure că toate produsele ***conectabile*** cu elemente digitale sunt proiectate și dezvoltate în conformitate cu cerințele esențiale prevăzute în prezentul regulament. Sunt incluse atât produsele care pot fi conectate fizic prin interfețe hardware, cât și produsele care sunt conectate logic, de exemplu prin intermediul unor prize de rețea, canale, fișiere, interfețe de programare a aplicațiilor sau orice alt tip de interfață software. Întrucât amenințările la adresa securității cibernetice se pot propaga prin diverse produse cu elemente digitale înainte de a atinge un anumit obiectiv, de exemplu prin înlănțuirea mai multor exploatări de vulnerabilități, producătorii ar trebui să asigure, de asemenea, securitatea cibernetică a produselor care sunt conectate doar indirect la alte dispozitive sau rețele.	sistem electronic de informații mai mare sau conectate la un astfel de sistem pot servi drept vector de atac pentru actorii rău-intenționați. În consecință, chiar și hardware-ul și software-ul considerate mai puțin critice pot facilita compromiterea inițială a unui dispozitiv sau a unei rețele, permițând actorilor rău-intenționați să obțină un acces privilegiat la un sistem sau să se deplaseze lateral între sisteme. Prin urmare, producătorii ar trebui să se asigure că toate produsele cu elemente digitale ***conectate la o rețea externă sau la un dispozitiv extern*** sunt proiectate și dezvoltate în conformitate cu cerințele esențiale prevăzute în prezentul regulament. Sunt incluse atât produsele care pot fi conectate fizic ***la rețele sau la dispozitive externe*** prin interfețe hardware, cât și produsele care sunt conectate logic, de exemplu prin intermediul unor prize de rețea, canale, fișiere, interfețe de programare a aplicațiilor sau orice alt tip de interfață software. Întrucât amenințările la adresa securității cibernetice se pot propaga prin diverse produse cu elemente digitale înainte de a atinge un anumit obiectiv, de exemplu prin înlănțuirea mai multor exploatări de vulnerabilități, producătorii ar trebui să asigure, de asemenea, securitatea cibernetică a produselor care sunt conectate doar indirect la alte dispozitive sau rețele.

Amendamentul 3

Propunere de regulament
Considerentul 7 a (nou)

Textul propus de Comisie	*Amendamentul*
	(7a) Prezentul regulament nu ar trebui să se aplice rețelelor interne ale unui produs cu elemente digitale, dacă aceste rețele au puncte terminale dedicate și sunt complet izolate și protejate față de conexiunile de date externe.

Amendamentul 4

Propunere de regulament
Considerentul 7 b (nou)

Textul propus de Comisie	*Amendamentul*
	(7b) Prezentul regulament nu ar trebui să se aplice în cazul pieselor de schimb destinate exclusiv înlocuirii componentelor defecte ale produselor cu elemente digitale, pentru a le restabili funcționalitatea.

Amendamentul 5

Propunere de regulament
Considerentul 9

Textul propus de Comisie	*Amendamentul*
(9) Prezentul regulament asigură un nivel ridicat de securitate cibernetică a produselor cu elemente digitale. Acesta nu reglementează serviciile, precum software-ul ca serviciu (SaaS)***, cu excepția soluțiilor de prelucrare de date la distanță referitoare la un produs cu elemente digitale, înțelese ca orice prelucrare de date la distanță pentru care software-ul este proiectat și dezvoltat de producătorul produsului în cauză sau sub responsabilitatea producătorului respectiv și a cărei absență ar împiedica un astfel de produs cu elemente digitale să își îndeplinească una dintre funcții***. [Directiva XXX/XXXX (NIS2)] instituie cerințe de raportare a securității cibernetice și a incidentelor pentru entitățile esențiale și importante, cum ar fi infrastructura critică, în vederea creșterii rezilienței serviciilor pe care le furnizează. [Directiva XXX/XXXX (NIS2)] se aplică serviciilor de cloud computing și modelelor de servicii de cloud, precum SaaS. Toate entitățile care furnizează servicii de cloud computing în Uniune și care ating sau depășesc pragul pentru întreprinderile	(9) Prezentul regulament asigură un nivel ridicat de securitate cibernetică a produselor cu elemente digitale. Acesta nu reglementează serviciile, precum software-ul ca serviciu (SaaS). [Directiva XXX/XXXX (NIS2)] instituie cerințe de raportare a securității cibernetice și a incidentelor pentru entitățile esențiale și importante, cum ar fi infrastructura critică, în vederea creșterii rezilienței serviciilor pe care le furnizează. [Directiva XXX/XXXX (NIS2)] se aplică serviciilor de cloud computing și modelelor de servicii de cloud, precum SaaS. Toate entitățile care furnizează servicii de cloud computing în Uniune și care ating sau depășesc pragul pentru întreprinderile mijlocii intră în domeniul de aplicare al directivei respective.

mijlocii intră în domeniul de aplicare al directivei respective.

Amendamentul 6

Propunere de regulament
Considerentul 10

Textul propus de Comisie	*Amendamentul*
(10) Pentru a nu împiedica inovarea sau cercetarea, software-ul liber și cu sursă deschisă dezvoltat sau furnizat în afara desfășurării unei activități comerciale nu ar trebui să intre sub incidența prezentului regulament. Acest lucru este valabil în special în cazul software-ului, inclusiv al codului sursă și al versiunilor modificate ale acestuia, care este partajat în mod deschis și care poate fi accesat, utilizat, modificat și distribuit în mod liber. ***În contextul software-ului***, o activitate comercială ar putea fi caracterizată ***nu numai*** prin perceperea unui preț pentru ***un produs***, ***ci*** și prin perceperea unui preț pentru servicii de asistență ***tehnică***, prin furnizarea unei platforme software prin intermediul căreia producătorul monetizează alte servicii sau prin utilizarea datelor cu caracter personal în alte scopuri decât îmbunătățirea securității, a compatibilității sau a interoperabilității software-ului.	(10) ***Software-ul și datele care sunt partajate în mod deschis și pe care utilizatorii le pot accesa, utiliza, modifica și redistribui în mod liber sau versiunile modificate ale acestora pot contribui la cercetarea și inovarea pe piață. De asemenea, cercetările Comisiei arată că software-ul liber și cu sursă deschisă poate contribui cu 65 până la 95 de miliarde EUR la PIB-ul Uniunii și poate oferi posibilități de creștere semnificative pentru economia europeană.*** Pentru a nu împiedica inovarea sau cercetarea, software-ul liber și cu sursă deschisă dezvoltat sau furnizat în afara desfășurării unei activități comerciale nu ar trebui să intre sub incidența prezentului regulament. Acest lucru este valabil în special în cazul software-ului, inclusiv al codului sursă și al versiunilor modificate ale acestuia, care este partajat în mod deschis și care poate fi accesat, utilizat, modificat și distribuit în mod liber. O activitate comercială, ***în sensul punerii la dispoziție pe piață,*** ar putea fi caracterizată ***însă*** prin perceperea unui preț pentru ***o componentă software liberă și cu sursă deschisă***, ***dar*** și prin ***monetizare, precum*** perceperea unui preț pentru servicii de asistență ***tehnică sau actualizări de software plătite, cu excepția cazului în care acest lucru servește numai la recuperarea costurilor reale***, prin furnizarea unei platforme software prin intermediul căreia producătorul monetizează alte servicii sau prin utilizarea datelor cu caracter personal în alte scopuri decât îmbunătățirea securității, a compatibilității sau a interoperabilității

software-ului. ***Nici dezvoltarea colaborativă a unor componente software libere și cu sursă deschisă, nici punerea lor la dispoziție în registre deschise nu ar trebui să constituie o introducere pe piață sau o punere în funcțiune. Circumstanțele în care a fost dezvoltat produsul sau modul în care a fost finanțată dezvoltarea nu ar trebui luate în considerare atunci când se stabilește natura comercială sau necomercială a activității respective. Atunci când software-ul cu sursă deschisă este integrat într-un produs finit cu elemente digitale care este introdus pe piață, operatorul economic care a introdus pe piață produsul finit cu elemente digitale ar trebui să fie responsabil pentru conformitatea produsului, inclusiv a componentelor libere și cu sursă deschisă.***

Amendamentul 7

Propunere de regulament
Considerentul 11

Textul propus de Comisie	*Amendamentul*
(11) Un internet sigur este indispensabil pentru funcționarea infrastructurilor critice și pentru societate în ansamblu. [Directiva XXX/XXXX (NIS2)] vizează asigurarea unui nivel ridicat de securitate cibernetică a serviciilor furnizate de entități esențiale și importante, inclusiv de furnizori de infrastructură digitală care sprijină funcțiile de bază ale internetului deschis și asigură accesul la internet și serviciile de internet. Prin urmare, este important ca produsele cu elemente digitale necesare pentru ca furnizorii de infrastructură digitală să asigure funcționarea internetului să fie dezvoltate în mod securizat și să respecte standardele consacrate în materie de securitate a internetului. Prezentul regulament, care se aplică tuturor produselor hardware și software ***conectabile***, are ca scop, de asemenea, să	(11) Un internet sigur este indispensabil pentru funcționarea infrastructurilor critice și pentru societate în ansamblu. [Directiva XXX/XXXX (NIS2)] vizează asigurarea unui nivel ridicat de securitate cibernetică a serviciilor furnizate de entități esențiale și importante, inclusiv de furnizori de infrastructură digitală care sprijină funcțiile de bază ale internetului deschis și asigură accesul la internet și serviciile de internet. Prin urmare, este important ca produsele cu elemente digitale necesare pentru ca furnizorii de infrastructură digitală să asigure funcționarea internetului să fie dezvoltate în mod securizat și să respecte standardele consacrate în materie de securitate a internetului. Prezentul regulament, care se aplică tuturor produselor hardware și software ***conectate la o rețea externă sau la un dispozitiv***

faciliteze respectarea de către furnizorii de infrastructură digitală a cerințelor lanțului de aprovizionare în temeiul [Directiva XXX/XXXX (NIS2)], prin asigurarea faptului că produsele cu elemente digitale pe care le utilizează pentru furnizarea serviciilor lor sunt dezvoltate în mod securizat și că au acces la actualizări de securitate în timp util pentru aceste produse.	***extern***, are ca scop, de asemenea, să faciliteze respectarea de către furnizorii de infrastructură digitală a cerințelor lanțului de aprovizionare în temeiul [Directiva XXX/XXXX (NIS2)], prin asigurarea faptului că produsele cu elemente digitale pe care le utilizează pentru furnizarea serviciilor lor sunt dezvoltate în mod securizat și că au acces la actualizări de securitate în timp util pentru aceste produse.

Amendamentul 8

Propunere de regulament
Considerentul 15

Textul propus de Comisie	*Amendamentul*
(15) Regulamentul delegat (UE) 2022/30 precizează că cerințele esențiale prevăzute la articolul 3 alineatul (3) litera (d) (prejudiciile aduse rețelei și utilizarea necorespunzătoare a resurselor acesteia), litera (e) (datele cu caracter personal și viața privată) și litera (f) (fraudele) din Directiva 2014/53/UE se aplică anumitor echipamente radio. [Decizia de punere în aplicare XXX/2022 a Comisiei privind o cerere de standardizare adresată organizațiilor europene de standardizare] stabilește cerințe pentru elaborarea unor standarde specifice care să detalieze modul în care ar trebui abordate aceste trei cerințe esențiale. Cerințele esențiale prevăzute de prezentul regulament includ toate elementele cerințelor esențiale menționate la articolul 3 alineatul (3) literele (d), (e) și (f) din Directiva 2014/53/UE. În plus, cerințele esențiale prevăzute de prezentul regulament sunt aliniate la obiectivele cerințelor pentru standardele specifice incluse în cererea de standardizare respectivă. Prin urmare, ***în cazul în care*** Comisia abrogă ***sau modifică*** Regulamentul delegat (UE) 2022/30, cu consecința că acesta încetează să se aplice în cazul anumitor produse care fac obiectul	(15) Regulamentul delegat (UE) 2022/30 precizează că cerințele esențiale prevăzute la articolul 3 alineatul (3) litera (d) (prejudiciile aduse rețelei și utilizarea necorespunzătoare a resurselor acesteia), litera (e) (datele cu caracter personal și viața privată) și litera (f) (fraudele) din Directiva 2014/53/UE se aplică anumitor echipamente radio. [Decizia de punere în aplicare XXX/2022 a Comisiei privind o cerere de standardizare adresată organizațiilor europene de standardizare] stabilește cerințe pentru elaborarea unor standarde specifice care să detalieze modul în care ar trebui abordate aceste trei cerințe esențiale. Cerințele esențiale prevăzute de prezentul regulament includ toate elementele cerințelor esențiale menționate la articolul 3 alineatul (3) literele (d), (e) și (f) din Directiva 2014/53/UE. În plus, cerințele esențiale prevăzute de prezentul regulament sunt aliniate la obiectivele cerințelor pentru standardele specifice incluse în cererea de standardizare respectivă. Prin urmare, ***atunci când*** Comisia abrogă Regulamentul delegat (UE) 2022/30, cu consecința că acesta încetează să se aplice în cazul anumitor produse care fac obiectul prezentului

prezentului regulament, Comisia și organizațiile europene de standardizare ar trebui să ia în considerare activitatea de standardizare desfășurată în contextul Deciziei de punere în aplicare C(2022) 5637 a Comisiei privind o cerere de standardizare pentru Regulamentul delegat (UE) 2022/30 RED atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a prezentului regulament.

regulament, Comisia și organizațiile europene de standardizare ar trebui să ia în considerare activitatea de standardizare desfășurată în contextul Deciziei de punere în aplicare C(2022) 5637 a Comisiei privind o cerere de standardizare pentru Regulamentul delegat (UE) 2022/30 RED atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a prezentului regulament.

Amendamentul 9

Propunere de regulament
Considerentul 18 a (nou)

Textul propus de Comisie	*Amendamentul*
	(18a) Pentru a garanta că dezvoltatorii individuali sau microdezvoltatorii de software, astfel cum sunt definiți în Recomandarea 2003/361/CE a Comisiei, nu se confruntă cu obstacole financiare majore și nu sunt descurajați să testeze validarea conceptului, precum și justificarea economică pe piață, aceste entități ar trebui să depună eforturi cât mai mari pentru a respecta cerințele din această propunere în timpul celor șase luni de la introducerea pe piață a unui software. Acest regim special ar trebui să prevină efectul de intimidare pe care l-ar putea avea costurile ridicate de conformitate și de intrare asupra antreprenorilor sau a persoanelor competente care iau în considerare posibilitatea dezvoltării de software în Uniune. Totuși, acest regim special nu ar trebui să se aplice produselor extrem de critice cu elemente digitale.

Amendamentul 10

Propunere de regulament
Considerentul 19

Textul propus de Comisie	*Amendamentul*
(19) Anumite sarcini prevăzute în prezentul regulament ar trebui să fie îndeplinite de ENISA, în conformitate cu articolul 3 alineatul (2) din Regulamentul (UE) 2019/881. În special, ENISA ar trebui să primească notificări de la producători cu privire la vulnerabilitățile exploatate activ conținute în produsele cu elemente digitale, precum și cu privire la incidentele care au un impact asupra securității acestor produse. ENISA ar trebui, de asemenea, să transmită aceste notificări echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) relevante sau, respectiv, punctelor unice de contact relevante din statele membre desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și să informeze autoritățile relevante de supraveghere a pieței cu privire la vulnerabilitatea notificată. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită grupului de cooperare menționat în Directiva [Directiva XXX/XXXX (NIS2)]. În plus, având în vedere expertiza și mandatul său, ENISA ar trebui să fie în măsură să sprijine procesul de punere în aplicare a prezentului regulament. În special, aceasta ar trebui să fie în măsură să propună activități comune care să fie desfășurate de autoritățile de supraveghere a pieței pe baza unor indicații sau informații privind o posibilă neconformitate cu prezentul regulament a produselor cu elemente digitale din mai multe state membre sau să identifice categoriile de produse pentru care ar trebui organizate acțiuni de control coordonate simultane. În circumstanțe excepționale, la cererea Comisiei, ENISA ar trebui să poată efectua evaluări cu privire la anumite produse cu elemente digitale care prezintă	(19) Anumite sarcini prevăzute în prezentul regulament ar trebui să fie îndeplinite de ENISA, în conformitate cu articolul 3 alineatul (2) din Regulamentul (UE) 2019/881. În special, ENISA ar trebui să primească notificări de la producători***, prin intermediul unei alerte timpurii,*** cu privire la vulnerabilitățile exploatate activ conținute în produsele cu elemente digitale, precum și cu privire la incidentele care au un impact ***semnificativ*** asupra securității acestor produse. ENISA ar trebui, de asemenea, să transmită aceste notificări echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) relevante sau, respectiv, punctelor unice de contact relevante din statele membre desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și să informeze ***imediat*** autoritățile relevante de supraveghere a pieței cu privire la ***existența unei vulnerabilități și, după caz, cu privire la măsurile potențiale de atenuare a riscurilor. În cazul în care o vulnerabilitate notificată nu dispune de măsuri corective sau de atenuare, ENISA ar trebui să se asigure că informațiile cu privire la*** vulnerabilitatea notificată ***sunt partajate în conformitate cu protocoale stricte de securitate și pe baza principiului necesității de a cunoaște***. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită grupului de cooperare menționat în Directiva [Directiva XXX/XXXX (NIS2)]. În plus, având în vedere expertiza și mandatul său, ENISA ar trebui să fie în măsură să sprijine procesul de punere în aplicare a prezentului regulament. În special, aceasta ar trebui să fie în măsură să propună activități comune care să fie desfășurate de autoritățile de

un risc semnificativ în materie de securitate cibernetică, în cazul în care este necesară o intervenție imediată pentru a menține buna funcționare a pieței interne.	supraveghere a pieței pe baza unor indicații sau informații privind o posibilă neconformitate cu prezentul regulament a produselor cu elemente digitale din mai multe state membre sau să identifice categoriile de produse pentru care ar trebui organizate acțiuni de control coordonate simultane. În circumstanțe excepționale, la cererea Comisiei, ENISA ar trebui să poată efectua evaluări cu privire la anumite produse cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică, în cazul în care este necesară o intervenție imediată pentru a menține buna funcționare a pieței interne.

Amendamentul 11

Propunere de regulament
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) Produsele cu elemente digitale ar trebui să poarte marcajul CE pentru a indica conformitatea lor cu prezentul regulament, astfel încât să poată circula liber în cadrul pieței interne. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață a produselor cu elemente digitale care sunt conforme cu cerințele prevăzute în prezentul regulament și care poartă marcajul CE.	(20) Produsele cu elemente digitale ar trebui să poarte marcajul CE pentru a indica ***în mod vizibil, lizibil și fără posibilitate de ștergere*** conformitatea lor cu prezentul regulament, astfel încât să poată circula liber în cadrul pieței interne. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață a produselor cu elemente digitale care sunt conforme cu cerințele prevăzute în prezentul regulament și care poartă marcajul CE.

Amendamentul 12

Propunere de regulament
Considerentul 22

Textul propus de Comisie	*Amendamentul*
(22) Pentru a se asigura că produsele cu elemente digitale, atunci când sunt introduse pe piață, nu prezintă riscuri în materie de securitate cibernetică pentru	(22) Pentru a se asigura că produsele cu elemente digitale, atunci când sunt introduse pe piață, nu prezintă riscuri în materie de securitate cibernetică pentru

persoane și organizații, ar trebui stabilite cerințe esențiale pentru astfel de produse. Atunci când produsele sunt modificate ulterior, prin mijloace fizice sau digitale, într-un mod care nu este prevăzut de producător și care poate implica faptul că acestea nu mai îndeplinesc cerințele esențiale relevante, modificarea ar trebui considerată substanțială. De exemplu, actualizările sau reparațiile software-ului ar putea fi asimilate operațiunilor de întreținere, cu condiția ca acestea să nu modifice un produs deja introdus pe piață astfel încât să poată fi afectată conformitatea cu cerințele aplicabile sau să poată fi schimbată utilizarea preconizată pentru care a fost evaluat produsul. La fel ca în cazul reparațiilor sau al modificărilor fizice, un produs cu elemente digitale ar trebui să fie considerat ca fiind modificat substanțial de o modificare a software-ului dacă actualizarea software-ului modifică tipul, performanța sau funcțiile inițiale preconizate ale produsului, iar aceste modificări nu au fost prevăzute în evaluarea inițială a riscurilor sau dacă natura pericolului s-a schimbat sau nivelul de risc a crescut ca urmare a actualizării software-ului.

persoane și organizații, ar trebui stabilite cerințe esențiale pentru astfel de produse. Atunci când produsele sunt modificate ulterior, prin mijloace fizice sau digitale, într-un mod care nu este prevăzut de producător și care poate implica faptul că acestea nu mai îndeplinesc cerințele esențiale relevante, modificarea ar trebui considerată substanțială. De exemplu, actualizările sau reparațiile software-ului***, precum ajustările minore ale codului sursă care pot îmbunătăți securitatea și funcționarea,*** ar putea fi asimilate operațiunilor de întreținere, cu condiția ca acestea să nu modifice un produs deja introdus pe piață astfel încât să poată fi afectată conformitatea cu cerințele aplicabile sau să poată fi schimbată utilizarea preconizată pentru care a fost evaluat produsul. La fel ca în cazul reparațiilor sau al modificărilor fizice, un produs cu elemente digitale ar trebui să fie considerat ca fiind modificat substanțial de o modificare a software-ului dacă actualizarea software-ului modifică tipul, performanța sau funcțiile inițiale preconizate ale produsului, iar aceste modificări nu au fost prevăzute în evaluarea inițială a riscurilor sau dacă natura pericolului s-a schimbat sau nivelul de risc a crescut ca urmare a actualizării software-ului.

