UNIUNEA EUROPEANĂ

PARLAMENTUL EUROPEAN **CONSILIUL**

Strasbourg, 23 octombrie 2024
(OR. en)

2022/0272(COD)
LEX 2395

PE-CONS 100/1/23
REV 1

CYBER 328
JAI 1731
DATAPROTECT 391
TELECOM 409
MI 1168
CSC 579
CSCI 215
CODEC 2601

REGULAMENT
AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
PRIVIND CERINȚELE ORIZONTALE
ÎN MATERIE DE SECURITATE CIBERNETICĂ
PENTRU PRODUSELE CU ELEMENTE DIGITALE
ȘI DE MODIFICARE A REGULAMENTELOR (UE) NR. 168/2013
ȘI (UE) 2019/1020, PRECUM ȘI A DIRECTIVEI (UE) 2020/1828
(REGULAMENTUL PRIVIND REZILIENȚA CIBERNETICĂ)

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

din 23 octombrie 2024

privind cerințele orizontale în materie de securitate cibernetică
pentru produsele cu elemente digitale și
de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020,
precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică)

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

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

după consultarea Comitetului Regiunilor,

hotărând în conformitate cu procedura legislativă ordinară[2],

---

1 JO C 100, 16.3.2023, p. 101.

2 Poziția Parlamentului European din 12 martie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 10 octombrie 2024.

întrucât:

(1) Securitatea cibernetică este una dintre principalele provocări pentru Uniune. 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 și a 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, precum 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 securizate 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 asistență pentru produsele cu elemente digitale puse la dispoziție pe piață.

(3) Dreptul relevant al Uniunii 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, dreptul Uniunii referitor la securitatea cibernetică, inclusiv Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[3] și Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[4], nu cuprinde în mod direct cerințele obligatorii de securitate a produselor cu elemente digitale.

---

[3] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

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

(4) Deși dreptul 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 unei serii de cerințe și obligații pentru tipuri similare de produse. Securitatea cibernetică a acestor produse are o dimensiune transfrontalieră deosebit de puternică, deoarece produsele cu elemente digitale fabricate într-un stat membru sau într-o țară terță 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 securitate juridică pentru utilizatori, organizații și întreprinderi, inclusiv microîntreprinderi și întreprinderi mici și mijlocii, în sensul definiției din anexa la Recomandarea 2003/361/CE a Comisiei[5]. Cadrul de reglementare al Uniunii ar trebui armonizat prin introducerea unor cerințe orizontale de securitate cibernetică pentru produsele cu elemente digitale. În plus, atât securitatea juridică pentru operatorii economici și pentru utilizatori, cât și o mai bună armonizare a pieței interne și proporționalitatea pentru microîntreprinderi și întreprinderile mici și mijlocii ar trebui să fie asigurate în întreaga Uniune, creând astfel condiții mai viabile pentru operatorii economici care doresc să intre pe piața respectivă.

[5] Recomandarea Comisiei 2003/361/CE din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii (JO L 124, 20.5.2003, p. 36).

(5) În ceea ce privește microîntreprinderile și întreprinderile mici și mijlocii, atunci când se stabilește categoria în care se încadrează o întreprindere, dispozițiile anexei la Recomandarea 2003/361/CE ar trebui să se aplice în întregime. Prin urmare, la calcularea numărului de angajați și a plafoanelor financiare care determină categoriile de întreprinderi, ar trebui să se aplice, de asemenea, dispozițiile articolului 6 din anexa la Recomandarea 2003/361/CE privind stabilirea datelor unei întreprinderi luând în considerare anumite tipuri de întreprinderi, cum ar fi întreprinderile partenere sau întreprinderile afiliate.

(6) Comisia ar trebui să ofere orientări pentru a sprijini operatorii economici, în special microîntreprinderile și întreprinderile mici și mijlocii, în aplicarea prezentului regulament. Aceste orientări ar trebui să cuprindă, printre altele, domeniul de aplicare al prezentului regulament, în special prelucrarea datelor la distanță și implicațiile sale pentru dezvoltatorii de software gratuite și cu sursă deschisă, aplicarea criteriilor utilizate pentru a stabili perioadele de asistență pentru produsele cu elemente digitale, interacțiunea dintre prezentul regulament și alte acte legislative ale Uniunii și conceptul de modificare substanțială.

(7) La nivelul Uniunii, diverse documente programatice și politice, cum ar fi comunicarea comună a Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 16 decembrie 2020 intitulată „Strategia de securitate cibernetică a UE pentru deceniul digital”, concluziile Consiliului din 2 decembrie 2020 privind securitatea cibernetică a dispozitivelor conectate și din 23 mai 2022 privind dezvoltarea poziției cibernetice a Uniunii Europene și rezoluția Parlamentului European din 10 iunie 2021 referitoare la Strategia de securitate cibernetică a UE pentru deceniul digital[6], au solicitat elaborarea de cerințe specifice în materie de securitate cibernetică ale Uniunii pentru produsele digitale sau conectate, mai multe țări terțe introducând măsuri de abordare a acestei chestiuni din proprie inițiativă. În raportul final al Conferinței privind viitorul Europei, 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 ambițios.

(8) 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.

---

[6] JO C 67, 8.2.2022, p. 81.