Amendamentul 13

Propunere de regulament
Considerentul 23

Textul propus de Comisie	*Amendamentul*
(23) În conformitate cu noțiunea stabilită de comun acord a modificării substanțiale pentru produsele reglementate de legislația de armonizare a Uniunii, ori de câte ori apare o modificare substanțială care ar putea afecta conformitatea produsului cu prezentul regulament sau atunci când scopul preconizat al produsului	(23) În conformitate cu noțiunea stabilită de comun acord a modificării substanțiale pentru produsele reglementate de legislația de armonizare a Uniunii, ori de câte ori apare o modificare substanțială care ar putea afecta conformitatea produsului cu prezentul regulament sau atunci când scopul preconizat al produsului

se modifică, este oportun ca conformitatea produsului cu elemente digitale să fie verificată și, după caz, ***ca acesta*** să fie ***supus unei noi evaluări a*** conformității. După caz, dacă producătorul efectuează o evaluare a conformității care implică un terț, modificările care ar putea duce la modificări substanțiale ar trebui notificate părții terțe.	se modifică, este oportun ca conformitatea produsului cu elemente digitale să fie verificată și, după caz, să fie ***actualizată evaluarea*** conformității. După caz, dacă producătorul efectuează o evaluare a conformității care implică un terț, modificările care ar putea duce la modificări substanțiale ar trebui notificate părții terțe. ***Evaluarea ulterioară a conformității ar trebui să abordeze modificările ce conduc la noua evaluare, cu excepția cazului în care aceste modificări au un impact semnificativ asupra conformității altor componente ale produsului. În cazul în care sunt implementate actualizări de software, producătorul nu ar trebui să fie obligat să efectueze o altă evaluare a conformității produsului cu elemente digitale, cu excepția cazului în care actualizarea software-ului duce la o modificare substanțială a produsului cu elemente digitale.***

Amendamentul 14

Propunere de regulament
Considerentul 24 a (nou)

Textul propus de Comisie	*Amendamentul*
	(24a) Producătorii de produse cu elemente digitale ar trebui să se asigure că actualizările software sunt furnizate într-o manieră clară și transparentă, făcând o diferențiere clară între actualizările de securitate și cele de funcționalitate. În timp ce actualizările de securitate sunt concepute pentru a reduce nivelul de risc al unui produs cu elemente digitale, adoptarea actualizărilor de funcționalitate furnizate de producător ar trebui să rămână întotdeauna la alegerea utilizatorului. Prin urmare, producătorii ar trebui să ofere aceste actualizări separat, cu excepția cazului în care acest lucru este imposibil din punct de vedere tehnic. Producătorii ar trebui să le ofere

consumatorilor informații adecvate privind motivele fiecărei actualizări și impactul prevăzut al acesteia asupra produsului, precum și un mecanism de renunțare clar și ușor de utilizat.

Amendamentul 15

Propunere de regulament
Considerentul 25

Textul propus de Comisie	*Amendamentul*
(25) Produsele cu elemente digitale ar trebui considerate critice dacă impactul negativ al exploatării potențialelor vulnerabilități în materie de securitate cibernetică ale produsului poate fi grav din cauza, printre altele, a funcționalității legate de securitatea cibernetică sau a utilizării preconizate. În special, vulnerabilitățile produselor cu elemente digitale care au o funcționalitate legată de securitatea cibernetică, de exemplu elementele de securitate, pot conduce la o propagare a problemelor de securitate în întregul lanț de aprovizionare. Gravitatea impactului unui incident de securitate cibernetică poate crește, de asemenea, atunci când se ia în considerare utilizarea preconizată a produsului***, de exemplu într-un cadru industrial*** sau în contextul unei entități esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)] sau pentru îndeplinirea unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal.	(25) Produsele cu elemente digitale ar trebui considerate critice dacă impactul negativ al exploatării potențialelor vulnerabilități în materie de securitate cibernetică ale produsului poate fi grav din cauza, printre altele, a funcționalității legate de securitatea cibernetică sau a utilizării preconizate. În special, vulnerabilitățile produselor cu elemente digitale care au o funcționalitate legată de securitatea cibernetică, de exemplu elementele de securitate, pot conduce la o propagare a problemelor de securitate în întregul lanț de aprovizionare. Gravitatea impactului unui incident de securitate cibernetică poate crește, de asemenea, atunci când se ia în considerare utilizarea preconizată a produsului ***în aplicații critice în medii sensibile*** sau în contextul unei entități esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)] sau pentru îndeplinirea unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal.

Amendamentul 16

Propunere de regulament
Considerentul 26

Textul propus de Comisie	*Amendamentul*
(26) Produsele critice cu elemente	(26) Produsele critice cu elemente

digitale ar trebui să facă obiectul unor proceduri mai stricte de evaluare a conformității, menținând, în același timp, o abordare proporțională. În acest scop, produsele critice cu elemente digitale ar trebui împărțite în două clase, în funcție de nivelul de risc de securitate cibernetică legat de aceste categorii de produse. Un potențial incident cibernetic care implică produse din clasa II ar putea avea un impact negativ mai mare decât un incident care implică produse din clasa I, de exemplu din cauza naturii funcției lor legate de securitatea cibernetică sau a utilizării preconizate în medii sensibile, și, prin urmare, ar trebui să facă obiectul unei proceduri mai stricte de evaluare a conformității.

digitale ar trebui să facă obiectul unor proceduri mai stricte de evaluare a conformității, menținând, în același timp, o abordare proporțională. În acest scop, produsele critice cu elemente digitale ar trebui împărțite în două clase, în funcție de nivelul de risc de securitate cibernetică legat de aceste categorii de produse. Un potențial incident cibernetic care implică produse din clasa II ar putea avea un impact negativ mai mare decât un incident care implică produse din clasa I, de exemplu din cauza naturii funcției lor legate de securitatea cibernetică sau a utilizării preconizate în medii sensibile, și, prin urmare, ar trebui să facă obiectul unei proceduri mai stricte de evaluare a conformității. ***Ca excepție, întreprinderile mici și microîntreprinderile ar trebui să poată utiliza procedura pentru produsele din clasa I.***

Amendamentul 17

Propunere de regulament
Considerentul 29

Textul propus de Comisie	*Amendamentul*
(29) Produsele cu elemente digitale clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul 6 din Regulamentul[27] [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament ar trebui să respecte cerințele esențiale prevăzute în prezentul regulament. Atunci când aceste sisteme de IA cu grad ridicat de risc îndeplinesc cerințele esențiale ale prezentului regulament, acestea ar trebui să fie considerate conforme cu cerințele de securitate cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], în măsura în care cerințele respective sunt acoperite de declarația de conformitate UE sau de anumite părți ale	(29) Produsele cu elemente digitale ***sau produsele parțial finalizate cu elemente digitale*** clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul 6 din Regulamentul[27] [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament ar trebui să respecte cerințele esențiale prevăzute în prezentul regulament. Atunci când aceste sisteme de IA cu grad ridicat de risc îndeplinesc cerințele esențiale ale prezentului regulament, acestea ar trebui să fie considerate conforme cu cerințele de securitate cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], în măsura în care cerințele respective sunt acoperite de declarația de

acesteia, emisă în temeiul prezentului regulament. În ceea ce privește procedurile de evaluare a conformității referitoare la cerințele esențiale de securitate cibernetică ale unui produs cu elemente digitale care face obiectul prezentului regulament și este clasificat ca sistem de IA cu grad ridicat de risc, dispozițiile relevante ***ale articolului 43*** din Regulamentul [Regulamentul privind inteligența artificială] ar trebui să se aplice de regulă în locul dispozițiilor respective din prezentul regulament. ***Totuși,*** această regulă ***nu*** ar trebui să ***conducă la reducerea nivelului necesar*** de asigurare pentru produsele critice cu elemente digitale care intră sub incidența prezentului regulament. ***Prin urmare, prin derogare de la această regulă,*** sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al Regulamentului [Regulamentul privind inteligența artificială] și sunt, de asemenea, clasificate drept produse critice cu elemente digitale în temeiul prezentului regulament ***și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa VI la Regulamentul [Regulamentul privind inteligența artificială]*** ar trebui să ***facă obiectul dispozițiilor privind evaluarea*** conformității ***ale prezentului regulament*** în ***ceea ce privește cerințele esențiale ale*** prezentului regulament***. În acest caz, pentru toate celelalte aspecte vizate de Regulamentul [Regulamentul privind inteligența artificială] ar trebui să se aplice dispozițiile privind evaluarea*** conformității ***bazată pe control intern prevăzute în anexa VI la Regulamentul [Regulamentul privind inteligența artificială]***.

[27] Regulamentul [Regulamentul privind inteligența artificială].

conformitate UE sau de anumite părți ale acesteia, emisă în temeiul prezentului regulament. În ceea ce privește procedurile de evaluare a conformității referitoare la cerințele esențiale de securitate cibernetică ale unui produs cu elemente digitale care face obiectul prezentului regulament și este clasificat ca sistem de IA cu grad ridicat de risc, dispozițiile relevante ***din [dispozițiile aplicabile]*** din Regulamentul [Regulamentul privind inteligența artificială] ar trebui să se aplice de regulă în locul dispozițiilor respective din prezentul regulament. Această regulă ar trebui să ***creeze un nivel ridicat*** de asigurare pentru produsele critice cu elemente digitale care intră sub incidența prezentului regulament. ***Pentru*** sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al Regulamentului [Regulamentul privind inteligența artificială] și sunt, de asemenea, clasificate drept produse critice cu elemente digitale în temeiul prezentului regulament***, organismul sectorial responsabil notificat*** ar trebui să ***fie responsabil pentru efectuarea evaluării*** conformității în ***temeiul*** prezentului regulament ***și să conducă procesul administrativ astfel încât operatorii economici să își poată adresa cererea de evaluare a*** conformității ***unui singur organism de reglementare***.

[27] Regulamentul [Regulamentul privind inteligența artificială].

Amendamentul 18

Propunere de regulament
Considerentul 32

Textul propus de Comisie	*Amendamentul*
(32) Pentru a se asigura faptul că produsele cu elemente digitale sunt sigure atât în momentul introducerii lor pe piață, cât și pe parcursul întregului lor ciclu de viață, este necesar să se stabilească cerințe esențiale pentru gestionarea vulnerabilităților și cerințe esențiale de securitate cibernetică legate de proprietățile produselor cu elemente digitale. Deși producătorii ar trebui să respecte toate cerințele esențiale legate de gestionarea vulnerabilităților și să se asigure că toate produsele lor sunt livrate fără nicio vulnerabilitate exploatabilă cunoscută, aceștia ar trebui să stabilească celelalte cerințe esențiale legate de proprietățile produsului care sunt relevante pentru tipul de produs în cauză. În acest scop, producătorii ar trebui să efectueze o evaluare a riscurilor de securitate cibernetică asociate unui produs cu elemente digitale pentru a identifica riscurile relevante și cerințele esențiale relevante și pentru a aplica în mod corespunzător standarde armonizate ***sau specificații comune*** adecvate.	(32) Pentru a se asigura faptul că produsele cu elemente digitale sunt sigure atât în momentul introducerii lor pe piață, cât și pe parcursul întregului lor ciclu de viață, este necesar să se stabilească cerințe esențiale pentru gestionarea vulnerabilităților și cerințe esențiale de securitate cibernetică legate de proprietățile produselor cu elemente digitale. Deși producătorii ar trebui să respecte toate cerințele esențiale legate de gestionarea vulnerabilităților și să se asigure că toate produsele lor sunt livrate fără nicio vulnerabilitate exploatabilă cunoscută, aceștia ar trebui să stabilească celelalte cerințe esențiale legate de proprietățile produsului care sunt relevante pentru tipul de produs în cauză. În acest scop, producătorii ar trebui să efectueze o evaluare a riscurilor de securitate cibernetică asociate unui produs cu elemente digitale pentru a identifica riscurile relevante și cerințele esențiale relevante și pentru a aplica în mod corespunzător standarde armonizate adecvate.

Amendamentul 19

Propunere de regulament
Considerentul 33 a (nou)

Textul propus de Comisie	*Amendamentul*
	(33a) Pentru a garanta că produsele sunt proiectate, dezvoltate și fabricate în conformitate cu cerințele esențiale prevăzute în secțiunea 1 din anexa I, producătorii ar trebui să dea dovadă de diligență atunci când integrează componente obținute de la terți în produsele cu elemente digitale. Acesta este cazul pentru componentele care sunt

adaptate și integrate, ținând cont de particularitățile produsului, în special în cazul software-ului liber și cu sursă deschisă care nu a fost introdus pe piață în schimbul unei monetizări financiare sau de alt tip.

Amendamentul 20

Propunere de regulament
Considerentul 34

Textul propus de Comisie	*Amendamentul*
(34) Pentru a se asigura că echipele CSIRT naționale și punctele unice de contact desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XX/XXXX (NIS2)] primesc informațiile necesare pentru îndeplinirea sarcinilor lor și pentru creșterea nivelului general de securitate cibernetică a entităților esențiale și importante, precum și pentru a asigura funcționarea eficace a autorităților de supraveghere a pieței, producătorii de produse cu elemente digitale ar trebui să informeze ENISA cu privire la vulnerabilitățile care sunt exploatate activ. Întrucât majoritatea produselor cu elemente digitale sunt comercializate pe întreaga piață internă, orice vulnerabilitate exploatată a unui produs cu elemente digitale ar trebui considerată o amenințare la adresa funcționării pieței interne. De asemenea, producătorii ar trebui să ia în considerare divulgarea vulnerabilităților remediate în baza de date europeană privind vulnerabilitățile instituită în temeiul Directivei [Directiva XX/XXXX (NIS2)] și gestionată de ENISA sau în orice altă bază de date privind vulnerabilitățile accesibilă publicului.	(34) Pentru a se asigura că echipele CSIRT naționale și punctele unice de contact desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XX/XXXX (NIS2)] primesc informațiile necesare pentru îndeplinirea sarcinilor lor și pentru creșterea nivelului general de securitate cibernetică a entităților esențiale și importante, precum și pentru a asigura funcționarea eficace a autorităților de supraveghere a pieței, producătorii de produse cu elemente digitale ar trebui să informeze ENISA***, fără întârzieri nejustificate și, în orice caz, în termen de 48 de ore de la data la care au luat cunoștință de aceasta, prin intermediul unei alerte timpurii,*** cu privire la vulnerabilitățile care sunt exploatate activ***. Producătorii ar trebui să comunice ENISA, fără întârzieri nejustificate, din momentul în care au luat cunoștință de vulnerabilitatea exploatată în mod activ care are un impact semnificativ asupra securității produsului cu elemente digitale, mai multe detalii cu privire la vulnerabilitatea exploatată. Toate celelalte vulnerabilități care nu au un impact semnificativ asupra securității produsului cu elemente digitale ar trebui notificate ENISA odată ce vulnerabilitatea a fost remediată***. Întrucât majoritatea produselor cu elemente digitale sunt comercializate pe întreaga piață internă, orice vulnerabilitate exploatată a

unui produs cu elemente digitale ar trebui considerată o amenințare la adresa funcționării pieței interne. De asemenea, producătorii ar trebui să ia în considerare divulgarea vulnerabilităților remediate în baza de date europeană privind vulnerabilitățile instituită în temeiul Directivei [Directiva XX/XXXX (NIS2)] și gestionată de ENISA sau în orice altă bază de date privind vulnerabilitățile accesibilă publicului.

Amendamentul 21

Propunere de regulament
Considerentul 34 a (nou)

Textul propus de Comisie	*Amendamentul*
	(34a) ENISA ar trebui să fie responsabilă pentru publicarea și menținerea unei baze de date a vulnerabilităților exploatate cunoscute. Producătorii ar trebui să monitorizeze baza de date și să notifice vulnerabilitățile care se regăsesc în produsele lor.

Amendamentul 22

Propunere de regulament
Considerentul 35

Textul propus de Comisie	*Amendamentul*
(35) Producătorii ar trebui, de asemenea, să raporteze către ENISA orice incident care are un impact asupra securității produsului cu elemente digitale. Fără a aduce atingere obligațiilor de raportare a incidentelor prevăzute în Directiva [Directiva XXX/XXXX (NIS2)] pentru entitățile esențiale și importante, este esențial ca ENISA, punctele unice de contact desemnate de statele membre în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și autoritățile de supraveghere a pieței să	(35) Producătorii ar trebui, de asemenea, să raporteze către ENISA***, printr-o alertă timpurie,*** orice incident care are un impact ***semnificativ*** asupra securității produsului cu elemente digitale. ***Producătorii ar trebui să comunice ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la data la care iau cunoștință de incidentul semnificativ legat de produsul cu elemente digitale, mai multe detalii cu privire la incidentul semnificativ.*** Fără a aduce atingere obligațiilor de raportare a incidentelor

primească informații de la producătorii de produse cu elemente digitale care să le permită să evalueze securitatea acestor produse. Pentru a se asigura că utilizatorii pot reacționa rapid la incidentele care au un impact asupra securității produselor lor cu elemente digitale, producătorii ar trebui, de asemenea, să își informeze utilizatorii cu privire la orice astfel de incident și, după caz, cu privire la orice măsuri corective pe care utilizatorii le pot adopta pentru a atenua impactul incidentului, de exemplu prin publicarea informațiilor relevante pe site-urile lor sau, dacă producătorul poate să contacteze utilizatorii și dacă riscurile justifică acest lucru, prin contactarea directă a utilizatorilor.

prevăzute în Directiva [Directiva XXX/XXXX (NIS2)] pentru entitățile esențiale și importante, este esențial ca ENISA, punctele unice de contact desemnate de statele membre în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și autoritățile de supraveghere a pieței să primească informații de la producătorii de produse cu elemente digitale care să le permită să evalueze securitatea acestor produse. Pentru a se asigura că utilizatorii pot reacționa rapid la incidentele care au un impact ***semnificativ*** asupra securității produselor lor cu elemente digitale, producătorii ar trebui, de asemenea, să își informeze utilizatorii cu privire la orice astfel de incident***, după caz, și dacă este probabil să fie afectați negativ de acesta,*** și, după caz, cu privire ***la atenuarea riscurilor și*** la orice măsuri corective pe care utilizatorii le pot adopta pentru a atenua impactul incidentului ***semnificativ***, de exemplu prin publicarea informațiilor relevante pe site-urile lor sau, dacă producătorul poate să contacteze utilizatorii și dacă riscurile justifică acest lucru, prin contactarea directă a utilizatorilor. ***Fără a aduce atingere altor obligații, producătorii care identifică vulnerabilități într-o componentă integrată într-un produs cu elemente digitale, inclusiv într-o componentă liberă și cu sursă deschisă, ar trebui să raporteze vulnerabilitatea persoanei sau entității care menține componenta împreună cu măsura corectivă adoptată.***

Amendamentul 23

Propunere de regulament
Considerentul 37 a (nou)

Textul propus de Comisie	*Amendamentul*
	(37a) Potrivit Acordului OMC privind barierele tehnice în calea comerțului, atunci când este nevoie de reglementări

tehnice și există standarde internaționale relevante, membrii OMC ar trebui să folosească aceste standarde drept bază pentru propriile reglementări tehnice. Este important să se evite suprapunerea activităților între organizațiile de standardizare, întrucât standardele internaționale sunt menite să faciliteze armonizarea reglementărilor și standardelor tehnice naționale și regionale, reducând astfel barierele tehnice netarifare în calea comerțului. Deoarece securitatea cibernetică este o problemă globală, Uniunea ar trebui să se străduiască să asigure o aliniere maximă. Pentru a atinge acest obiectiv, solicitarea de standardizare pentru prezentul regulament, astfel cum este prevăzută la articolul 10 din Regulamentul (UE) nr. 1025/2012, ar trebui să vizeze reducerea obstacolelor în calea acceptării standardelor prin publicarea referințelor la acestea în Jurnalul Oficial al Uniunii Europene, în conformitate cu articolul 10 alineatul (6) din Regulamentul (UE) nr. 1025/2012.

Amendamentul 24

Propunere de regulament
Considerentul 37 b (nou)

Textul propus de Comisie	*Amendamentul*
	(37b) Ținând cont de domeniul amplu de aplicare al prezentului regulament, dezvoltarea la timp a unor standarde armonizate reprezintă o provocare semnificativă. Pentru a îmbunătăți securitatea produselor cu componente digitale pe piața Uniunii cât mai curând posibil, Comisia ar trebui împuternicită, pentru o perioadă limitată, să declare standardele internaționale existente pentru securitatea cibernetică a produselor ca îndeplinind cerințele prezentului regulament. Aceste standarde ar trebui publicate drept standarde care

oferă prezumția de conformitate.

Amendamentul 25

Propunere de regulament
Considerentul 38

Textul propus de Comisie	*Amendamentul*
(38) Pentru a facilita evaluarea conformității cu cerințele prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu standardele armonizate, care transpun cerințele esențiale ale prezentului regulament în specificații tehnice detaliate și care sunt adoptate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[29]. Regulamentul (UE) nr. 1025/2012 prevede o procedură pentru formularea de obiecții cu privire la standardele armonizate în cazul în care standardele respective nu îndeplinesc în totalitate cerințele prezentului regulament.	(38) Pentru a facilita evaluarea conformității cu cerințele prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu standardele armonizate, care transpun cerințele esențiale ale prezentului regulament în specificații tehnice detaliate și care sunt adoptate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[29]. Regulamentul (UE) nr. 1025/2012 prevede o procedură pentru formularea de obiecții cu privire la standardele armonizate în cazul în care standardele respective nu îndeplinesc în totalitate cerințele prezentului regulament. ***Procesul de standardizare ar trebui să asigure o reprezentare echilibrată a intereselor și participarea eficace a părților interesate din cadrul societății civile, inclusiv a organizațiilor de consumatori.***
[29] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).	[29] Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

Amendamentul 26

Propunere de regulament
Considerentul 41

Textul propus de Comisie	*Amendamentul*
(41) În cazul în care ***nu se adoptă standarde*** armonizate ***sau*** în ***cazul*** în ***care standardele armonizate*** nu ***abordează suficient cerințele esențiale ale prezentului regulament***, Comisia ar trebui să poată adopta specificații comune prin intermediul unor acte de punere în aplicare. Câteva motive pentru elaborarea unor astfel de specificații comune, în locul utilizării standardelor armonizate, ar putea fi refuzarea cererii de standardizare de către una dintre organizațiile europene de standardizare, întârzieri nejustificate în stabilirea standardelor armonizate adecvate sau nerespectarea de către standardele elaborate a cerințelor prezentului regulament sau a unei cereri din partea Comisiei. Pentru a facilita evaluarea conformității cu cerințele esențiale prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu specificațiile comune adoptate de Comisie în temeiul prezentului regulament în scopul exprimării specificațiilor tehnice detaliate ale cerințelor respective.	(41) În cazul în care ***nicio trimitere la standardele*** armonizate ***care acoperă cerințele prevăzute în anexa I nu a fost publicată*** în ***Jurnalul Oficial al Uniunii Europene*** în ***conformitate cu Regulamentul (UE) nr. 1025/2012 și*** nu ***se preconizează că o astfel de trimitere va fi publicată într-un termen rezonabil***, Comisia ar trebui să poată adopta specificații comune prin intermediul unor acte de punere în aplicare. Câteva motive pentru elaborarea unor astfel de specificații comune, în locul utilizării standardelor armonizate, ar putea fi refuzarea cererii de standardizare de către una dintre organizațiile europene de standardizare, întârzieri nejustificate în stabilirea standardelor armonizate adecvate sau nerespectarea de către standardele elaborate a cerințelor prezentului regulament sau a unei cereri din partea Comisiei. Pentru a facilita evaluarea conformității cu cerințele esențiale prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu specificațiile comune adoptate de Comisie în temeiul prezentului regulament în scopul exprimării specificațiilor tehnice detaliate ale cerințelor respective.

Amendamentul 27

Propunere de regulament
Considerentul 43

Textul propus de Comisie	*Amendamentul*
(43) Marcajul CE, ca indicație a conformității unui produs, este consecința	(43) Marcajul CE, ca indicație a conformității unui produs, este consecința

vizibilă a unui întreg proces care cuprinde evaluarea conformității în sens larg. Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului stabilește principiile generale care reglementează marcajul CE[30]. Prezentul regulament ar trebui să prevadă norme de reglementare a aplicării marcajului CE pe produsele cu elemente digitale. Marcajul CE ar trebui să fie singurul marcaj care garantează faptul că produsele cu elemente digitale sunt conforme cu cerințele prezentului regulament.	vizibilă a unui întreg proces care cuprinde evaluarea conformității în sens larg. Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului stabilește principiile generale care reglementează marcajul CE[30]. Prezentul regulament ar trebui să prevadă norme de reglementare a aplicării marcajului CE pe produsele cu elemente digitale. Marcajul CE ar trebui să fie singurul marcaj care garantează faptul că produsele cu elemente digitale sunt conforme cu cerințele prezentului regulament. ***Totuși, pe un produs cu elemente digitale finalizat parțial nu se aplică marcajul CE în temeiul prezentului regulament, fără a se aduce atingere dispozițiilor privind marcarea rezultate din alte acte legislative aplicabile ale Uniunii. Pentru produsele parțial finalizate cu elemente digitale, producătorii ar trebui să întocmească o declarație UE de încorporare.***
[30] Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).	[30] Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de supraveghere a pieței în ceea ce privește comercializarea produselor și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

Amendamentul 28

Propunere de regulament
Considerentul 45

Textul propus de Comisie	*Amendamentul*
(45) Ca regulă generală, evaluarea conformității produselor cu elemente digitale ar trebui să fie efectuată de producător pe propria răspundere, urmând procedura bazată pe modulul A din Decizia nr. 768/2008/CE. Producătorul ar trebui să păstreze flexibilitatea de a alege o procedură mai strictă de evaluare a conformității care să implice o parte terță.	(45) Ca regulă generală, ***cerințele pentru*** evaluarea conformității produselor cu elemente digitale ar trebui ***să se bazeze pe riscuri, iar în acest sens, în multe cazuri, evaluarea ar putea*** să fie efectuată de producător pe propria răspundere, urmând procedura bazată pe modulul A din Decizia nr. 768/2008/CE. Producătorul ar trebui să păstreze flexibilitatea de a alege o

În cazul în care produsul este clasificat ca produs critic din clasa I, este necesară o asigurare suplimentară pentru a demonstra conformitatea cu cerințele esențiale prevăzute în prezentul regulament. Producătorul ar trebui să aplice standardele armonizate***, specificațiile comune*** sau sistemele de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 care au fost identificate de Comisie într-un act de punere în aplicare, dacă dorește să efectueze evaluarea conformității pe propria răspundere (modulul A). În cazul în care nu aplică astfel de standarde armonizate***, specificații comune*** sau sisteme de certificare de securitate cibernetică, producătorul ar trebui să fie supus unei evaluări a conformității care implică o parte terță. Ținând seama de sarcina administrativă a producătorilor și de faptul că securitatea cibernetică joacă un rol important în etapa de proiectare și dezvoltare a produselor cu elemente digitale, fizice sau nu, procedurile de evaluare a conformității bazate pe modulele B+C sau, respectiv, pe modulul H din Decizia nr. 768/2008/CE au fost alese ca fiind cele mai adecvate pentru evaluarea conformității produselor critice cu elemente digitale în mod proporțional și eficace. Producătorul care efectuează evaluarea conformității de către terți poate alege procedura care se potrivește cel mai bine procesului său de proiectare și de producție. Având în vedere riscul și mai mare de securitate cibernetică legat de utilizarea produselor clasificate ca produse critice din clasa II, evaluarea conformității ar trebui să implice întotdeauna o parte terță.	procedură mai strictă de evaluare a conformității care să implice o parte terță. În cazul în care produsul este clasificat ca produs critic din clasa I, este necesară o asigurare suplimentară pentru a demonstra conformitatea cu cerințele esențiale prevăzute în prezentul regulament. Producătorul ar trebui să aplice standardele armonizate sau sistemele de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 care au fost identificate de Comisie într-un act de punere în aplicare, dacă dorește să efectueze evaluarea conformității pe propria răspundere (modulul A). În cazul în care nu aplică astfel de standarde armonizate sau sisteme de certificare de securitate cibernetică, producătorul ar trebui să fie supus unei evaluări a conformității care implică o parte terță. Ținând seama de sarcina administrativă a producătorilor și de faptul că securitatea cibernetică joacă un rol important în etapa de proiectare și dezvoltare a produselor cu elemente digitale, fizice sau nu, procedurile de evaluare a conformității bazate pe modulele B+C sau, respectiv, pe modulul H din Decizia nr. 768/2008/CE au fost alese ca fiind cele mai adecvate pentru evaluarea conformității produselor critice cu elemente digitale în mod proporțional și eficace. Producătorul care efectuează evaluarea conformității de către terți poate alege procedura care se potrivește cel mai bine procesului său de proiectare și de producție. Având în vedere riscul și mai mare de securitate cibernetică legat de utilizarea produselor clasificate ca produse critice din clasa II, evaluarea conformității ar trebui să implice întotdeauna o parte terță.

Amendamentul 29

Propunere de regulament
Considerentul 46 a (nou)

Textul propus de Comisie	*Amendamentul*
	(46a) Dacă produsele cu elemente digitale sunt echivalente, unul dintre aceste produse poate fi acceptat ca fiind reprezentativ pentru o familie sau o categorie de produse în scopul anumitor proceduri de evaluare a conformității.

Amendamentul 30

Propunere de regulament
Considerentul 55

Textul propus de Comisie	*Amendamentul*
(55) În conformitate cu Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru respectiv. Prezentul regulament nu ar trebui să împiedice statele membre să aleagă autoritățile competente pentru îndeplinirea sarcinilor respective. Fiecare stat membru ar trebui să desemneze una sau mai multe autorități de supraveghere a pieței pe teritoriul său. Statele membre pot alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile naționale competente menționate la articolul ***[articolul X]*** din ***Directiva [Directiva XXX/XXXX*** (NIS2)***]*** sau autoritățile naționale desemnate de certificare a securității cibernetice menționate la articolul 58 din Regulamentul (UE) 2019/881. Operatorii economici ar trebui să coopereze pe deplin cu autoritățile de supraveghere a pieței și cu alte autorități competente. Fiecare stat membru ar trebui să informeze Comisia și celelalte state membre cu privire la autoritățile sale de supraveghere a pieței și la domeniile de competență ale fiecăreia dintre aceste autorități și ar trebui să asigure resursele și competențele necesare pentru îndeplinirea	(55) În conformitate cu Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru respectiv. Prezentul regulament nu ar trebui să împiedice statele membre să aleagă autoritățile competente pentru îndeplinirea sarcinilor respective. Fiecare stat membru ar trebui să desemneze una sau mai multe autorități de supraveghere a pieței pe teritoriul său. Statele membre pot alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile naționale competente menționate la articolul ***8 din 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) sau autoritățile naționale desemnate de certificare a securității cibernetice menționate la articolul 58 din Regulamentul (UE) 2019/881. Operatorii economici ar trebui să coopereze pe deplin cu autoritățile de supraveghere a pieței și cu alte autorități competente. Fiecare stat

sarcinilor de supraveghere legate de prezentul regulament. În conformitate cu articolul 10 alineatele (2) și (3) din Regulamentul (UE) 2019/1020, fiecare stat membru ar trebui să numească un birou unic de legătură care ar trebui să fie responsabil, printre altele, de reprezentarea poziției coordonate a autorităților de supraveghere a pieței și de acordarea de asistență pentru cooperarea dintre autoritățile de supraveghere a pieței din diferite state membre.	membru ar trebui să informeze Comisia și celelalte state membre cu privire la autoritățile sale de supraveghere a pieței și la domeniile de competență ale fiecăreia dintre aceste autorități și ar trebui să asigure resursele și competențele necesare pentru îndeplinirea sarcinilor de supraveghere legate de prezentul regulament. În conformitate cu articolul 10 alineatele (2) și (3) din Regulamentul (UE) 2019/1020, fiecare stat membru ar trebui să numească un birou unic de legătură care ar trebui să fie responsabil, printre altele, de reprezentarea poziției coordonate a autorităților de supraveghere a pieței și de acordarea de asistență pentru cooperarea dintre autoritățile de supraveghere a pieței din diferite state membre.

Amendamentul 31

Propunere de regulament
Considerentul 56 a (nou)

Textul propus de Comisie	*Amendamentul*
	(56a) Pentru ca operatorii economici care sunt IMM-uri și microîntreprinderi să poată face față noilor obligații impuse de prezentul regulament, Comisia ar trebui să le ofere orientări și consiliere, de exemplu printr-un canal direct pentru a lua legătura cu experți în cazul în care au întrebări, ținând seama de necesitatea de a simplifica și limita sarcinile administrative. Atunci când elaborează aceste orientări, Comisia ar trebui să țină seama de nevoile IMM-urilor, astfel încât sarcinile administrative și financiare să fie menținute la un nivel minim, înlesnind în același timp respectarea prezentului regulament. Comisia ar trebui să consulte părțile interesate relevante care au cunoștințe de specialitate în domeniul securității cibernetice.

Amendamentul 32

Propunere de regulament
Considerentul 58

Textul propus de Comisie	*Amendamentul*
(58) În anumite cazuri, un produs cu elemente digitale care respectă prezentul regulament poate prezenta totuși un risc semnificativ în materie de securitate cibernetică sau poate prezenta un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin utilizarea unui sistem electronic de informații de către entitățile esențiale de tipul celor menționate în ***[anexa*** I la Directiva ***XXX/XXXX (***NIS2)***]*** sau în ceea ce privește alte aspecte ale protecției interesului public. Prin urmare, este necesar să se stabilească norme care să asigure atenuarea acestor riscuri. În consecință, autoritățile de supraveghere a pieței ar trebui să ia măsuri pentru a solicita operatorului economic să se asigure că produsul nu mai prezintă riscul respectiv, să îl recheme sau să îl retragă, în funcție de risc. De îndată ce o autoritate de supraveghere a pieței restricționează sau interzice libera circulație a unui produs în acest mod, statul membru în cauză ar trebui să informeze fără întârziere Comisia și celelalte state membre cu privire la măsurile provizorii, justificându-și și motivându-și decizia. Atunci când o autoritate de supraveghere a pieței adoptă astfel de măsuri în ceea ce privește produsele care prezintă un risc, Comisia ar trebui să inițieze fără întârziere consultări cu statele membre și cu operatorul economic sau operatorii economici în cauză și ar trebui să evalueze măsura națională. Pe baza rezultatelor acestei evaluări, Comisia ar trebui să decidă dacă măsura națională este sau nu justificată.	(58) În anumite cazuri, un produs cu elemente digitale care respectă prezentul regulament poate prezenta totuși un risc semnificativ în materie de securitate cibernetică sau poate prezenta un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin utilizarea unui sistem electronic de informații de către entitățile esențiale de tipul celor menționate în ***anexa*** I la Directiva ***(UE)/2022/2555(Directiva*** NIS2) sau în ceea ce privește alte aspecte ale protecției interesului public. Prin urmare, este necesar să se stabilească norme care să asigure atenuarea acestor riscuri. În consecință, autoritățile de supraveghere a pieței ar trebui să ia măsuri pentru a solicita operatorului economic să se asigure că produsul nu mai prezintă riscul respectiv, să îl recheme sau să îl retragă, în funcție de risc. De îndată ce o autoritate de supraveghere a pieței restricționează sau interzice libera circulație a unui produs în acest mod, statul membru în cauză ar trebui să informeze fără întârziere Comisia și celelalte state membre cu privire la măsurile provizorii, justificându-și și motivându-și decizia. Atunci când o autoritate de supraveghere a pieței adoptă astfel de măsuri în ceea ce privește produsele care prezintă un risc, Comisia ar trebui să inițieze fără întârziere consultări cu statele membre și cu operatorul economic sau operatorii economici în cauză și ar trebui să evalueze măsura națională. Pe baza rezultatelor acestei evaluări, Comisia ar trebui să decidă dacă măsura națională este sau nu justificată.

Comisia ar trebui să adreseze decizia sa tuturor statelor membre și să o comunice imediat acestora și operatorului (operatorilor) economic(i) în cauză. Dacă măsura este considerată justificată, Comisia poate avea în vedere, de asemenea, adoptarea unor propuneri de revizuire a legislației respective a Uniunii.	Comisia ar trebui să adreseze decizia sa tuturor statelor membre și să o comunice imediat acestora și operatorului (operatorilor) economic(i) în cauză. Dacă măsura este considerată justificată, Comisia poate avea în vedere, de asemenea, adoptarea unor propuneri de revizuire a legislației respective a Uniunii.

Amendamentul 33

Propunere de regulament
Considerentul 59

Textul propus de Comisie	*Amendamentul*
(59) În cazul produselor cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică și dacă există motive să se creadă că acestea nu sunt conforme cu prezentul regulament sau în cazul produselor care sunt conforme cu prezentul regulament, dar care prezintă alte riscuri importante, precum riscuri la adresa sănătății sau siguranței persoanelor, a drepturilor fundamentale sau a furnizării de servicii de către entități esențiale de tipul celor menționate în ***[***anexa I la Directiva ***XXX/XXXX*** (NIS2)***]***, Comisia poate solicita ENISA să efectueze o evaluare. Pe baza evaluării respective, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea produselor respective, într-un termen rezonabil, proporțional cu natura riscului. Comisia poate recurge la o astfel de intervenție numai în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne și numai în cazul în care autoritățile de supraveghere nu au luat măsuri eficace pentru remedierea situației. Astfel de circumstanțe excepționale pot fi situații de urgență în care, de exemplu, un produs neconform este pus la dispoziție pe scară largă de către	(59) În cazul produselor cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică și dacă există motive să se creadă că acestea nu sunt conforme cu prezentul regulament sau în cazul produselor care sunt conforme cu prezentul regulament, dar care prezintă alte riscuri importante, precum riscuri la adresa sănătății sau siguranței persoanelor, a drepturilor fundamentale sau a furnizării de servicii de către entități esențiale de tipul celor menționate în anexa I la Directiva ***(UE)/2022/2555*** (***Directiva*** NIS2), Comisia poate solicita ENISA să efectueze o evaluare. Pe baza evaluării respective, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea produselor respective, într-un termen rezonabil, proporțional cu natura riscului. Comisia poate recurge la o astfel de intervenție numai în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne și numai în cazul în care autoritățile de supraveghere nu au luat măsuri eficace pentru remedierea situației. Astfel de circumstanțe excepționale pot fi situații de urgență în care, de exemplu, un produs neconform este pus la dispoziție pe scară largă de către

producător în mai multe state membre, este utilizat și în sectoare-cheie de către entități care intră în domeniul de aplicare al ***[***Directivei ***XXX/XXXX*** (NIS2)***]***, acesta conținând vulnerabilități cunoscute care sunt exploatate de actori răuintenționați și pentru care producătorul nu oferă corecții disponibile. Comisia poate interveni în astfel de situații de urgență numai pe durata circumstanțelor excepționale și dacă neconformitatea cu prezentul regulament sau riscurile importante prezentate persistă.

producător în mai multe state membre, este utilizat și în sectoare-cheie de către entități care intră în domeniul de aplicare al Directivei ***(UE)/2022/2555*** (***Directiva*** NIS2), acesta conținând vulnerabilități cunoscute care sunt exploatate de actori răuintenționați și pentru care producătorul nu oferă corecții disponibile. Comisia poate interveni în astfel de situații de urgență numai pe durata circumstanțelor excepționale și dacă neconformitatea cu prezentul regulament sau riscurile importante prezentate persistă.

Amendamentul 34

Propunere de regulament
Considerentul 62

Textul propus de Comisie	*Amendamentul*
(62) Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul 290 din tratat pentru a actualiza lista produselor critice din anexa III și pentru a preciza definițiile acestor categorii de produse. Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv pentru a identifica produsele cu elemente digitale care fac obiectul altor norme ale Uniunii care asigură același nivel de protecție ca prezentul regulament, specificând dacă va fi necesară o limitare sau o excludere din domeniul de aplicare al prezentului regulament, precum și domeniul de aplicare al limitării respective, dacă este cazul. De asemenea, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv în ceea ce privește eventuala ***impunere a certificării*** anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor referitoare la caracterul critic prevăzute în prezentul regulament, precum și în ceea ce privește precizarea	(62) Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul 290 din tratat pentru a actualiza lista produselor critice din anexa III și pentru a preciza definițiile acestor categorii de produse. Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv pentru a identifica produsele cu elemente digitale care fac obiectul altor norme ale Uniunii care asigură același nivel de protecție ca prezentul regulament, specificând dacă va fi necesară o limitare sau o excludere din domeniul de aplicare al prezentului regulament, precum și domeniul de aplicare al limitării respective, dacă este cazul. De asemenea, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv în ceea ce privește eventuala ***certificare voluntară a*** anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor referitoare la caracterul critic prevăzute în prezentul regulament, precum și în ceea ce privește precizarea

conținutului minim al declarației de conformitate UE și completarea elementelor care trebuie incluse în documentația tehnică. Este deosebit de important ca, în cursul activității sale pregătitoare, Comisia să organizeze consultări corespunzătoare, inclusiv la nivel de experți, și ca aceste consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016[33]. 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.

[33] JO L 123, 12.5.2016, p. 1.

conținutului minim al declarației de conformitate UE și completarea elementelor care trebuie incluse în documentația tehnică. Este deosebit de important ca, în cursul activității sale pregătitoare, Comisia să organizeze consultări corespunzătoare, inclusiv la nivel de experți, și ca aceste consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016[33]. 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.

[33] JO L 123, 12.5.2016, p. 1.

Amendamentul 35

Propunere de regulament
Considerentul 63

Textul propus de Comisie	*Amendamentul*
(63) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să îi fie conferite competențe de executare: pentru a preciza formatul și elementele listei materialelor software, pentru a preciza mai detaliat tipul de informații, formatul și procedura notificărilor privind vulnerabilitățile exploatate activ și incidentele transmise către ENISA de către producători, pentru a preciza sistemele europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu anumite părți ale acestora, astfel cum sunt prevăzute în	(63) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să îi fie conferite competențe de executare: pentru a preciza formatul și elementele listei materialelor software, pentru a preciza mai detaliat tipul de informații, formatul și procedura notificărilor privind vulnerabilitățile exploatate activ și incidentele transmise către ENISA de către producători, ***pe baza celor mai bune practici de la nivelul industriei,*** pentru a preciza sistemele europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu anumite părți

anexa I la prezentul regulament, pentru a adopta specificații comune cu privire la cerințele esențiale prevăzute în anexa I, pentru a stabili specificații tehnice pentru pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale și mecanisme de promovare a utilizării acestora, pentru a decide măsuri corective sau restrictive la nivelul Uniunii în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne. Aceste competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[34].	ale acestora, astfel cum sunt prevăzute în anexa I la prezentul regulament, pentru a adopta specificații comune cu privire la cerințele esențiale prevăzute în anexa I, pentru a stabili specificații tehnice pentru pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale și mecanisme de promovare a utilizării acestora, pentru a decide măsuri corective sau restrictive la nivelul Uniunii în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne. Aceste competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[34].
[34] Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).	[34] Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

Amendamentul 36

Propunere de regulament
Considerentul 69

Textul propus de Comisie	*Amendamentul*
(69) Operatorilor economici ar trebui să li se acorde suficient timp pentru a se adapta la cerințele prevăzute de prezentul regulament. Prezentul regulament ar trebui să se aplice la [***24 de*** luni] de la intrarea sa în vigoare***, cu excepția obligațiilor de raportare privind vulnerabilitățile exploatate activ și incidentele, care ar trebui să se aplice la [12 luni] de la intrarea în vigoare a regulamentului***.	(69) Operatorilor economici ar trebui să li se acorde suficient timp pentru a se adapta la cerințele prevăzute de prezentul regulament. Prezentul regulament ar trebui să se aplice la [***36 de*** luni] de la intrarea sa în vigoare.

Amendamentul 37

Propunere de regulament
Articolul 1 – paragraful 1 – partea introductivă

Textul propus de Comisie	*Amendamentul*
Prezentul regulament stabilește:	***Obiectivul prezentului regulament este îmbunătățirea funcționării pieței interne, asigurând în același timp un nivel înalt de protecție a consumatorilor și de securitate cibernetică.*** Prezentul regulament stabilește ***norme armonizate privind***:

Amendamentul 38

Propunere de regulament
Articolul 1 – paragraful 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) ***norme pentru*** introducerea pe piață a produselor cu elemente digitale în vederea asigurării securității cibernetice a acestor produse;	(a) introducerea pe piață a produselor cu elemente digitale în vederea asigurării securității cibernetice a acestor produse;

Amendamentul 39

Propunere de regulament
Articolul 1 – paragraful 1 – litera d

Textul propus de Comisie	*Amendamentul*
(d) ***norme privind*** supravegherea pieței și asigurarea respectării normelor și cerințelor menționate mai sus.	(d) supravegherea pieței și asigurarea respectării normelor și cerințelor menționate mai sus.

Amendamentul 40

Propunere de regulament
Articolul 2 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Prezentul regulament se aplică	1. Prezentul regulament se aplică

produselor cu elemente digitale a căror utilizare preconizată sau previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv sau la o rețea.	produselor cu elemente digitale ***introduse pe piață*** a căror utilizare preconizată sau previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv ***extern*** sau la o rețea ***externă***.

Amendamentul 41

Propunere de regulament
Articolul 2 – alineatul 5 a (nou)

Textul propus de Comisie	*Amendamentul*
	5a. Prezentul regulament nu se aplică programelor software gratuite și cu sursă deschisă, inclusiv codului sursă și versiunilor modificate, cu excepția cazului în care software-ul este furnizat în cursul activității comerciale, fie:
	(i) percepând un preț pentru un produs;
	(ii) oferind o platformă software care se bazează pe alte servicii pe care producătorul le monetizează;
	(iii) utilizând date cu caracter personal generate de software din alte motive decât exclusiv pentru îmbunătățirea securității, compatibilității sau interoperabilității software-ului;
	(iv) percepând un preț pentru serviciile de asistență tehnică.
	Conformitatea componentelor libere și cu sursă deschisă ale produselor este asigurată de fabricantul produsului în care acestea sunt incluse.

Amendamentul 42

Propunere de regulament
Articolul 2 – paragraful 5 b (nou)

Textul propus de Comisie	*Amendamentul*
	5b. Prezentul regulament nu se aplică rețelelor interne ale unui produs cu

	elemente digitale, dacă aceste rețele au puncte terminale dedicate și sunt complet izolate și protejate față de conexiunile de date externe.

Amendamentul 43

Propunere de regulament
Articolul 2 – alineatul 5 c (nou)

Textul propus de Comisie	*Amendamentul*
	5c. Prezentul regulament nu se aplică în cazul pieselor de schimb destinate exclusiv înlocuirii componentelor defecte ale produselor cu elemente digitale, pentru a le restabili funcționalitatea.

Amendamentul 44

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 1

Textul propus de Comisie	*Amendamentul*
(1) „produs cu elemente digitale” înseamnă orice produs software sau hardware ***și soluțiile sale de prelucrare de date la distanță***, inclusiv componentele software sau hardware care urmează să fie introduse pe piață separat;	(1) „produs cu elemente digitale” înseamnă orice produs software sau hardware, inclusiv componentele software sau hardware care urmează să fie introduse pe piață separat;

Amendamentul 45

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
(2) „prelucrare de date la distanță” înseamnă orice prelucrare de date la distanță pentru care software-ul este proiectat și dezvoltat de producător sau sub responsabilitatea producătorului și a cărei absență ar împiedica produsul cu elemente digitale să își îndeplinească	***eliminat***

vreuna dintre funcții;

Amendamentul 46

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	(6a) „software cu sursă deschisă” înseamnă un software distribuit în baza unei licențe care le permite utilizatorilor rularea, copierea, distribuția, studierea, modificarea și îmbunătățirea acestuia în mod liber, precum și integrarea sa drept componentă în alte produse, furnizarea sa ca serviciu sau furnizarea de asistență comercială pentru el;

Amendamentul 47

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 18

Textul propus de Comisie	*Amendamentul*
(18) „producător” înseamnă orice persoană fizică sau juridică care dezvoltă sau fabrică produse cu elemente digitale sau pentru care sunt proiectate, dezvoltate sau fabricate produsele cu elemente digitale și care le comercializează sub numele sau marca sa, contra cost sau gratuit;	*(Nu privește versiunea în limba română.)*

Amendamentul 48

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 19

Textul propus de Comisie	*Amendamentul*
(19) „reprezentant autorizat” înseamnă orice persoană fizică sau juridică stabilită în Uniune care a primit un mandat scris din partea unui producător pentru a acționa în	(19) „reprezentant autorizat” înseamnă orice persoană fizică sau juridică stabilită în Uniune**,** care a primit un mandat scris din partea unui producător pentru a acționa

numele acestuia în legătură cu sarcini specifice;	în numele acestuia în legătură cu sarcini specifice ***legate de obligațiile producătorului***;

Amendamentul 49

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 23 a (nou)

Textul propus de Comisie	*Amendamentul*
	(23a) „rechemare” înseamnă o rechemare astfel cum este definită la articolul 3 punctul 22 din Regulamentul (UE) 2019/1020;

Amendamentul 50

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 26

Textul propus de Comisie	*Amendamentul*
(26) „utilizare necorespunzătoare previzibilă în mod rezonabil” înseamnă utilizarea unui produs cu elemente digitale într-un mod care nu este conform cu scopul său preconizat, dar care poate rezulta din comportamentul uman sau interacțiunea previzibilă în mod rezonabil cu alte sisteme;	***eliminat***

Amendamentul 51

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 31

Textul propus de Comisie	*Amendamentul*
(31) „modificare substanțială” înseamnă o modificare a produsului cu elemente digitale în urma introducerii sale pe piață care afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 sau care are ca rezultat o modificare a utilizării	(31) „modificare substanțială” înseamnă o modificare a produsului cu elemente digitale***, cu excepția actualizărilor de securitate și de întreținere,*** în urma introducerii sale pe piață care afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în

preconizate pentru care a fost evaluat respectivul produs cu elemente digitale;	anexa I secțiunea 1 sau care are ca rezultat o modificare a utilizării preconizate pentru care a fost evaluat respectivul produs cu elemente digitale;

Amendamentul 52

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 39

Textul propus de Comisie	*Amendamentul*
(39) „vulnerabilitate exploatată activ” înseamnă o vulnerabilitate pentru care există dovezi fiabile că executarea unui cod dăunător a fost efectuată de un actor pe un sistem fără permisiunea proprietarului sistemului;	(39) „vulnerabilitate exploatată activ” înseamnă o vulnerabilitate ***remediată*** pentru care există dovezi fiabile că executarea unui cod dăunător a fost efectuată de un actor pe un sistem fără permisiunea proprietarului sistemului;

Amendamentul 53

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 40 a (nou)

Textul propus de Comisie	*Amendamentul*
	(40a) „produs cu elemente digitale finalizat parțial” înseamnă un element tangibil care nu poate funcționa în mod independent și care este produs doar pentru a fi integrat într-un produs cu elemente digitale sau în alt produs cu elemente digitale finalizat parțial sau să fie asamblat cu acesta și a cărui conformitate poate fi evaluată în mod eficace doar ținând cont de modul în care este integrat într-un produs finit proiectat, cu elemente digitale;

Amendamentul 54

Propunere de regulament
Articolul 3 – paragraful 1 – punctul 40 b (nou)

Textul propus de Comisie	*Amendamentul*
	(40b) „ciclu de viață” înseamnă perioada cuprinsă între momentul în care produsul vizat de prezentul regulament este introdus pe piață sau pus în funcțiune și momentul în care acesta este eliminat, inclusiv timpul efectiv în care poate fi utilizat și fazele de transport, asamblare, dezasamblare, demontare, casare sau alte modificări fizice ori digitale prevăzute de producător.

Amendamentul 55

Propunere de regulament
Articolul 4 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre nu împiedică, în ceea ce privește aspectele reglementate de prezentul regulament, punerea la dispoziție pe piață a produselor cu elemente digitale care sunt conforme cu prezentul regulament.	1. Statele membre nu împiedică, în ceea ce privește aspectele reglementate de prezentul regulament, punerea la dispoziție pe piață a produselor cu elemente digitale ***sau a produselor cu elemente digitale finalizate parțial,*** care sunt conforme cu prezentul regulament.

Amendamentul 56

Propunere de regulament
Articolul 4 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. La târguri comerciale, expoziții și demonstrații sau evenimente similare, statele membre nu împiedică prezentarea și utilizarea unui produs cu elemente digitale care nu este conform cu prezentul regulament.	2. La târguri comerciale, expoziții și demonstrații sau evenimente similare, statele membre nu împiedică prezentarea și utilizarea unui produs cu elemente digitale***, a unui prototip de produs cu elemente digitale sau a unui produs parțial finalizat cu elemente digitale*** care nu este conform cu prezentul regulament***, cu condiția ca produsul cu elemente digitale să fie utilizat exclusiv în scopuri de prezentare în cursul evenimentului și ca un semn***

	vizibil să indice în mod clar neconformitatea acestuia cu prezentul regulament.

Amendamentul 57

Propunere de regulament
Articolul 4 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Statele membre nu împiedică punerea la dispoziție a unui ***software*** nefinalizat care nu este conform cu prezentul regulament, cu condiția ca ***software-ul respectiv*** să fie pus la dispoziție numai ***pentru o perioadă limitată necesară*** pentru testare și să se indice în mod clar printr-un un semn vizibil că acesta nu este conform cu prezentul regulament și nu va fi disponibil pe piață în alte scopuri decât testarea.	3. Statele membre nu împiedică punerea la dispoziție a unui ***produs*** nefinalizat ***cu elemente digitale sau a unui prototip de produs cu elemente digitale*** care nu este conform cu prezentul regulament, cu condiția ca ***el*** să fie pus la dispoziție numai ***într-o versiune care nu este destinată producției*** pentru testare și să se indice în mod clar printr-un un semn vizibil că acesta nu este conform cu prezentul regulament și nu va fi disponibil pe piață în alte scopuri decât testarea.

Amendamentul 58

Propunere de regulament
Articolul 4 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. Prezentul regulament nu împiedică statele membre să supună produsele cu elemente digitale unor măsuri suplimentare atunci când aceste produse specifice vor fi utilizate în scopuri militare, de apărare sau de securitate națională, în conformitate cu dreptul intern sau cu dreptul Uniunii, iar aceste măsuri sunt necesare și proporționale pentru realizarea acestor scopuri.

Amendamentul 59

Propunere de regulament
Articolul 5 – paragraful 1 – punctul 1

Textul propus de Comisie	*Amendamentul*
(1) îndeplinesc cerințele esențiale prevăzute în anexa I secțiunea 1, cu condiția să fie instalate, întreținute, utilizate în mod corespunzător pentru scopul preconizat sau în condiții care pot fi prevăzute în mod rezonabil și, după caz, ***actualizate*** și	(1) îndeplinesc cerințele esențiale prevăzute în anexa I secțiunea 1, cu condiția să fie instalate, întreținute, utilizate în mod corespunzător pentru scopul preconizat sau în condiții care pot fi prevăzute în mod rezonabil și, după caz, ***cu actualizările de securitate necesare*** și

Amendamentul 60

Propunere de regulament
Articolul 6 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Produsele cu elemente digitale care aparțin unei categorii enumerate în anexa III sunt considerate produse critice cu elemente digitale. Produsele care au funcționalitatea de bază a unei categorii enumerate în anexa III la prezentul regulament trebuie considerate ca făcând parte din categoria respectivă. Categoriile de produse critice cu elemente digitale se împart în clasele I și II, astfel cum sunt prevăzute în anexa III, în funcție de nivelul riscului de securitate cibernetică aferent acestor produse.	1. Produsele cu elemente digitale care aparțin unei categorii enumerate în anexa III sunt considerate produse critice cu elemente digitale. ***Doar*** produsele care au funcționalitatea de bază a unei categorii enumerate în anexa III la prezentul regulament trebuie considerate ca făcând parte din categoria respectivă. Categoriile de produse critice cu elemente digitale se împart în clasele I și II, astfel cum sunt prevăzute în anexa III, în funcție de nivelul riscului de securitate cibernetică aferent acestor produse. ***Integrarea unei componente cu o clasă critică superioară într-un produs cu o importanță critică mai scăzută nu modifică neapărat nivelul critic pentru produsul în care este integrată componenta.***

Amendamentul 61

Propunere de regulament
Articolul 6 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) utilizarea preconizată în ***medii sensibile, inclusiv în*** medii ***industriale*** sau de către entități esențiale de tipul celor	(b) utilizarea preconizată în ***aplicații critice în cadrul unor*** medii ***sensibile*** sau de către entități esențiale de tipul celor

menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)];	menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)];

Amendamentul 62

Propunere de regulament
Articolul 6 – alineatul 2 – litera c

Textul propus de Comisie	*Amendamentul*
(c) utilizarea preconizată ***constând în îndeplinirea*** unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal;	(c) utilizarea preconizată ***și amploarea îndeplinirii*** unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal;

Amendamentul 63

Propunere de regulament
Articolul 6 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Produsele critice cu elemente digitale fac obiectul procedurilor de evaluare a conformității menționate la articolul 24 alineatele (2) și (3).	4. Produsele critice cu elemente digitale fac obiectul procedurilor de evaluare a conformității menționate la articolul 24 alineatele (2) și (3). ***Ca excepție, întreprinderile mici și microîntreprinderile pot utiliza procedura menționată la articolul 24 alineatul (2).***

Amendamentul 64

Propunere de regulament
Articolul 6 – alineatul 5 – partea introductivă

Textul propus de Comisie	*Amendamentul*
5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea categoriilor de produse deosebit de critice cu elemente digitale, pentru care producătorii ***au obligația de a*** obține un certificat european de securitate cibernetică în cadrul unui sistem european de certificare de securitate	5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea categoriilor de produse deosebit de critice cu elemente digitale, pentru care producătorii ***pot*** obține un certificat european de securitate cibernetică în cadrul unui sistem european de certificare de securitate cibernetică în

cibernetică în temeiul Regulamentului (UE) 2019/881 pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I sau cu anumite părți ale acestora. Atunci când stabilește aceste categorii de produse deosebit de critice cu elemente digitale, Comisia ține seama de nivelul de risc de securitate cibernetică aferent categoriei respective de produse cu elemente digitale, având în vedere unul sau mai multe dintre criteriile enumerate la alineatul (2), precum și evaluând dacă respectiva categorie de produse:

temeiul Regulamentului (UE) 2019/881 pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I sau cu anumite părți ale acestora. Atunci când stabilește aceste categorii de produse deosebit de critice cu elemente digitale, Comisia ține seama de nivelul de risc de securitate cibernetică aferent categoriei respective de produse cu elemente digitale, având în vedere unul sau mai multe dintre criteriile enumerate la alineatul (2), precum și evaluând dacă respectiva categorie de produse:

Amendamentul 65

Propunere de regulament
Articolul 8 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Produsele cu elemente digitale clasificate drept sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament și care îndeplinesc cerințele esențiale prevăzute în secțiunea 1 din anexa I la prezentul regulament sunt considerate, în cazul în care procesele instituite de producător respectă cerințele esențiale prevăzute în secțiunea 2 din anexa I, conforme cu cerințele legate de securitatea cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], fără a aduce atingere celorlalte cerințe legate de acuratețe și robustețe incluse la articolul menționat anterior și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate a UE emisă în temeiul prezentului regulament.	1. Produsele cu elemente digitale ***sau produsele cu elemente digitale finalizate parțial*** clasificate drept sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament și care îndeplinesc cerințele esențiale prevăzute în secțiunea 1 din anexa I la prezentul regulament sunt considerate, în cazul în care procesele instituite de producător respectă cerințele esențiale prevăzute în secțiunea 2 din anexa I, conforme cu cerințele legate de securitatea cibernetică prevăzute la articolul [articolul 15] din Regulamentul [Regulamentul privind inteligența artificială], fără a aduce atingere celorlalte cerințe legate de acuratețe și robustețe incluse la articolul menționat anterior și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate a UE emisă în temeiul prezentului regulament.

Amendamentul 66

Propunere de regulament
Articolul 8 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Pentru produsele și cerințele de securitate cibernetică menționate la alineatul (1), se aplică procedura relevantă de evaluare a conformității, astfel cum este prevăzută ***la articolul [articolul 43]*** din Regulamentul [Regulamentul privind inteligența artificială]. În scopul efectuării acestei evaluări, organismele notificate care au dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc în temeiul Regulamentului [Regulamentul privind inteligența artificială] au, de asemenea, dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în anexa I la prezentul regulament***, cu condiția ca respectarea de către organismele notificate respective a cerințelor prevăzute la articolul 29 din prezentul regulament să fi fost evaluată în contextul procedurii de notificare în temeiul Regulamentului [Regulamentul privind inteligența artificială]***.	2. Pentru produsele și cerințele de securitate cibernetică menționate la alineatul (1), se aplică procedura relevantă de evaluare a conformității, astfel cum este prevăzută ***în [dispozițiile aplicabile]*** din Regulamentul [Regulamentul privind inteligența artificială]. În scopul efectuării acestei evaluări, organismele notificate care au dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc în temeiul Regulamentului [Regulamentul privind inteligența artificială] au, de asemenea, dreptul să verifice conformitatea sistemelor de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în anexa I la prezentul regulament.

Amendamentul 67

Propunere de regulament
Articolul 8 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Prin derogare de la alineatul (2), produsele critice cu elemente digitale enumerate în anexa III la prezentul regulament, care trebuie să aplice procedurile de evaluare a conformității menționate la articolul 24 alineatul (2) litera (a), la articolul 24 alineatul (2) litera (b) și la articolul 24 alineatul (3) literele (a) și (b) în temeiul prezentului	***eliminat***

regulament, care sunt clasificate, de asemenea, ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul [articolul 6] din Regulamentul [Regulamentul privind inteligența artificială] și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa [anexa VI] la Regulamentul [Regulamentul privind inteligența artificială] fac obiectul procedurilor de evaluare a conformității prevăzute de prezentul regulament în ceea ce privește cerințele esențiale ale prezentului regulament.

Amendamentul 68

Propunere de regulament
Articolul 9 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului [Propunerea de regulament privind produsele asimilate mașinilor] care sunt produse cu elemente digitale în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate UE pe baza prezentului regulament sunt considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în anexa [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul [Propunerea de regulament privind produsele asimilate mașinilor] în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.	Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului [Propunerea de regulament privind produsele asimilate mașinilor] care sunt produse cu elemente digitale ***sau produse cu elemente digitale finalizate parțial*** în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate UE pe baza prezentului regulament sunt considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în anexa [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul [Propunerea de regulament privind produsele asimilate mașinilor] în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.

Amendamentul 69

Propunere de regulament
Articolul 10 – alineatul -1 (nou)

Textul propus de Comisie	*Amendamentul*
	-1. Producătorii de software care se califică drept microîntreprinderi, astfel cum sunt definite în Recomandarea 2003/361/CE a Comisiei, depun toate eforturile pentru a respecta cerințele prezentului regulament în cele șase luni de la introducerea pe piață a unui software. Această dispoziție nu se aplică produselor extrem de critice cu elemente digitale.

Amendamentul 70

Propunere de regulament
Articolul 10 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Atunci când introduc pe piață un produs cu elemente digitale, producătorii se asigură că acesta a fost proiectat, dezvoltat și ***produs*** în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 1.	1. Atunci când introduc pe piață un produs cu elemente digitale, producătorii se asigură că acesta a fost proiectat, dezvoltat și ***fabricat*** în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 1.

Amendamentul 71

Propunere de regulament
Articolul 10 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. În scopul respectării obligației prevăzute la alineatul (1), producătorii exercită diligența necesară atunci când integrează în produsele cu elemente digitale componente obținute de la terți. ***Aceștia*** se ***asigură*** că respectivele componente nu compromit securitatea produsului cu elemente digitale.	4. În scopul respectării obligației prevăzute la alineatul (1), producătorii exercită diligența necesară atunci când integrează în produsele cu elemente digitale componente obținute de la terți. ***Responsabilitatea de a*** se ***asigura*** că respectivele componente nu compromit securitatea produsului cu elemente digitale ***le revine producătorilor***.

Amendamentul 72

Propunere de regulament
Articolul 10 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. Producătorii de componente furnizează informațiile și documentația necesare pentru a se conforma cerințelor prezentului regulament, atunci când furnizează astfel de componente producătorului de produse finite. Aceste informații sunt puse la dispoziție gratuit.

Amendamentul 73

Propunere de regulament
Articolul 10 – alineatul 6 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Atunci când introduc pe piață un produs cu elemente digitale și pe durata de viață preconizată a produsului sau pentru o perioadă de cinci ani de la introducerea produsului pe piață, oricare dintre acestea este mai ***scurtă***, producătorii se asigură că vulnerabilitățile produsului respectiv sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 2.	Atunci când introduc pe piață un produs cu elemente digitale și pe durata de viață preconizată a produsului ***la momentul introducerii pe piață a produsului respectiv*** sau pentru o perioadă de cinci ani de la introducerea produsului pe piață, oricare dintre acestea este mai ***lungă***, producătorii se asigură că vulnerabilitățile produsului respectiv sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 2***, cu condiția ca producătorul să aibă control asupra acestui lucru***.

Amendamentul 74

Propunere de regulament
Articolul 10 – alineatul 7 – paragraful 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	În cazul în care sunt implementate actualizări de software, producătorul nu

	este obligat să efectueze o altă evaluare a conformității produsului cu elemente digitale, cu excepția cazului în care actualizarea software-ului duce la o modificare substanțială a produsului cu elemente digitale în sensul articolului 3 alineatul (31) din prezentul regulament.

Amendamentul 75

Propunere de regulament
Articolul 10 – alineatul 9

Textul propus de Comisie	*Amendamentul*
9. Producătorii se asigură că există proceduri care să garanteze conformitatea continuă a produselor cu elemente digitale care fac parte dintr-o producție în serie. Producătorul ține seama în mod adecvat de modificările survenite în procesul de dezvoltare și de producție sau în proiectarea ori caracteristicile produsului cu elemente digitale și de modificările standardelor armonizate, ale sistemelor europene de certificare de securitate cibernetică sau ale specificațiilor comune menționate la articolul 19 în raport cu care se declară conformitatea produsului cu elemente digitale sau prin aplicarea cărora este verificată conformitatea acestuia.	9. Producătorii se asigură că există proceduri care să garanteze conformitatea continuă a produselor cu elemente digitale care fac parte dintr-o producție în serie. Producătorul ține seama în mod adecvat de modificările survenite în procesul de dezvoltare și de producție sau în proiectarea ori caracteristicile produsului cu elemente digitale și de modificările standardelor armonizate, ale sistemelor europene de certificare de securitate cibernetică sau ale specificațiilor comune menționate la articolul 19 în raport cu care se declară conformitatea produsului cu elemente digitale sau prin aplicarea cărora este verificată conformitatea acestuia. ***Atunci când devin disponibile noi cunoștințe, tehnici sau standarde care nu erau disponibile la momentul proiectării unui produs în serie, producătorul poate lua în considerare punerea în aplicare a unor astfel de îmbunătățiri în mod periodic pentru viitoarele generații ale produsului.***

Amendamentul 76

Propunere de regulament
Articolul 10 – alineatul 9 a (nou)

Textul propus de Comisie	*Amendamentul*
	9a. Producătorii comunică public durata de viață preconizată a produselor lor într-o manieră clară și inteligibilă.

Amendamentul 77

Propunere de regulament
Articolul 10 – alineatul 12

Textul propus de Comisie	*Amendamentul*
12. De la introducerea pe piață și pentru durata de viață preconizată a produsului sau pentru o perioadă de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai ***scurtă***, producătorii care știu sau au motive să creadă că produsul cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor producătorului, pentru a retrage sau a rechema produsul, după caz.	12. De la introducerea pe piață și pentru durata de viață preconizată a produsului sau pentru o perioadă de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai ***lungă***, producătorii care știu sau au motive să creadă că produsul cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor producătorului, pentru a retrage sau a rechema produsul, după caz.

Amendamentul 78

Propunere de regulament
Articolul 11 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de ***24*** de ore de la momentul la care a luat cunoștință de aceasta, cu privire la orice vulnerabilitate exploatată activ conținută în produsul cu elemente digitale. ***Notificarea include detalii privind vulnerabilitatea respectivă și, după caz, eventualele măsuri corective sau de atenuare adoptate. ENISA transmite***	1. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de ***48*** de ore de la momentul la care a luat cunoștință de aceasta, ***printr-o avertizare timpurie,*** cu privire la orice vulnerabilitate exploatată activ conținută în produsul cu elemente digitale.

notificarea, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, către CSIRT desemnată în scopul divulgării coordonate a vulnerabilităților în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre în cauză la primirea notificării și informează autoritatea de supraveghere a pieței cu privire la vulnerabilitatea notificată.

Amendamentul 79

Propunere de regulament
Articolul 11 – alineatul 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	1a. Producătorul comunică ENISA, fără întârzieri nejustificate, din momentul în care a luat cunoștință de vulnerabilitatea exploatată în mod activ care are un impact semnificativ asupra securității produsului cu elemente digitale, mai multe detalii cu privire la vulnerabilitatea exploatată.

Amendamentul 80

Propunere de regulament
Articolul 11 – alineatul 1 b (nou)

Textul propus de Comisie	*Amendamentul*
	1b. Toate celelalte vulnerabilități care nu au un impact semnificativ asupra securității produsului cu elemente digitale se notifică ENISA odată ce vulnerabilitatea a fost abordată.

Amendamentul 81

Propunere de regulament
Articolul 11 – alineatul 1 c (nou)

Textul propus de Comisie	*Amendamentul*
	1c. Notificarea include detalii privind vulnerabilitatea respectivă și, după caz, eventualele măsuri corective sau de atenuare adoptate și măsurile recomandate pentru atenuarea riscurilor. ENISA transmite notificarea, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, către CSIRT desemnată în scopul divulgării coordonate a vulnerabilităților în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre în cauză la primirea notificării și informează imediat autoritatea de supraveghere a pieței cu privire la existența unei vulnerabilități și, după caz, cu privire la potențialele măsuri de atenuare a riscurilor. În cazul în care o vulnerabilitate notificată nu dispune de măsuri corective sau de atenuare, ENISA se asigură că informațiile cu privire la vulnerabilitatea notificată sunt partajate în conformitate cu protocoale stricte de securitate și pe baza principiului necesității de a cunoaște.

Amendamentul 82

Propunere de regulament
Articolul 11 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la momentul la care a luat cunoștință de acesta, orice incident care afectează securitatea produsului cu elemente digitale. ENISA transmite notificările, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, punctului unic de contact desemnat în conformitate cu articolul	2. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la momentul la care a luat cunoștință de acesta, ***printr-o avertizare timpurie,*** orice incident care afectează ***semnificativ*** securitatea produsului cu elemente digitale. ***Producătorul comunică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la data la care ia cunoștință de incidentul semnificativ legat***

[articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre în cauză și informează autoritatea de supraveghere a pieței cu privire la incidentele notificate. Notificarea incidentului include informații privind gravitatea și impactul incidentului și, după caz, indică dacă producătorul suspectează că incidentul este cauzat de acte ilegale sau rău-intenționate sau consideră că acesta are un impact transfrontalier.	***de produsul cu elemente digitale, mai multe detalii cu privire la incidentul semnificativ.*** ENISA transmite notificările, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, punctului unic de contact desemnat în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre în cauză și informează ***imediat*** autoritatea de supraveghere a pieței cu privire la incidentele ***semnificative*** notificate. Notificarea incidentului include informații ***strict necesare pentru a informa autoritatea competentă cu privire la incident și, atunci când este relevant și proporțional cu riscul, informații*** privind gravitatea și impactul incidentului și, după caz, indică dacă producătorul suspectează că incidentul este cauzat de acte ilegale sau rău-intenționate sau consideră că acesta are un impact transfrontalier. ***Simpla notificare nu expune entitatea notificatoare unei răspunderi sporite.***

Amendamentul 83

Propunere de regulament
Articolul 11 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Operatorii economici care sunt, de asemenea, identificați ca entități esențiale sau entități importante în temeiul NIS2 și care transmit notificarea incidentelor în temeiul NIS2 ar trebui să fie considerați conformi cu cerințele de la punctul 2 din prezentul articol.

Amendamentul 84

Propunere de regulament
Articolul 11 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. ENISA transmite Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) instituită prin articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] informațiile notificate în temeiul alineatelor (1) și (2) dacă aceste informații sunt relevante pentru gestionarea coordonată la nivel operațional a incidentelor și crizelor de securitate cibernetică de mare amploare.	3. ENISA transmite Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) instituită prin articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] informațiile notificate în temeiul alineatelor (1) și (2) dacă aceste informații sunt relevante pentru gestionarea coordonată la nivel operațional a incidentelor și crizelor ***semnificative*** de securitate cibernetică de mare amploare.

Amendamentul 85

Propunere de regulament
Articolul 11 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Producătorul informează, fără întârzieri nejustificate și după ce a luat cunoștință de acesta, utilizatorii produsului cu elemente digitale cu privire la ***incident*** și, dacă este necesar, cu privire la măsurile corective pe care utilizatorul le poate aplica pentru a atenua impactul incidentului.	4. Producătorul informează, fără întârzieri nejustificate și după ce a luat cunoștință de acesta, utilizatorii produsului cu elemente digitale cu privire la ***incidentul semnificativ, dacă este cazul și dacă riscă să fie afectați negativ de acesta,*** și, dacă este necesar, cu privire la măsurile ***de atenuare a riscurilor și orice măsuri*** corective pe care utilizatorul le poate aplica pentru a atenua impactul incidentului ***semnificativ în ceea ce privește eventualele date afectate și daunele potențiale***.

Amendamentul 86

Propunere de regulament
Articolul 11 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. Obligațiile prevăzute la alineatele (1), (2) și (4) se aplică pe durata de viață a produsului. Pe durata de viață preconizată a produsului, producătorul va

	furniza actualizări de securitate gratuite, care se vor aplica numai produselor cu elemente digitale pentru care producătorul a întocmit o declarație de conformitate UE, în conformitate cu articolul 20 din prezentul regulament.

Amendamentul 87

Propunere de regulament
Articolul 11 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Comisia poate, prin intermediul unor acte de punere în aplicare, să precizeze mai detaliat tipul de informații care trebuie notificate, formatul notificărilor și procedura de efectuare a notificărilor transmise în temeiul alineatelor (1) și (2). Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).	5. ***După consultarea părților interesate și a CSIRT,*** Comisia poate, prin intermediul unor acte de punere în aplicare, să precizeze mai detaliat tipul de informații care trebuie notificate, formatul notificărilor și procedura de efectuare a notificărilor transmise în temeiul alineatelor (1) și (2). Aceste acte de punere în aplicare ***țin seama de standardele europene și internaționale și*** se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Amendamentul 88

Propunere de regulament
Articolul 11 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. Pe baza notificărilor primite în temeiul alineatelor (1) și (2), ENISA pregătește un raport tehnic bienal referitor la tendințele emergente în ceea ce privește riscurile de securitate cibernetică ale produselor cu elemente digitale și îl transmite grupului de cooperare menționat la articolul ***[articolul X]*** din Directiva ***[Directiva XXX/XXXX*** (***NIS2***)***]***. Primul raport de acest tip se prezintă în termen de 24 de luni de la data la care încep să se aplice obligațiile prevăzute la alineatele (1)	6. Pe baza notificărilor primite în temeiul alineatelor (1) și (2), ENISA pregătește un raport tehnic bienal referitor la tendințele emergente în ceea ce privește riscurile de securitate cibernetică ale produselor cu elemente digitale și îl transmite grupului de cooperare menționat la articolul ***14*** din Directiva (***UE***) ***2022/2555***. Primul raport de acest tip se prezintă în termen de 24 de luni de la data la care încep să se aplice obligațiile prevăzute la alineatele (1) și (2).

și (2).

Amendamentul 89

Propunere de regulament
Articolul 11 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. Atunci când identifică o vulnerabilitate a unei componente, inclusiv a unei componente cu sursă deschisă, care este integrată în produsul cu elemente digitale, producătorii raportează vulnerabilitatea persoanei sau entității care întreține componenta respectivă.	7. Atunci când identifică o vulnerabilitate a unei componente, inclusiv a unei componente cu sursă deschisă, care este integrată în produsul cu elemente digitale, producătorii raportează vulnerabilitatea ***și măsura corectivă sau de atenuare adoptată*** persoanei sau entității care întreține componenta respectivă. ***Acest lucru nu îl exonerează pe producător de obligația de a menține conformitatea produsului cu cerințele prezentului regulament și nu creează obligații pentru dezvoltatorii de componente libere și cu sursă deschisă care nu au nicio relație contractuală cu respectivul producător.***

Amendamentul 90

Propunere de regulament
Articolul 12 – alineatul 3 – partea introductivă

Textul propus de Comisie	*Amendamentul*
3. Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la producător. Mandatul permite reprezentantului autorizat să îndeplinească cel puțin următoarele:	3. Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la producător. ***Acesta furnizează, la cerere, o copie a mandatului autorităților de supraveghere a pieței.*** Mandatul permite reprezentantului autorizat să îndeplinească cel puțin următoarele:

Amendamentul 91

Propunere de regulament
Articolul 12 – alineatul 3 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) în cazul în care reprezentantul autorizat are motive să creadă că un produs cu elemente digitale în cauză prezintă un risc de securitate cibernetică, informează producătorul;

Amendamentul 92

Propunere de regulament
Articolul 12 – alineatul 3 – litera b

Textul propus de Comisie	*Amendamentul*
(b) în urma unei cereri motivate din partea unei autorități de supraveghere a pieței, să furnizeze autorității respective toate informațiile și ***documentația*** necesare pentru a demonstra conformitatea produsului cu elemente digitale;	(b) în urma unei cereri motivate din partea unei autorități de supraveghere a pieței, să furnizeze autorității respective toate informațiile și ***documentele*** necesare pentru a demonstra ***siguranța și*** conformitatea produsului cu elemente digitale***, într-o limbă care poate fi ușor înțeleasă de către autoritatea în cauză***;

Amendamentul 93

Propunere de regulament
Articolul 12 – alineatul 3 – litera c

Textul propus de Comisie	*Amendamentul*
(c) să coopereze cu autoritățile de supraveghere a pieței, la cererea acestora, cu privire la orice acțiune întreprinsă pentru eliminarea riscurilor reprezentate de produsul cu elemente digitale acoperit de mandatul reprezentantului autorizat.	(c) să coopereze cu autoritățile de supraveghere a pieței, la cererea acestora, cu privire la orice acțiune întreprinsă pentru eliminarea ***efectivă a*** riscurilor reprezentate de produsul cu elemente digitale acoperit de mandatul reprezentantului autorizat.

Amendamentul 94

Propunere de regulament
Articolul 13 – alineatul 2 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) toate documentele care demonstrează îndeplinirea cerințelor prevăzute la prezentul articol au fost primite de la producător și pot fi inspectate pe o perioadă de 10 ani.

Amendamentul 95

Propunere de regulament
Articolul 13 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. În cazul în care un importator consideră sau are motive să creadă că un produs cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I, importatorul nu introduce produsul pe piață până când produsul respectiv sau procesele instituite de producător nu au fost aduse în conformitate cu cerințele esențiale prevăzute în anexa I. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, importatorul informează producătorul și autoritățile de supraveghere a pieței în acest sens.	3. În cazul în care un importator consideră sau are motive să creadă***, pe baza informațiilor la dispoziția lui,*** că un produs cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I, importatorul nu introduce produsul pe piață până când produsul respectiv sau procesele instituite de producător nu au fost aduse în conformitate cu cerințele esențiale prevăzute în anexa I. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, importatorul informează producătorul și autoritățile de supraveghere a pieței în acest sens.

Amendamentul 96

Propunere de regulament
Articolul 13 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Importatorii indică pe produsul cu elemente digitale sau, dacă acest lucru nu este posibil, pe ambalaj sau într-un document care însoțește respectivul produs, numele, denumirea lor comercială înregistrată sau marca lor înregistrată, adresa poștală și adresa de e-mail la care	4. Importatorii indică pe produsul cu elemente digitale sau, dacă acest lucru nu este posibil, pe ambalaj sau într-un document care însoțește respectivul produs, numele ***lor***, denumirea lor comercială înregistrată sau marca lor înregistrată, adresa poștală și adresa de e-mail la care

pot fi contactați. Datele de contact trebuie să fie prezentate într-o limbă ușor de înțeles pentru utilizatori și pentru autoritățile de supraveghere a pieței.	pot fi contactați. Datele de contact trebuie să fie prezentate într-o limbă ușor de înțeles pentru utilizatori și pentru autoritățile de supraveghere a pieței.

Amendamentul 97

Propunere de regulament
Articolul 13 – alineatul 6 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Importatorii care știu sau au motive să creadă că un produs cu elemente digitale pe care l-au introdus pe piață sau procesele instituite de producătorul acestuia nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor instituite de producătorul acestuia cu cerințele esențiale prevăzute în anexa I sau pentru a retrage sau a rechema produsul, după caz.	Importatorii care știu sau au motive să creadă că un produs cu elemente digitale pe care l-au introdus pe piață sau procesele instituite de producătorul acestuia nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor instituite de producătorul acestuia cu cerințele esențiale prevăzute în anexa I sau pentru a retrage sau a rechema produsul, după caz. ***Pe baza unei evaluări a riscurilor, distribuitorii și utilizatorii finali sunt informați în timp util cu privire la lipsa conformității și cu privire la măsurile de atenuare a riscurilor pe care le pot adopta.***

Amendamentul 98

Propunere de regulament
Articolul 14 – alineatul 2 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	(ba) au primit de la producător sau de la importator toate informațiile și documentele prevăzute în prezentul regulament.

Amendamentul 99

Propunere de regulament
Articolul 16 – paragraful 1

Textul propus de Comisie	*Amendamentul*
O persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul, care efectuează o modificare substanțială a produsului cu elemente digitale este considerată producător în sensul prezentului regulament.	O persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul, care***, în cadrul activității profesionale,*** efectuează o modificare substanțială a produsului cu elemente digitale ***și pune la dispoziție produsul pe piață*** este considerată producător în sensul prezentului regulament.

Amendamentul 100

Propunere de regulament
Articolul 18 – alineatul 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	1a. Comisia solicită, în temeiul articolului 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații europene de standardizare să elaboreze standarde armonizate pentru cerințele prevăzute în anexa I.

Amendamentul 101

Propunere de regulament
Articolul 18 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. În conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, atunci când elaborează cererea de standardizare pentru produsele care intră în domeniul de aplicare al prezentului regulament, Comisia vizează o armonizare maximă cu standardele internaționale existente sau iminente în materie de securitate cibernetică. În primii trei ani după data aplicării prezentului regulament, Comisia este împuternicită să declare un standard internațional existent ca îndeplinind

	cerințele prezentului regulament, fără modificări la nivel european, cu condiția ca respectarea acestor standarde să îmbunătățească suficient securitatea produselor cu elemente digitale, iar standardul să fie publicat ca versiune separată de una dintre organizațiile europene de standardizare.

Amendamentul 102

Propunere de regulament
Articolul 19 – paragraful 1

Textul propus de Comisie	*Amendamentul*
În cazul în care standardele armonizate menționate la articolul 18 nu există sau în cazul în care Comisia ***consideră că standardele armonizate relevante sunt insuficiente pentru a satisface cerințele prezentului regulament sau pentru a răspunde cererii*** de ***standardizare*** a ***Comisiei sau în cazul în*** care ***există întârzieri nejustificate în procedura de standardizare sau în cazul în*** care ***solicitarea de standarde armonizate din partea Comisiei nu*** a ***fost acceptată de organizațiile europene de standardizare, Comisia este împuternicită să adopte, prin intermediul unor acte*** de ***punere în*** aplicare***, specificații comune cu privire la cerințele esențiale prevăzute în anexa I***. Aceste acte de punere în aplicare se adoptă în ***conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).***	***1.*** Comisia ***poate adopta acte de punere în aplicare*** de ***stabilire*** a ***unor specificații comune*** care ***să acopere cerințele tehnice*** care ***oferă un mijloc de respectare*** a ***cerințelor esențiale privind sănătatea și siguranța prevăzute în anexa I pentru produsele care intră în domeniul*** de aplicare ***al prezentului regulament***. Aceste acte de punere în aplicare se adoptă în ***cazul în care sunt îndeplinite următoarele condiții:***
	(a) Comisia a solicitat, în temeiul articolului 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații europene de standardizare să elaboreze un standard armonizat pentru cerințele esențiale prevăzute în anexa I și:
	(i) cererea nu a fost acceptată; sau
	(ii) standardele armonizate care răspund cererii respective nu sunt

furnizate în termenul stabilit în conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012; sau

(iii) standardele armonizate nu respectă cererea; și dacă

(b) în Jurnalul Oficial al Uniunii Europene nu este publicată nicio referință la standardele armonizate care acoperă cerințele prevăzute în anexa I, în conformitate cu Regulamentul (UE) nr. 1025/2012, și nu se preconizează publicarea niciunei astfel de referințe într-un termen rezonabil.

Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 48 alineatul (3).

Amendamentul 103

Propunere de regulament
Articolul 19 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	1a. Înainte de a pregăti proiectul de act de punere în aplicare menționat la alineatul (3), Comisia informează comitetul menționat la articolul 22 din Regulamentul (UE) nr. 1025/2012 că, în opinia sa, condițiile de la alineatul (3) sunt îndeplinite.

Amendamentul 104

Propunere de regulament
Articolul 19 – paragraful 1 b (nou)

Textul propus de Comisie	*Amendamentul*
	1b. La elaborarea proiectului de act de punere în aplicare menționat la alineatul (1), Comisia ține seama de opiniile organismelor relevante sau ale grupului de experți și consultă în mod

corespunzător toate părțile interesate relevante.

Amendamentul 105

Propunere de regulament
Articolul 19 – paragraful 1 c (nou)

Textul propus de Comisie	*Amendamentul*
	1c. În cazul în care un standard armonizat este adoptat de o organizație de standardizare europeană și este propus Comisiei în vederea publicării referinței sale în Jurnalul Oficial al Uniunii Europene, Comisia evaluează standardul armonizat în conformitate cu Regulamentul (UE) nr. 1025/2012. Atunci când referința unui standard armonizat este publicată în Jurnalul Oficial al Uniunii Europene, Comisia abrogă actele de punere în aplicare menționate la alineatul (1) sau acele părți ale lor care vizează aceleași cerințe precum cele vizate de respectivul standard armonizat.

Amendamentul 106

Propunere de regulament
Articolul 19 – paragraful 1 d (nou)

Textul propus de Comisie	*Amendamentul*
	1d. În cazul în care un stat membru consideră că o specificație comună nu satisface în totalitate cerințele prevăzute în anexa I, acesta informează Comisia, prezentând o explicație detaliată. Comisia evaluează această explicație detaliată și poate, dacă este cazul, să modifice actul de punere în aplicare prin care se stabilește specificația comună în cauză.

Amendamentul 107

Propunere de regulament
Articolul 20 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Declarația de conformitate UE trebuie să fie structurată după modelul prevăzut în anexa IV și să conțină elementele specificate în procedurile relevante de evaluare a conformității stabilite în anexa VI. O astfel de declarație trebuie actualizată ***în permanență***. Aceasta trebuie pusă la dispoziție ***în limba sau limbile solicitate*** de ***statul*** membru în care produsul cu elemente digitale este introdus pe piață sau pus la dispoziție.	2. Declarația de conformitate UE trebuie să fie structurată după modelul prevăzut în anexa IV și să conțină elementele specificate în procedurile relevante de evaluare a conformității stabilite în anexa VI. O astfel de declarație trebuie actualizată ***după caz***. Aceasta trebuie pusă la dispoziție ***într-o limbă care poate fi înțeleasă ușor*** de ***autoritățile statului*** membru în care produsul cu elemente digitale este introdus pe piață sau pus la dispoziție.

Amendamentul 108

Propunere de regulament
Articolul 20 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 20 a
	Declarația UE de încorporare pentru produsele cu elemente digitale finalizate parțial
	1. Declarația UE de încorporare este întocmită de producători în conformitate cu articolul 10 alineatul (7) și prevede faptul că îndeplinirea cerințelor esențiale relevante prevăzute în anexa I a fost demonstrată.
	2. Declarația UE de încorporare are structura modelului prevăzut în anexa IVa (nouă). O astfel de declarație trebuie actualizată după caz. Aceasta trebuie pusă la dispoziție în limba sau limbile solicitate de statul membru în care produsul cu elemente digitale finalizat parțial este introdus pe piață sau pus la dispoziție.
	3. În cazul în care un produs cu elemente digitale finalizat parțial face obiectul mai multor acte ale Uniunii care

impun o declarație a UE de încorporare, se întocmește o singură declarație a UE de încorporare în temeiul tuturor acestor acte ale Uniunii. Declarația respectivă conține elementele de identificare a actelor în cauză ale Uniunii, inclusiv referințele de publicare ale acestora.

4. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin adăugarea de elemente la conținutul minim al declarației UE de încorporare prevăzute în anexa IVa (nouă), pentru a ține seama de evoluțiile tehnologice.

Amendamentul 109

Propunere de regulament
Articolul 22 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Marcajul CE se aplică în mod vizibil, lizibil și indelebil pe produsul cu elemente digitale. În cazul în care acest lucru nu este posibil sau nu este justificat din cauza naturii produsului cu elemente digitale, marcajul se aplică pe ambalaj și pe declarația de conformitate UE menționată la articolul 20 care însoțește produsul cu elemente digitale. Pentru produsele cu elemente digitale care sunt sub formă de software, marcajul CE se aplică fie pe declarația de conformitate UE menționată la articolul 20, fie pe site-ul care însoțește produsul software.	1. Marcajul CE se aplică în mod vizibil, lizibil și indelebil pe produsul cu elemente digitale. În cazul în care acest lucru nu este posibil sau nu este justificat din cauza naturii produsului cu elemente digitale, marcajul se aplică pe ambalaj și pe declarația de conformitate UE menționată la articolul 20 care însoțește produsul cu elemente digitale. Pentru produsele cu elemente digitale care sunt sub formă de software, marcajul CE se aplică fie pe declarația de conformitate UE menționată la articolul 20, fie pe site-ul care însoțește produsul software. ***În această ultimă situație, secțiunea relevantă a site-ului trebuie să fie accesibilă cu ușurință și în mod direct pentru consumatori.***

Amendamentul 110

Propunere de regulament
Articolul 22 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Marcajul CE se aplică înainte ca produsul cu elemente digitale să fie introdus pe piață. Acesta poate fi urmat de o pictogramă sau de orice alt marcaj care indică un risc special sau o utilizare specială prevăzut(ă) în actele de punere în aplicare menționate la alineatul (6).	3. Marcajul CE se aplică înainte ca produsul cu elemente digitale să fie introdus pe piață. Acesta poate fi urmat de o pictogramă sau de orice alt marcaj care indică ***consumatorilor*** un risc special sau o utilizare specială prevăzut(ă) în actele de punere în aplicare menționate la alineatul (6).

Amendamentul 111

Propunere de regulament
Articolul 22 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Statele membre se bazează pe mecanismele existente pentru a asigura aplicarea corectă a regimului aplicabil marcajului CE și întreprind acțiuni corespunzătoare în cazul utilizării inadecvate a respectivului marcaj. În cazul în care produsul cu elemente digitale face obiectul altor acte legislative ale Uniunii care prevăd și aplicarea marcajului CE, marcajul indică faptul că produsul îndeplinește și cerințele celorlalte acte legislative.	5. Statele membre se bazează pe mecanismele existente pentru a asigura aplicarea corectă ***și armonizată*** a regimului aplicabil marcajului CE și întreprind acțiuni corespunzătoare ***și coordonate*** în cazul utilizării inadecvate a respectivului marcaj. În cazul în care produsul cu elemente digitale face obiectul altor acte legislative ale Uniunii care prevăd și aplicarea marcajului CE, marcajul indică faptul că produsul îndeplinește și cerințele celorlalte acte legislative.

Amendamentul 112

Propunere de regulament
Articolul 22 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. Comisia poate stabili, prin intermediul unor acte ***de punere în aplicare***, specificații tehnice pentru pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale, precum și mecanisme de promovare a utilizării acestora***.*** ***Aceste acte de punere*** în ***aplicare*** se adoptă în conformitate cu	6. Comisia poate stabili, prin intermediul unor acte ***delegate***, specificații tehnice pentru ***sistemele de etichetare, inclusiv etichete armonizate,*** pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale, precum și mecanisme de promovare a utilizării acestora ***în rândul întreprinderilor și al***

procedura ***de examinare*** menționată la articolul ***51 alineatul (2)***.	***consumatorilor și pentru a îmbunătăți conștientizarea*** în ***rândul publicului cu privire la securitatea produselor cu elemente digitale. Aceste acte delegate*** se adoptă în conformitate cu procedura menționată la articolul ***50***.

Amendamentul 113

Propunere de regulament
Articolul 22 – alineatul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	6a. Pe un produs cu elemente digitale finalizat parțial nu se aplică marcajul CE în temeiul prezentului regulament, fără a se aduce atingere dispozițiilor privind marcarea rezultate din alte acte legislative aplicabile ale Uniunii.

Amendamentul 114

Propunere de regulament
Articolul 22 – alineatul 6 b (nou)

Textul propus de Comisie	*Amendamentul*
	6b. Comisia adoptă orientări și oferă consiliere operatorilor economici, în special celor care se califică drept IMM-uri, inclusiv microîntreprinderilor, cu privire la punerea în aplicare a prezentului regulament. În special, orientările și consilierea vizează simplificarea și limitarea sarcinilor administrative și financiare, asigurând în același timp aplicarea efectivă și consecventă a prezentului regulament, în conformitate cu obiectivul general de garantare a siguranței produselor și a protecției consumatorilor. Comisia ar trebui să consulte părțile interesate relevante care au cunoștințe de specialitate în domeniul securității cibernetice.

Amendamentul 115

Propunere de regulament
Articolul 23 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Documentația tehnică se întocmește înainte de introducerea pe piață a produsului cu elemente digitale și se actualizează în permanență, după caz, pe durata de viață preconizată a produsului sau pe parcursul unei perioade de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai ***scurtă***.	2. Documentația tehnică se întocmește înainte de introducerea pe piață a produsului cu elemente digitale și se actualizează în permanență, după caz, pe durata de viață preconizată a produsului sau pe parcursul unei perioade de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai ***lungă***.

Amendamentul 116

Propunere de regulament
Articolul 23 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Pentru produsele cu elemente digitale ***menționate la articolul 8 și la articolul 24 alineatul (4)*** care fac, de asemenea, obiectul altor acte ale Uniunii, se întocmește o singură documentație tehnică care conține informațiile menționate în anexa V la prezentul regulament și informațiile prevăzute în respectivele acte ale Uniunii.	3. Pentru produsele cu elemente digitale care fac, de asemenea, obiectul altor acte ale Uniunii, se întocmește o singură documentație tehnică care conține informațiile menționate în anexa V la prezentul regulament și informațiile prevăzute în respectivele acte ale Uniunii.

Amendamentul 117

Propunere de regulament
Articolul 23 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament cu elementele care trebuie	5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament cu elementele care trebuie

incluse în documentația tehnică prevăzută în anexa V, pentru a ține seama de evoluțiile tehnologice, precum și de situațiile întâlnite în procesul de punere în aplicare a prezentului regulament.	incluse în documentația tehnică prevăzută în anexa V, pentru a ține seama de evoluțiile tehnologice, precum și de situațiile întâlnite în procesul de punere în aplicare a prezentului regulament. ***Comisia depune eforturi pentru a reduce la minimum sarcina administrativă, în special pentru microîntreprinderi și întreprinderile mici și mijlocii.***

Amendamentul 118

Propunere de regulament
Articolul 24 – alineatul 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) un sistem european de certificare de securitate cibernetică, adoptat în conformitate cu articolul 18 alineatul (4) din Regulamentul (UE) nr. 2019/881.

Amendamentul 119

Propunere de regulament
Articolul 24 – alineatul 3 – litera b

Textul propus de Comisie	*Amendamentul*
(b) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VI**.**	(b) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VI***; sau***

Amendamentul 120

Propunere de regulament
Articolul 24 – alineatul 3 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	(ba) după caz, un sistem european de certificare a securității cibernetice, cu nivelul de asigurare „substanțial” sau „ridicat”, conform Regulamentului (UE) 2019/881.

Amendamentul 121

Propunere de regulament
Articolul 24 – alineatul 4 a (nou)

Textul propus de Comisie	*Amendamentul*
	4a. În cazul produselor cărora li se aplică legislația de armonizare a Uniunii, pe baza noului cadru legislativ, producătorul urmează evaluarea conformității relevantă, conform respectivelor acte juridice. Cerințele prevăzute la capitolul III se aplică în cazul produselor respective.

Amendamentul 122

Propunere de regulament
Articolul 24 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Atunci când stabilesc taxele pentru procedurile de evaluare a conformității, organismele notificate țin seama de interesele și nevoile specifice ale întreprinderilor mici și mijlocii ***(IMM-uri)*** și reduc taxele respective în mod proporțional cu interesele și nevoile specifice ale acestora.	5. Atunci când stabilesc taxele pentru procedurile de evaluare a conformității, organismele notificate țin seama de interesele și nevoile specifice ale ***microîntreprinderilor,*** întreprinderilor mici și mijlocii și reduc taxele respective în mod proporțional cu interesele și nevoile specifice ale acestora. ***Comisia ia măsuri pentru a asigura proceduri mai accesibile și mai abordabile și un sprijin financiar adecvat în cadrul programelor existente ale Uniunii, în special pentru a ușura sarcina microîntreprinderilor și a întreprinderilor mici și mijlocii.***

Amendamentul 123

Propunere de regulament
Articolul 24 – alineatul 5 a (nou)

Textul propus de Comisie	*Amendamentul*
	5a. Pentru produsele cu elemente digitale care fac obiectul prezentului regulament și care sunt introduse pe piață sau puse în funcțiune de instituții de credit reglementate de Directiva 2013/36/UE, evaluarea conformității se efectuează în cadrul procedurii menționate la articolele 97-101 din directiva respectivă.

Amendamentul 124

Propunere de regulament
Articolul 24 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 24 a
	Dacă produsele cu elemente digitale au elemente hardware sau software echivalente, un model de produs poate fi reprezentativ pentru o familie de produse în scopurile următoarelor proceduri de evaluare a conformității:
	(a) procedura controlului intern (pe baza modulului A) prevăzută în anexa VI sau
	(b) procedura examinării UE de tip (pe baza modulului B) prevăzută în anexa VI, urmată de conformitatea cu tipul UE bazată pe controlul intern al producției (pe baza modulului C) prevăzută în anexa VI.

Amendamentul 125

Propunere de regulament
Articolul 27 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Autoritatea de notificare garantează confidențialitatea informațiilor obținute.	5. Autoritatea de notificare garantează confidențialitatea informațiilor***, inclusiv drepturile de proprietate intelectuală,***

informațiile comerciale confidențiale și secretele comerciale obținute.

Amendamentul 126

Propunere de regulament
Articolul 27 – alineatul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	6a. O autoritate de notificare reduce la minimum birocrația și taxele, în special pentru IMM-uri.

Amendamentul 127

Propunere de regulament
Articolul 29 – alineatul 7 a (nou)

Textul propus de Comisie	*Amendamentul*
	7a. Statele membre și Comisia instituie măsuri adecvate pentru a asigura o disponibilitate suficientă a profesioniștilor calificați, în vederea reducerii la minimum a blocajelor în activitățile organismelor de evaluare a conformității.

Amendamentul 128

Propunere de regulament
Articolul 29 – alineatul 10

Textul propus de Comisie	*Amendamentul*
10. Personalul organismului de evaluare a conformității păstrează secretul profesional referitor la toate informațiile obținute în îndeplinirea sarcinilor sale în temeiul anexei VI sau al oricărei dispoziții din legislația națională de punere în aplicare a acesteia, excepție făcând relația cu autoritățile de supraveghere a pieței ale statului membru în care își desfășoară activitățile. Drepturile de ***autor*** sunt	10. Personalul organismului de evaluare a conformității păstrează secretul profesional referitor la toate informațiile obținute în îndeplinirea sarcinilor sale în temeiul anexei VI sau al oricărei dispoziții din legislația națională de punere în aplicare a acesteia, excepție făcând relația cu autoritățile de supraveghere a pieței ale statului membru în care își desfășoară activitățile. Drepturile de ***proprietate***

protejate. Organismul de evaluare a conformității trebuie să dispună de proceduri documentate care să asigure conformitatea cu prezentul alineat.	***intelectuală, informațiile comerciale confidențiale și secretele comerciale*** sunt protejate. Organismul de evaluare a conformității trebuie să dispună de proceduri documentate care să asigure conformitatea cu prezentul alineat.

Amendamentul 129

Propunere de regulament
Articolul 29 – alineatul 12

Textul propus de Comisie	*Amendamentul*
12. Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termene și condiții coerente, echitabile și rezonabile, ținând seama în mod special de interesele ***IMM-urilor*** în ceea ce privește taxele.	12. Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termene și condiții coerente, echitabile și rezonabile, ***în conformitate cu articolul 37 alineatul (2),*** ținând seama în mod special de interesele ***microîntreprinderilor, întreprinderilor mici și mijlocii*** în ceea ce privește taxele.

Amendamentul 130

Propunere de regulament
Articolul 36 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Comisia se asigură că toate informațiile ***sensibile*** obținute pe parcursul investigațiilor sale sunt tratate ***în mod*** confidențial.	3. Comisia se asigură că toate informațiile***, inclusiv drepturile de proprietate intelectuală, informațiile comerciale confidențiale și secretele comerciale confidențiale,*** obținute pe parcursul investigațiilor sale sunt tratate confidențial.

Amendamentul 131

Propunere de regulament
Articolul 37 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. ***Evaluările*** conformității ***sunt***	2. ***Evaluarea*** conformității ***se***

realizate în mod proporțional, evitând sarcinile inutile pentru operatorii economici. Organismul de evaluare a conformității își desfășoară activitatea ținând seama în mod corespunzător de dimensiunea întreprinderii, de domeniul de activitate și structura acesteia, de gradul de complexitate ***al*** tehnologiei utilizate pentru produse, precum și de caracterul de serie sau de masă al procesului de producție.	***efectuează*** în mod proporțional, evitând sarcinile inutile pentru operatorii economici ***și importatorii privați, acordând o atenție deosebită IMM-urilor***. Organismul de evaluare a conformității își desfășoară activitatea ținând seama în mod corespunzător de dimensiunea întreprinderii, de domeniul de activitate și structura acesteia, de gradul de complexitate ***și de expunerea la risc a tipului de produs și a*** tehnologiei utilizate pentru produse, precum și de caracterul de serie sau de masă al procesului de producție.

Amendamentul 132

Propunere de regulament
Articolul 37 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Atunci când pe parcursul monitorizării conformității efectuate după eliberarea certificatului organismul notificat constată că un produs nu mai este conform cu cerințele prevăzute în prezentul regulament, acesta solicită producătorului să ia măsurile corective adecvate și suspendă sau retrage certificatul, dacă este necesar.	5. Atunci când pe parcursul monitorizării conformității efectuate după eliberarea certificatului organismul notificat constată că un produs nu mai este conform cu cerințele prevăzute în prezentul regulament, acesta solicită producătorului să ia măsurile corective adecvate și ***restricționează,*** suspendă sau retrage certificatul, dacă este necesar.

Amendamentul 133

Propunere de regulament
Articolul 40 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Comisia se asigură că între organismele notificate există o coordonare și o cooperare adecvată, care funcționează în cadrul unui grup transsectorial al organismelor notificate.	1. Comisia se asigură că între organismele notificate există o coordonare și o cooperare adecvată, ***ținând seama și de necesitatea de a reduce birocrația și taxele,*** care funcționează în cadrul unui grup transsectorial al organismelor notificate.

Amendamentul 134

Propunere de regulament
Articolul 40 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Statele membre se asigură că organismele notificate de ele participă la activitatea grupului respectiv, în mod direct sau prin intermediul unor reprezentanți desemnați.	2. Statele membre se asigură că organismele notificate de ele participă la activitatea grupului respectiv, în mod direct sau prin intermediul unor reprezentanți desemnați***, ținând seama și de necesitatea de a reduce birocrația și taxele***.

Amendamentul 135

Propunere de regulament
Articolul 41 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu autoritățile naționale de certificare a securității cibernetice desemnate în temeiul articolului 58 din Regulamentul (UE) 2019/881 și fac schimb de informații în mod regulat. În ceea ce privește supravegherea punerii în aplicare a obligațiilor de raportare în temeiul articolului 11 din prezentul regulament, autoritățile de supraveghere a pieței desemnate cooperează cu ENISA.	3. Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu autoritățile naționale de certificare a securității cibernetice desemnate în temeiul articolului 58 din Regulamentul (UE) 2019/881 și fac schimb de informații în mod regulat. În ceea ce privește supravegherea punerii în aplicare a obligațiilor de raportare în temeiul articolului 11 din prezentul regulament, autoritățile de supraveghere a pieței desemnate cooperează ***în mod eficace*** cu ENISA. ***Autoritățile de supraveghere a pieței pot solicita ENISA să furnizeze consiliere tehnică pe teme legate de punerea în aplicare și asigurarea respectării prezentului regulament, inclusiv în timpul investigațiilor derulate în conformitate cu articolul 43, în cadrul cărora autoritățile de supraveghere a pieței pot solicita ENISA să ofere evaluări fără caracter obligatoriu în ceea ce privește conformitatea produselor cu elemente digitale.***

Amendamentul 136

Propunere de regulament
Articolul 41 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. Comisia facilitează schimbul de experiență între autoritățile de supraveghere a pieței desemnate.	7. Comisia facilitează schimbul de experiență ***regulat și structurat*** între autoritățile de supraveghere a pieței desemnate***, inclusiv printr-un grup specific de cooperare administrativă (ADCO), instituit în temeiul alineatului (11) de la prezentul articol***.

Amendamentul 137

Propunere de regulament
Articolul 41 – alineatul 8

Textul propus de Comisie	*Amendamentul*
8. ***Autoritățile de supraveghere a pieței pot oferi orientări și recomandări operatorilor economici*** cu privire la punerea în aplicare a prezentului regulament, cu ***sprijinul Comisiei***.	8. ***Comisia adoptă orientări și oferă consiliere operatorilor economici, în special celor care se califică drept IMM-uri, inclusiv microîntreprinderilor,*** cu privire la punerea în aplicare a prezentului regulament***. În special***, ***orientările și consilierea vizează simplificarea și limitarea sarcinilor administrative și financiare, asigurând în același timp aplicarea efectivă și consecventă, în conformitate*** cu ***obiectivul general de garantare a siguranței produselor și a protecției consumatorilor***.

Amendamentul 138

Propunere de regulament
Articolul 41 – alineatul 8 a (nou)

Textul propus de Comisie	*Amendamentul*
	8a. Autoritățile de supraveghere a pieței sunt în măsură să primească plângeri din partea consumatorilor în conformitate cu articolul 11 din

	Regulamentul 2019/1020, în special stabilind mecanisme clare și accesibile pentru facilitarea raportării vulnerabilităților, incidentelor și amenințărilor cibernetice.

Amendamentul 139

Propunere de regulament
Articolul 41 – alineatul 11

Textul propus de Comisie	*Amendamentul*
11. Se instituie un grup specific de cooperare administrativă (ADCO) pentru aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO trebuie să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate și, dacă este cazul, din reprezentanți ai birourilor unice de legătură.	11. Se instituie un grup specific de cooperare administrativă (ADCO) pentru aplicarea uniformă a prezentului regulament, ***pentru a facilita cooperarea structurată în legătură cu punerea în aplicare a prezentului regulament și pentru a simplifica practicile autorităților de supraveghere a pieței de la nivelul Uniunii,*** în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO ***are, în special, sarcinile menționate la articolul 32 alineatul (2) din Regulamentul (UE) 2019/1020 și*** trebuie să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate***, ai ENISA*** și, dacă este cazul, din reprezentanți ai birourilor unice de legătură. ***ADCO se reunește la intervale regulate și, atunci când este nevoie, la solicitarea justificată în mod corespunzător a Comisiei, a ENISA sau a unui stat membru și își coordonează acțiunile cu alte activități existente ale Uniunii legate de supravegherea pieței și de siguranța consumatorilor și, acolo unde este relevant, cooperează și face schimb de informații cu alte rețele, grupuri și organisme ale Uniunii. ADCO poate invita experți și alți terți, inclusiv organizații ale consumatorilor, să participe la întâlnirile sale.***

Amendamentul 140

Propunere de regulament
Articolul 41 – alineatul 11 a (nou)

Textul propus de Comisie	*Amendamentul*
	11a. Pentru produsele cu elemente digitale care fac obiectul prezentului regulament și sunt distribuite, puse în funcțiune sau utilizate de instituții financiare reglementate prin legislația relevantă a Uniunii privind serviciile financiare, autoritatea de supraveghere a pieței în scopurile prezentului regulament este autoritatea relevantă responsabilă pentru supravegherea financiară a instituțiilor respective, în temeiul acelei legislații.

Amendamentul 141

Propunere de regulament
Articolul 42 – paragraful 1

Textul propus de Comisie	*Amendamentul*
În cazul în care este necesar pentru a evalua conformitatea produselor cu elemente digitale și a proceselor instituite de producătorii lor cu cerințele esențiale prevăzute în anexa I și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă acces la datele necesare pentru a evalua proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților acestor produse, inclusiv la documentația internă aferentă a operatorului economic respectiv.	În cazul în care este necesar pentru a evalua conformitatea produselor cu elemente digitale și a proceselor instituite de producătorii lor cu cerințele esențiale prevăzute în anexa I și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă acces la datele necesare pentru a evalua proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților acestor produse, inclusiv la documentația internă aferentă a operatorului economic respectiv. ***După caz și în conformitate cu articolul 52 alineatul (1) litera (a), aceste demersuri se desfășoară într-un mediu sigur și controlat, stabilit de producător.***

Amendamentul 142

Propunere de regulament
Articolul 43 – alineatul 1 – paragraful 2

Textul propus de Comisie	*Amendamentul*
În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că produsul cu elemente digitale nu respectă cerințele prevăzute în prezentul regulament, aceasta solicită fără întârziere operatorului relevant să întreprindă toate acțiunile corective adecvate pentru a aduce produsul în conformitate cu cerințele sau pentru a retrage produsul de pe piață ori pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului și stabilit de autoritatea respectivă.	În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că produsul cu elemente digitale nu respectă cerințele prevăzute în prezentul regulament ***sau prezintă în alt mod o amenințare pentru securitatea națională***, aceasta solicită fără întârziere operatorului ***economic*** relevant să întreprindă toate acțiunile corective adecvate pentru a aduce produsul în conformitate cu cerințele sau pentru a retrage produsul de pe piață ori pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului și stabilit de autoritatea respectivă. ***Înainte de efectuarea evaluării menționate mai sus, dacă este necesar, ținând seama de importanța riscului de securitate cibernetică, autoritatea de supraveghere a pieței poate solicita operatorului relevant să suspende sau să restricționeze imediat disponibilitatea produsului pe piață pentru perioada evaluării menționate mai sus.***

Amendamentul 143

Propunere de regulament
Articolul 43 – alineatul 4 – paragraful 1

Textul propus de Comisie	*Amendamentul*
În cazul în care producătorul unui produs cu elemente digitale nu întreprinde acțiuni corective adecvate în termenul menționat la alineatul (1) al doilea paragraf, autoritatea de supraveghere a pieței ia toate măsurile provizorii adecvate pentru a interzice sau a restricționa punerea la dispoziție a produsului respectiv pe piața sa națională, pentru a-l retrage de pe piață sau pentru a-l rechema.	În cazul în care producătorul unui produs cu elemente digitale nu întreprinde acțiuni corective adecvate în termenul menționat la alineatul (1) al doilea paragraf ***sau dacă autoritatea relevantă din statul membru consideră că produsul prezintă o amenințare pentru securitatea națională***, autoritatea de supraveghere a pieței ia toate măsurile provizorii adecvate pentru a interzice sau a restricționa punerea la dispoziție a produsului respectiv pe piața sa națională, pentru a-l retrage de pe piață sau

pentru a-l rechema.

Amendamentul 144

Propunere de regulament
Articolul 45 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În cazul în care Comisia are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică nu respectă cerințele prevăzute în prezentul regulament, aceasta ***poate solicita*** autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43.	1. În cazul în care Comisia are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ***autoritățile competente ale statelor membre, de echipele de intervenție în caz de incidente de securitate informatică (CSIRT) desemnate sau stabilite în conformitate cu Directiva (UE) 2022/2555 sau de*** ENISA, că un produs cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică nu respectă cerințele prevăzute în prezentul regulament, aceasta ***solicită*** autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43.

Amendamentul 145

Propunere de regulament
Articolul 45 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. În circumstanțe ***excepționale*** care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive ***suficiente*** să considere că produsul menționat la alineatul (1) continuă să nu respecte cerințele prevăzute în prezentul regulament, iar autoritățile relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia ***poate solicita*** ENISA să efectueze o evaluare a conformității. Comisia informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează	2. În circumstanțe care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive să considere că produsul menționat la alineatul (1) continuă să nu respecte cerințele prevăzute în prezentul regulament, iar autoritățile relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia ***solicită*** ENISA să efectueze o evaluare a conformității. Comisia informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție

cu ENISA în funcție de necesități.

de necesități.

Amendamentul 146

Propunere de regulament
Articolul 46 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În cazul în care, în urma efectuării unei evaluări în temeiul articolului 43, autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un produs cu elemente digitale și procesele instituite de producător sunt conforme cu prezentul regulament, acestea prezintă un risc semnificativ în materie de securitate cibernetică și, în plus, prezintă un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin intermediul unui sistem informatic electronic de tipul celor menționate în ***[anexa*** I la Directiva ***XXX/XXXX*** (NIS2)***]*** sau în ceea ce privește alte aspecte ale protecției interesului public, aceasta impune operatorului relevant să ia toate măsurile adecvate pentru a se asigura că respectivul produs cu elemente digitale și procesele instituite de producătorul în cauză nu mai prezintă riscul respectiv la introducerea pe piață, pentru a retrage produsul cu elemente digitale de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului.	1. În cazul în care, în urma efectuării unei evaluări în temeiul articolului 43, autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un produs cu elemente digitale și procesele instituite de producător sunt conforme cu prezentul regulament, acestea prezintă un risc semnificativ în materie de securitate cibernetică și, în plus, prezintă un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin intermediul unui sistem informatic electronic de tipul celor menționate în ***anexa*** I la 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)***,*** sau în ceea ce privește alte aspecte ale protecției interesului public, aceasta impune operatorului ***economic*** relevant să ia toate măsurile adecvate pentru a se asigura că respectivul produs cu elemente digitale și procesele instituite de producătorul în cauză nu mai prezintă riscul respectiv la introducerea pe piață, pentru a retrage produsul cu elemente digitale de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului.

Amendamentul 147

Propunere de regulament
Articolul 46 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Producătorul sau alți operatori relevanți se asigură că sunt întreprinse acțiuni corective cu privire la produsele cu elemente digitale în cauză pe care aceștia le-au pus la dispoziție pe piață în întreaga Uniune, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).	2. Producătorul sau alți operatori ***economici*** relevanți se asigură că sunt întreprinse acțiuni corective cu privire la produsele cu elemente digitale în cauză pe care aceștia le-au pus la dispoziție pe piață în întreaga Uniune, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).

Amendamentul 148

Propunere de regulament
Articolul 46 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. În cazul în care are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale, deși este conform cu prezentul regulament, prezintă riscurile menționate la alineatul (1), Comisia ***poate solicita*** autorității sau autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43 și la alineatele (1), (2) și (3) din prezentul articol.	6. În cazul în care are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale, deși este conform cu prezentul regulament, prezintă riscurile menționate la alineatul (1), Comisia ***solicită*** autorității sau autorităților relevante de supraveghere a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43 și la alineatele (1), (2) și (3) din prezentul articol.

Amendamentul 149

Propunere de regulament
Articolul 46 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. În circumstanțe excepționale care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive	7. În circumstanțe excepționale care justifică o intervenție imediată pentru a menține buna funcționare a pieței interne și în cazul în care Comisia are motive

suficiente să considere că produsul menționat la alineatul (6) continuă să prezinte riscurile prevăzute la alineatul (1), iar autoritățile naționale relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia ***poate solicita*** ENISA să efectueze o evaluare a riscurilor prezentate de produs și informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.	suficiente să considere că produsul menționat la alineatul (6) continuă să prezinte riscurile prevăzute la alineatul (1), iar autoritățile naționale relevante de supraveghere a pieței nu au luat măsuri eficace, Comisia ***solicită*** ENISA să efectueze o evaluare a riscurilor prezentate de produs și informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.

Amendamentul 150

Propunere de regulament
Articolul 48 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Autoritățile de supraveghere a pieței ***pot conveni cu alte autorități relevante să desfășoare activități comune*** menite să asigure securitatea cibernetică și protecția consumatorilor în ceea ce privește anumite produse cu elemente digitale introduse sau puse la dispoziție pe piață, în special produsele despre care se constată adesea că prezintă riscuri de securitate cibernetică.	1. Autoritățile de supraveghere a pieței ***desfășoară în mod regulat activități comune cu alte autorități relevante*** menite să asigure securitatea cibernetică și protecția consumatorilor în ceea ce privește anumite produse cu elemente digitale introduse sau puse la dispoziție pe piață, în special produsele despre care se constată adesea că prezintă riscuri de securitate cibernetică. ***Aceste activități includ inspecții ale produselor achiziționate sub o identitate falsă.***

Amendamentul 151

Propunere de regulament
Articolul 48 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Comisia sau ENISA ***poate*** propune desfășurarea de activități comune de verificare a conformității cu prezentul regulament de către autoritățile de supraveghere a pieței pe baza unor indicii sau informații privind o potențială neconformitate în mai multe state membre	2. Comisia sau ENISA propune desfășurarea de activități comune de verificare a conformității cu prezentul regulament de către autoritățile de supraveghere a pieței pe baza unor indicii sau informații privind o potențială neconformitate în mai multe state membre

a unor produse care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în acesta.	a unor produse care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în acesta.

Amendamentul 152

Propunere de regulament
Articolul 49 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Autoritățile de supraveghere a pieței ***pot decide să desfășoare*** acțiuni de control coordonate simultane („acțiuni de verificare”) pentru anumite produse cu elemente digitale sau pentru anumite categorii de astfel de produse, în scopul de a verifica respectarea prezentului regulament sau de a detecta încălcările acestuia.	1. Autoritățile de supraveghere a pieței ***desfășoară periodic*** acțiuni de control coordonate simultane („acțiuni de verificare”) pentru anumite produse cu elemente digitale sau pentru anumite categorii de astfel de produse, în scopul de a verifica respectarea prezentului regulament sau de a detecta încălcările acestuia.

Amendamentul 153

Propunere de regulament
Articolul 49 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Cu excepția cazului în care autoritățile de supraveghere a pieței în cauză convin altfel, acțiunile de verificare sunt coordonate de Comisie. Coordonatorul acțiunii de verificare ***poate***, dacă este cazul, ***să pună*** la dispoziția publicului rezultatele agregate.	2. Cu excepția cazului în care autoritățile de supraveghere a pieței în cauză convin altfel, acțiunile de verificare sunt coordonate de Comisie. Coordonatorul acțiunii de verificare ***pune***, dacă este cazul, la dispoziția publicului rezultatele agregate.

Amendamentul 154

Propunere de regulament
Articolul 49 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. ENISA ***poate identifica***, în îndeplinirea sarcinilor sale, inclusiv pe baza notificărilor primite în conformitate	3. ENISA ***identifică***, în îndeplinirea sarcinilor sale, inclusiv pe baza notificărilor primite în conformitate cu

cu articolul 11 alineatele (1) și (2), categoriile de produse pentru care ***pot fi organizate*** acțiuni de verificare. Propunerea de acțiuni de verificare este prezentată coordonatorului potențial menționat la alineatul (2) pentru a fi examinată de autoritățile de supraveghere a pieței.	articolul 11 alineatele (1) și (2), categoriile de produse pentru care ***se organizează*** acțiuni de verificare. Propunerea de acțiuni de verificare este prezentată coordonatorului potențial menționat la alineatul (2) pentru a fi examinată de autoritățile de supraveghere a pieței.

Amendamentul 155

Propunere de regulament
Articolul 49 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Autoritățile de supraveghere a pieței ***pot invita*** funcționari ai Comisiei și alte persoane însoțitoare autorizate de Comisie să participe la acțiunile de verificare.	5. Autoritățile de supraveghere a pieței ***invită*** funcționari ai Comisiei și alte persoane însoțitoare autorizate de Comisie să participe la acțiunile de verificare.

Amendamentul 156

Propunere de regulament
Articolul 49 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 49 a
	Furnizarea de consiliere tehnică
	1. Printr-un act de punere în aplicare, Comisia numește un grup de experți care să furnizeze consiliere tehnică autorităților de supraveghere a pieței pe teme legate de punerea în aplicare și asigurarea respectării prezentului regulament. Actul de punere în aplicare specifică, printre altele, detaliile legate de componența grupului, de funcționarea acestuia și de remunerarea membrilor săi. În special, grupul de experți oferă evaluări fără caracter obligatoriu ale produselor cu elemente digitale, la cererea unei autorități de supraveghere a pieței care

efectuează o investigație în temeiul articolului 43, și ale listei de produse critice cu elemente digitale stabilite în anexa II, precum și cu privire la eventuala necesitate de a actualiza lista respectivă.

2. Grupul de experți este alcătuit din experți independenți numiți de Comisie pentru un mandat de trei ani, care poate fi reînnoit, pe baza expertizei lor științifice sau tehnice în domeniu.

3. Comisia numește un număr de experți considerat suficient pentru a acoperi nevoile prevăzute.

4. Comisia ia toate măsurile necesare pentru a gestiona și a preveni orice conflicte de interese. Declarațiile de interese ale membrilor grupului de experți sunt puse la dispoziția publicului.

5. Experții numiți își îndeplinesc sarcinile cu cel mai înalt nivel de profesionalism, independență, imparțialitate și obiectivitate.

6. Atunci când adoptă poziții, opinii și rapoarte, grupul de experți încearcă să ajungă la un consens. Dacă nu se poate ajunge la un consens, deciziile se iau cu majoritatea simplă a membrilor grupului.

Amendamentul 157

Propunere de regulament
Articolul 53 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor prezentului regulament de către operatorii economici și iau toate măsurile necesare asigurării punerii în aplicare a acestora. ***Aceste sancțiuni*** trebuie să fie ***efective***, proporționale și ***cu efect de descurajare***.	1. Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor prezentului regulament de către operatorii economici și iau toate măsurile necesare asigurării punerii în aplicare a acestora. ***Sancțiunile*** trebuie să fie ***eficace***, proporționale și ***disuasive și iau în considerare caracteristicile specifice ale microîntreprinderilor, întreprinderilor***

mici și mijlocii.

Amendamentul 158

Propunere de regulament
Articolul 53 – alineatul 6 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) dacă încălcarea este neintenționată;

Amendamentul 159

Propunere de regulament
Articolul 53 – alineatul 6 – litera b

Textul propus de Comisie	*Amendamentul*
(b) dacă alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator pentru o încălcare similară;	(b) dacă ***aceleași sau*** alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator pentru o încălcare similară;

Amendamentul 160

Propunere de regulament
Articolul 53 – alineatul 6 – litera c

Textul propus de Comisie	*Amendamentul*
(c) dimensiunea și cota de piață ale operatorului care a săvârșit încălcarea**.**	(c) dimensiunea și cota de piață ale operatorului care a săvârșit încălcarea***, ținând cont de amploarea riscurilor, de consecințe și de particularitățile financiare ale microîntreprinderilor și ale întreprinderilor mici și mijlocii;***

Amendamentul 161

Propunere de regulament
Articolul 53 – alineatul 6 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) comportamentul ulterior al operatorului în urma informațiilor sau a cunoștințelor cu privire la neconformitatea respectivă, inclusiv dacă, atunci când ia cunoștință de neconformitatea respectivă, operatorul a utilizat toate măsurile corective adecvate, precum și măsurile necesare în mod rezonabil pentru a evita sau a reduce la minimum potențialele consecințe negative.

Amendamentul 162

Propunere de regulament
Capitolul VII a (nou)

Textul propus de Comisie	*Amendamentul*
	MĂSURI DE SPRIJINIRE A INOVĂRII

Amendamentul 163

Propunere de regulament
Articolul 53 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 53 a
	Spațiile de testare în materie de reglementare
	Comisia și ENISA pot institui un spațiu european de testare în materie de reglementare, cu participarea voluntară a fabricanților de produse cu elemente digitale, pentru:
	(a) a asigura un mediu controlat care facilitează dezvoltarea, testarea și validarea proiectării, dezvoltării și producției de produse cu elemente digitale, înainte de introducerea lor pe piață sau de punerea lor în funcțiune

conform unui plan concret;

(b) a oferi un sprijin practic operatorilor economici, inclusiv prin orientări și prin bune practici, pentru a îndeplini cerințele esențiale prevăzute în anexa I;

(c) a contribui la învățarea bazată pe dovezi în materie de reglementare.

Amendamentul 164

Propunere de regulament
Articolul 54 – titlu

Textul propus de Comisie	*Amendamentul*
Modificare adusă Regulamentului (UE) 2019/1020	Modificare adusă Regulamentului (UE) 2019/1020 ***și Directivei 2020/1828/CE***

Amendamentul 165

Propunere de regulament
Articolul 54 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	1a. În anexa I la Directiva (UE) 2020/1828/CE se adaugă următorul punct:
	„67. [Regulamentul XXX] [Actul european privind reziliența cibernetică].”

Amendamentul 166

Propunere de regulament
Articolul 54 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 54 a
	Regulamentul delegat (UE) 2022/30
	Prezentul regulament este conceput astfel încât toate produsele care fac obiectul cerințelor esențiale prevăzute la

	articolul 3 alineatul (3) literele (d), (e) și (f) din Directiva 2014/53/UE, astfel cum sunt descrise în regulamentul delegat (UE) 2022/30, să fie conforme cu prezentul regulament. Pentru a genera securitate juridică, regulamentul delegat (UE) 2022/30 va fi abrogat la intrarea în vigoare a prezentului regulament.

Amendamentul 167

Propunere de regulament
Articolul 57 – alineatul 2

Textul propus de Comisie	*Amendamentul*
Se aplică de la [***24*** de luni de la data intrării în vigoare a prezentului regulament]. Cu ***toate acestea***, ***articolul 11*** se aplică de ***la*** [***12*** luni de la data ***intrării*** în ***vigoare a*** prezentului regulament].	Se aplică de la [***36*** de luni de la data intrării în vigoare a prezentului regulament]. ***În ceea ce privește produsele*** cu ***elemente critice***, ***capitolele II, III, V și VII*** se aplică ***nu mai devreme*** de [***20*** luni de la data ***publicării standardelor armonizate elaborate*** în ***temeiul standardizării necesare în sensul*** prezentului regulament]. ***În termen de cel mult 6 luni de la data intrării în vigoare a prezentului regulament, Comisia emite orientări cu privire la modul de aplicare a cerințelor prezentului regulament în cazul produselor netangibile.***

Amendamentul 168

Propunere de regulament
Anexa I – partea 1 – punctul 3 – partea introductivă

Textul propus de Comisie	*Amendamentul*
(3) Pe baza evaluării riscurilor menționate la articolul 10 alineatul (2) și după caz, produsele cu elemente digitale trebuie:	(3) Pe baza evaluării riscurilor ***de securitate cibernetică*** menționate la articolul 10 alineatul (2) și după caz, produsele cu elemente digitale trebuie:

Amendamentul 169

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera -a (nouă)

Textul propus de Comisie	*Amendamentul*
	(-a) să fie introduse pe piață fără vulnerabilități exploatabile cunoscute față de un dispozitiv extern sau o rețea externă;

Amendamentul 170

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera a

Textul propus de Comisie	*Amendamentul*
(a) să fie livrate cu o configurație securizată implicită***, inclusiv cu posibilitatea de a reseta produsul la starea sa inițială***;	(a) să fie livrate cu o configurație securizată implicită;

Amendamentul 171

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera c

Textul propus de Comisie	*Amendamentul*
(c) să protejeze confidențialitatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, de exemplu prin criptarea datelor relevante în repaus sau în tranzit prin mecanisme de ultimă generație;	(c) să protejeze confidențialitatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, de exemplu prin criptarea***, tokenizarea, controale de compensare sau alte mecanisme de protecție adecvată a*** datelor relevante în repaus sau în tranzit prin mecanisme de ultimă generație;

Amendamentul 172

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera d

Textul propus de Comisie	*Amendamentul*
(d) să protejeze integritatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, a comenzilor, a programelor și a configurației împotriva oricărei manipulări sau modificări neautorizate de către utilizator, și să raporteze cu privire la fișierele corupte;	(d) să protejeze integritatea datelor stocate, transmise sau prelucrate în alt mod, cu caracter personal sau de altă natură, a comenzilor, a programelor și a configurației împotriva oricărei manipulări sau modificări neautorizate de către utilizator, și să raporteze cu privire la fișierele corupte ***sau la eventualul acces neautorizat***;

Amendamentul 173

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera f

Textul propus de Comisie	*Amendamentul*
(f) să protejeze disponibilitatea funcțiilor esențiale, inclusiv reziliența împotriva atacurilor vizând blocarea accesului la servicii și atenuarea acestora;	(f) să protejeze disponibilitatea funcțiilor esențiale ***și de bază***, inclusiv reziliența împotriva atacurilor vizând blocarea accesului la servicii și atenuarea acestora;

Amendamentul 174

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera i

Textul propus de Comisie	*Amendamentul*
(i) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se reducă impactul unui incident prin utilizarea de mecanisme și tehnici adecvate de prevenire a exploatării vulnerabilităților;	(i) să fie proiectate, dezvoltate și fabricate de așa manieră încât să se reducă impactul unui incident ***semnificativ*** prin utilizarea de mecanisme și tehnici adecvate de prevenire a exploatării vulnerabilităților;

Amendamentul 175

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera j

Textul propus de Comisie	*Amendamentul*
(j) să furnizeze informații legate de securitate ***prin înregistrarea*** și/sau ***monitorizarea activității interne relevante***, inclusiv accesul la date, servicii sau funcții sau modificarea acestora;	(j) să furnizeze informații legate de securitate***, oferind, la solicitarea utilizatorului, capacități de înregistrare*** și/sau ***monitorizare, la nivel local și la nivel de dispozitiv, pentru activitatea internă relevantă***, inclusiv accesul la date, servicii sau funcții sau modificarea acestora;

Amendamentul 176

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera k

Textul propus de Comisie	*Amendamentul*
(k) să asigure faptul că vulnerabilitățile pot fi abordate prin actualizări de securitate, inclusiv, după caz, prin actualizări automate și prin notificarea utilizatorilor cu privire la actualizările disponibile.	(k) să asigure faptul că vulnerabilitățile pot fi abordate prin actualizări de securitate, inclusiv, după caz, ***separate de actualizările de funcționalitate, și*** prin actualizări automate și prin notificarea utilizatorilor cu privire la actualizările disponibile;

Amendamentul 177

Propunere de regulament
Anexa I – partea 1 – punctul 3 – litera ka (nouă)

Textul propus de Comisie	*Amendamentul*
	(ka) să fie proiectate, dezvoltate și produse pentru a permite întreruperea în condiții de siguranță și reciclarea lor potențială atunci când ajung la sfârșitul ciclului de viață, inclusiv permițând utilizatorilor să retragă și să elimine toate datele în mod permanent.

Amendamentul 178

Propunere de regulament
Anexa I – partea 2 – paragraful 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
(2) în ceea ce privește riscurile pe care le prezintă produsele cu elemente digitale, să abordeze și să remedieze fără întârziere vulnerabilitățile, inclusiv prin furnizarea de actualizări de securitate;	(2) în ceea ce privește riscurile pe care le prezintă produsele cu elemente digitale, să abordeze și să remedieze fără întârziere vulnerabilitățile ***critice și ridicate***, inclusiv prin furnizarea de actualizări de securitate***, sau să explice motivele pentru care nu a fost remediată vulnerabilitatea***;

Amendamentul 179

Propunere de regulament
Anexa I – partea 2 – paragraful 1 – punctul 4

Textul propus de Comisie	*Amendamentul*
(4) după punerea la dispoziție a unei actualizări de securitate, să publice informații cu privire la vulnerabilitățile remediate, inclusiv o descriere a vulnerabilităților, informații care să permită utilizatorilor să identifice produsul cu elemente digitale afectat, impactul vulnerabilităților, gravitatea acestora și informații care să ajute utilizatorii să remedieze vulnerabilitățile;	(4) după punerea la dispoziție a unei actualizări de securitate, să publice ***sau să comunice în alt mod, conform bunelor practici de la nivelul sectorului,*** informații cu privire la vulnerabilitățile remediate ***cunoscute***, inclusiv o descriere a vulnerabilităților, informații care să permită utilizatorilor să identifice produsul cu elemente digitale afectat, impactul vulnerabilităților, gravitatea acestora și informații ***clare și accesibile*** care să ajute utilizatorii să remedieze vulnerabilitățile;

Amendamentul 180

Propunere de regulament
Anexa I – partea 2 – paragraful 1 – litera 4 a (nouă)

Textul propus de Comisie	*Amendamentul*
	(4a) să partajeze și să comunice într-o manieră controlată informațiile privind remedierile și vulnerabilitățile, respectând principiile de „reducere a riscurilor” și secrete comerciale, prin dezvăluirea responsabilă a vulnerabilităților către actorii care pot acționa pentru a atenua vulnerabilitatea și asigurându-se că acestea nu sunt făcute publice, pentru a

	evita riscul de a-i informa din greșeală pe potențialii atacatori;

Amendamentul 181

Propunere de regulament
Anexa I – partea 2 – paragraful 1 – punctul 7

Textul propus de Comisie	*Amendamentul*
(7) să prevadă mecanisme de distribuire securizată a actualizărilor pentru produsele cu elemente digitale, pentru a se asigura că vulnerabilitățile exploatabile sunt remediate sau atenuate în timp util;	(7) să prevadă mecanisme de distribuire securizată a actualizărilor ***de securitate*** pentru produsele cu elemente digitale, pentru a se asigura că vulnerabilitățile exploatabile sunt remediate sau atenuate în timp util;

Amendamentul 182

Propunere de regulament
Anexa I – partea 2 – paragraful 1 – punctul 8

Textul propus de Comisie	*Amendamentul*
(8) să se asigure că, în cazul în care ***sunt disponibile*** corecții de securitate sau actualizări pentru abordarea problemelor de securitate identificate, ***acestea sunt difuzate*** fără întârziere și gratuit, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse.	(8) să se asigure că, în cazul în care ***pot fi puse la dispoziție în mod rezonabil*** corecții de securitate sau actualizări pentru abordarea problemelor de securitate identificate, ***există mijloace prin care utilizatorii le pot obține*** fără întârziere și gratuit ***sau cu un cost transparent și nediscriminatoriu***, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse.

Amendamentul 183

Propunere de regulament
Anexa II – paragraful 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
2. punctul de contact unde pot fi raportate și primite informații cu privire la vulnerabilitățile în materie de securitate	2. punctul ***unic*** de contact unde pot fi raportate și primite informații cu privire la vulnerabilitățile în materie de securitate

cibernetică ale produsului;	cibernetică ale produsului;

Amendamentul 184

Propunere de regulament
Anexa II – paragraful 1 – punctul 5

Textul propus de Comisie	*Amendamentul*
5. orice circumstanță cunoscută sau previzibilă legată de utilizarea produsului cu elemente digitale în conformitate cu scopul preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil care poate conduce la riscuri semnificative de securitate cibernetică;	***eliminat***

Amendamentul 185

Propunere de regulament
Anexa II – paragraful 1 – punctul 6

Textul propus de Comisie	*Amendamentul*
6. dacă și, după caz, unde poate fi accesată lista materialelor software;	6. dacă și, după caz, unde poate fi accesată lista materialelor software ***de către autoritățile competente***;

Amendamentul 186

Propunere de regulament
Anexa II – paragraful 1 – punctul 8

Textul propus de Comisie	*Amendamentul*
8. tipul de asistență tehnică de securitate oferită de producător și data până la care aceasta va fi furnizată***, cel puțin data până la care utilizatorii se pot aștepta să primească actualizări de securitate***;	8. tipul de asistență tehnică de securitate oferită de producător și data până la care aceasta va fi furnizată;

Amendamentul 187

Propunere de regulament
Anexa II – paragraful 1 – punctul 8 a (nou)

Textul propus de Comisie	*Amendamentul*
	8a. termenul preconizat de încetare a duratei de viață a produsului, care să afișeze în mod clar, acolo unde este cazul, pe ambalajul produsului, până când trebuie să asigure producătorul gestionarea eficace a vulnerabilităților și furnizarea actualizărilor de securitate;

Amendamentul 188

Propunere de regulament
Anexa I – paragraful 1 – punctul 9 – litera a

Textul propus de Comisie	*Amendamentul*
(a) măsurile necesare în timpul punerii în funcțiune inițiale și pe toată durata de viață a produsului pentru a se asigura o utilizare securizată a acestuia;	***eliminat***

Amendamentul 189

Propunere de regulament
Anexa I – paragraful 1 – punctul 9 – litera b

Textul propus de Comisie	*Amendamentul*
(b) modul în care modificările aduse produsului pot afecta securitatea datelor;	***eliminat***

Amendamentul 190

Propunere de regulament
Anexa I – paragraful 1 – punctul 9 – litera ca (nou)

Textul propus de Comisie	*Amendamentul*
	(ca) termenul preconizat de încetare a duratei de viață a produsului și până când asigură producătorul gestionarea eficace a vulnerabilităților și furnizarea

	actualizărilor de securitate;

Amendamentul 191

Propunere de regulament
Anexa I – paragraful 1 – punctul 9 – litera d

Textul propus de Comisie	*Amendamentul*
(d) dezafectarea securizată a produsului, inclusiv informații privind modul în care datele utilizatorilor pot fi eliminate în mod securizat.	***eliminat***

Amendamentul 192

Propunere de regulament
Anexa III – partea I – punctul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. Platforme de autentificare, autorizare și contabilizare;

Amendamentul 193

Propunere de regulament
Anexa III – partea I – punctul 15

Textul propus de Comisie	*Amendamentul*
15. Interfețe fizice de rețea;	15. Interfețe fizice ***și virtuale*** de rețea;

Amendamentul 194

Propunere de regulament
Anexa III – partea I – punctul 18

Textul propus de Comisie	*Amendamentul*
18. Routere, modemuri destinate conectării la internet și comutatoare care nu sunt incluse în clasa II;	***eliminat***

Amendamentul 195

Propunere de regulament
Anexa III – partea I – punctul 23

Textul propus de Comisie	*Amendamentul*
23. ***Internetul industrial al*** obiectelor neinclus în clasa II.	23. ***Produse industriale cu elemente digitale care pot fi considerate parte a internetului*** obiectelor neinclus în clasa II.

Amendamentul 196

Propunere de regulament
Anexa III – partea II – punctul 4

Textul propus de Comisie	*Amendamentul*
4. Firewall-uri, sisteme de detectare și/sau prevenire a intruziunilor destinate utilizării industriale;	4. Firewall-uri, ***portaluri de securitate,*** sisteme de detectare și/sau prevenire a intruziunilor destinate utilizării industriale;

Amendamentul 197

Propunere de regulament
Anexa III – partea II – punctul 7

Textul propus de Comisie	*Amendamentul*
7. Routere, modemuri destinate conectării la internet și ***comutatoare,*** de ***uz industrial***;	7. Routere, modemuri destinate conectării la internet***, comutatoare*** și ***alte noduri*** de ***rețea necesare pentru furnizarea serviciului de conectivitate***;

Amendamentul 198

Propunere de regulament
Anexa IV a (nouă)

Textul propus de Comisie	*Amendamentul*
	ANEXA IVa
	DECLARAȚIA UE DE ÎNCORPORARE PENTRU PRODUSELE CU

	ELEMENTE DIGITALE FINALIZATE PARȚIAL
	Declarația UE de încorporare pentru produsele cu elemente digitale finalizate parțial menționată la articolul 20a trebuie să conțină toate informațiile următoare:
	1. denumirea și tipul și orice informații suplimentare care permit identificarea unică a produsului cu elemente digitale finalizat parțial;
	2. obiectul declarației (identificarea produsului finalizat parțial pentru a permite trasabilitatea. dacă este cazul, poate fi inclusă o fotografie);
	3. o declarație potrivit căreia produsul finalizat parțial descris mai sus este conform cu legislația de armonizare relevantă a Uniunii;
	4. trimiteri la orice acte relevant și în cauză ale Uniunii, inclusiv referințele de publicare ale acestora;
	5. Informații suplimentare:
	Semnat pentru și în numele:
	……
	(locul și data emiterii):
	(numele, funcția) (semnătura):

Amendamentul 199

Propunere de regulament
Anexa V – paragraful 1 – punctul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) scopul preconizat al acestuia;	***eliminat***

Amendamentul 200

Propunere de regulament
Anexa V – paragraful 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
2. o descriere a proiectării, dezvoltării și producției produsului și a proceselor de gestionare a vulnerabilităților, inclusiv:	***eliminat***
(a) informații complete privind proiectarea și dezvoltarea produsului cu elemente digitale, inclusiv, dacă este cazul, desene și scheme și/sau o descriere a arhitecturii sistemului, care să explice modul în care componentele software se bazează unele pe altele sau se alimentează reciproc și se integrează în prelucrarea generală;	
(b) informații și specificații complete privind procesele de gestionare a vulnerabilităților instituite de producător, inclusiv lista materialelor software, politica coordonată de divulgare a vulnerabilităților, dovezi ale furnizării unei adrese de contact pentru raportarea vulnerabilităților și o descriere a soluțiilor tehnice alese pentru distribuirea securizată a actualizărilor;	
(c) informații și specificații complete privind procesele de producție și de monitorizare a produsului cu elemente digitale și validarea acestor procese;	

Amendamentul 201

Propunere de regulament
Anexa V – paragraful 1 – punctul 3

Textul propus de Comisie	*Amendamentul*
3. o evaluare a riscurilor de securitate cibernetică împotriva cărora este proiectat, dezvoltat, fabricat, livrat și întreținut produsul cu elemente digitale, astfel cum se prevede la articolul 10 din prezentul regulament;	3. ***o declarație sau o sinteză a riscurilor de securitate cibernetică împotriva cărora este proiectat, dezvoltat, produs, livrat și întreținut produsul cu elemente digitale, astfel cum se prevede la articolul 10 din prezentul regulament și, în urma unei cereri motivate din partea unei autorități de supraveghere a pieței, cu condiția ca acest lucru să fie necesar***

pentru ca autoritatea respectivă să poată verifica conformitatea cu cerințele esențiale prevăzute în anexa I, o evaluare ***detaliată*** a riscurilor de securitate cibernetică împotriva cărora este proiectat, dezvoltat, fabricat, livrat și întreținut produsul cu elemente digitale, astfel cum se prevede la articolul 10 din prezentul regulament;

ANEXĂ: LISTA ENTITĂȚILOR SAU A PERSOANELOR DE LA CARE RAPORTORUL A PRIMIT CONTRIBUȚII

Următoarea listă este întocmită în mod absolut voluntar, sub responsabilitatea exclusivă a raportorului. Raportorul a primit contribuții de la următoarele entități sau persoane la pregătirea proiectului de raport:

Entitatea și/sau persoana
Apple
BDI Federation of German Industries
BEUC
BSA The Software Alliance
Confederation of Danish Industries
Digital Europe
ETNO
Kaspersky
Microsoft
Samsung
TIC Council
Xiaomi

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Cerințe orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și modificarea Regulamentului (UE) 2019/1020
Referințe	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Comisie competentă Data anunțului în plen	ITRE 9.11.2022
Aviz emis de către Data anunțului în plen	IMCO 9.11.2022
Comisii asociate - data anunțului în plen	20.4.2023
Raportor/Raportoare pentru aviz Data numirii	Morten Løkkegaard 16.12.2022
Examinare în comisie	2.3.2023 25.4.2023 23.5.2023
Data adoptării	29.6.2023
Rezultatul votului final	+: 41 –: 1 0: 0
Membri titulari prezenți la votul final	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Biljana Borzan, Vlad-Marius Botoş, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Alexandra Geese, Maria Grapini, Svenja Hahn, Krzysztof Hetman, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Kateřina Konečná, Andrey Kovatchev, Maria-Manuel Leitão-Marques, Antonius Manders, Beata Mazurek, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, René Repasi, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Kim Van Sparrentak, Marion Walsmann
Membri supleanți prezenți la votul final	Marco Campomenosi, Maria da Graça Carvalho, Geoffroy Didier, Francisco Guerreiro, Tsvetelina Penkova, Catharina Rinzema, Kosma Złotowski
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Asger Christensen, Nicolás González Casares, Grzegorz Tobiszowski

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA SESIZATĂ PENTRU AVIZ

41	+
ECR	Beata Mazurek, Grzegorz Tobiszowski, Kosma Złotowski
ID	Alessandra Basso, Marco Campomenosi, Virginie Joron
NI	Miroslav Radačovský
PPE	Pablo Arias Echeverría, Maria da Graça Carvalho, Deirdre Clune, Geoffroy Didier, Krzysztof Hetman, Arba Kokalari, Andrey Kovatchev, Antonius Manders, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Marion Walsmann
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Asger Christensen, Svenja Hahn, Catharina Rinzema
S&D	Alex Agius Saliba, Biljana Borzan, Nicolás González Casares, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Tsvetelina Penkova, René Repasi, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Francisco Guerreiro, Kim Van Sparrentak

1	-
ECR	Eugen Jurzyca

0	0

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

PROCEDURA COMISIEI COMPETENTE

Titlu	Cerințe orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și modificarea Regulamentului (UE) 2019/1020
Referințe	COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)
Data prezentării în PE	15.9.2022
Comisie competentă Data anunțului în plen	ITRE 9.11.2022
Comisii sesizate pentru aviz Data anunțului în plen	IMCO 9.11.2022 LIBE 9.11.2022
Comisii asociate Data anunțului în plen	LIBE 20.4.2023 IMCO 20.4.2023
Raportori Data numirii	Nicola Danti 26.10.2022
Examinare în comisie	25.4.2023
Data adoptării	19.7.2023
Rezultatul votului final	+: 61 –: 1 0: 10
Membri titulari prezenți la votul final	Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Vasile Blaga, Michael Bloss, Paolo Borchia, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Ignazio Corrao, Beatrice Covassi, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Jens Geier, Nicolás González Casares, Christophe Grudler, Henrike Hahn, Robert Hajšel, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Zdzisław Krasnodębski, Andrius Kubilius, Thierry Mariani, Marisa Matias, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Maria Spyraki, Grzegorz Tobiszowski, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Membri supleanți prezenți la votul final	Damian Boeselager, Franc Bogovič, Francesca Donato, Matthias Ecke, Ladislav Ilčić, Elena Lizzi, Dace Melbārde, Jutta Paulus, Massimiliano Salini, Jordi Solé, Susana Solís Pérez, Ivan Štefanec, Nils Torvalds, Emma Wiesner
Membri supleanți [articolul 209 alineatul (7)] prezenți la votul final	Rosanna Conte, Arnaud Danjean, César Luena, Nicola Procaccini, Elżbieta Rafalska, Antonio Maria Rinaldi, Daniela Rondinelli, Nacho Sánchez Amor, Edina Tóth
Data depunerii	27.7.2023

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA COMPETENTĂ

61	+
ECR	Ladislav Ilčić, Zdzisław Krasnodębski, Nicola Procaccini, Elżbieta Rafalska, Grzegorz Tobiszowski
NI	Francesca Donato, Edina Tóth
PPE	François-Xavier Bellamy, Hildegard Bentele, Vasile Blaga, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Arnaud Danjean, Christian Ehler, Seán Kelly, Andrius Kubilius, Dace Melbārde, Markus Pieper, Massimiliano Salini, Maria Spyraki, Ivan Štefanec, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Christophe Grudler, Ivars Ijabs, Mauri Pekkarinen, Morten Petersen, Susana Solís Pérez, Nils Torvalds, Emma Wiesner
S&D	Beatrice Covassi, Matthias Ecke, Niels Fuglsang, Jens Geier, Nicolás González Casares, Robert Hajšel, Ivo Hristov, Romana Jerković, César Luena, Dan Nica, Tsvetelina Penkova, Daniela Rondinelli, Nacho Sánchez Amor, Patrizia Toia, Carlos Zorrinho
Verts/ALE	Michael Bloss, Damian Boeselager, Ignazio Corrao, Henrike Hahn, Niklas Nienass, Ville Niinistö, Jutta Paulus, Manuela Ripa, Jordi Solé

1	-
The Left	Marina Mesure

10	0
ECR	Johan Nissinen, Robert Roos
ID	Paolo Borchia, Rosanna Conte, Marie Dauchy, Elena Lizzi, Thierry Mariani, Antonio Maria Rinaldi
PPE	Sara Skyttedal
The Left	Marisa Matias

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