(9) 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 a fi 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 sunt proiectate și dezvoltate în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament. Această obligație se referă atât la produsele care pot fi conectate fizic prin interfețe hardware, cât și la 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 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 cu elemente digitale care sunt conectate doar indirect la alte dispozitive sau rețele.

(10) Prin stabilirea unor cerințe de securitate cibernetică pentru introducerea pe piață a produselor cu elemente digitale, se urmărește ca securitatea cibernetică a acestor produse să fie îmbunătățită atât pentru consumatori, cât și pentru întreprinderi. 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 și a componentelor lor. Sunt incluse, de asemenea, cerințe privind introducerea pe piață a produselor de consum cu elemente digitale destinate consumatorilor vulnerabili, cum ar fi jucăriile și sistemele de monitorizare pentru bebeluși. Produsele de consum cu elemente digitale clasificate în prezentul regulament ca produse importante cu elemente digitale prezintă un risc mai mare în materie de securitate cibernetică prin îndeplinirea unei funcții care prezintă un risc semnificativ de efecte negative în ceea ce privește intensitatea lor și capacitatea de a afecta sănătatea, securitatea sau siguranța utilizatorilor unor astfel de produse și ar trebui să facă obiectul unei proceduri mai stricte de evaluare a conformității. Acest lucru este valabil pentru produse cum ar fi produsele casnice inteligente cu funcționalități legate de securitate, inclusiv încuietorile inteligente pentru uși, sistemele de monitorizare a bebelușilor și sistemele de alarmă, jucăriile conectate și tehnologiile medicale portabile personale. În plus, procedurile mai stricte de evaluare a conformității la care trebuie supuse alte produse cu elemente digitale clasificate în prezentul regulament ca fiind produse importante sau esențiale cu elemente digitale vor contribui la împiedicarea potențialelor efecte negative ale exploatării vulnerabilităților asupra consumatorilor.

(11) Obiectivul prezentului regulament este de a asigura 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 ar trebui să fie definite ca fiind o procesare de date la distanță pentru care software-ul este conceput și dezvoltat de către sau în numele producătorului produsului cu elemente digitale în cauză și a cărui absență ar împiedica produsul cu elemente digitale să îndeplinească una dintre funcțiile sale. Această abordare asigură că astfel de produse sunt securizate în mod adecvat și integral de către producătorii lor, indiferent dacă datele sunt prelucrate sau stocate local pe dispozitivul utilizatorului sau la distanță de către producător. În același timp, prelucrarea sau stocarea la distanță intră în domeniul de aplicare al prezentului regulament numai în măsura în care este necesar ca un produs cu elemente digitale să îndeplinească funcțiile sale. O astfel de prelucrare sau stocare la distanță include situația în care o aplicație mobilă necesită accesul la o interfață de programare a aplicațiilor sau la o bază de date furnizată prin intermediul unui serviciu dezvoltat de producător. Într-un astfel de caz, serviciul intră în domeniul de aplicare al prezentului regulament ca soluție de prelucrare a datelor la distanță. Prin urmare, cerințele privind soluțiile de prelucrare a datelor la distanță care intră în domeniul de aplicare al prezentului regulament nu implică măsuri tehnice, operaționale sau organizatorice menite să gestioneze riscurile la adresa securității rețelelor și a sistemelor informatice ale unui producător în ansamblu.

(12) Soluțiile cloud constituie soluții de prelucrare a datelor la distanță în înțelesul prezentului regulament numai dacă corespund definiției prevăzute în prezentul regulament. De exemplu, funcționalitățile activate în cloud furnizate de un producător de dispozitive inteligente pentru casă care permit utilizatorilor să controleze dispozitivul de la distanță intră în domeniul de aplicare al prezentului regulament. Pe de altă parte, site-urile web care nu sprijină funcționalitatea unui produs cu elemente digitale sau serviciile de cloud concepute și dezvoltate în afara responsabilității unui producător de produse cu elemente digitale nu intră în domeniul de aplicare al prezentului regulament. Directiva (UE) 2022/2555 se aplică serviciilor de cloud computing și modelelor de servicii de cloud, precum software ca serviciu (SaaS), platforma ca serviciu (PaaS) sau infrastructura ca serviciu (IaaS). Entitățile care furnizează servicii de cloud computing în Uniune și care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) din articolul respectiv intră în domeniul de aplicare al directivei respective.

(13) În conformitate cu obiectivul prezentului regulament de a elimina obstacolele din calea liberei circulații a produselor cu elemente digitale, statele membre nu ar trebui să împiedice, 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. Prin urmare, în ceea ce privește aspectele armonizate prin prezentul regulament, statele membre nu pot impune cerințe suplimentare în materie de securitate cibernetică pentru punerea la dispoziție pe piață a produselor cu elemente digitale. Cu toate acestea, orice entitate, publică sau privată, poate stabili cerințe suplimentare față de cele prevăzute în prezentul regulament pentru achiziționarea sau utilizarea de produse cu elemente digitale în scopurile sale specifice și, prin urmare, poate alege să utilizeze produse cu elemente digitale care îndeplinesc cerințe de securitate cibernetică mai stricte sau mai specifice decât cele aplicabile pentru punerea la dispoziție pe piață în temeiul prezentului regulament. Fără a aduce atingere Directivelor 2014/24/UE[7] și 2014/25/UE[8] ale Parlamentului European și ale Consiliului, atunci când achiziționează produse cu elemente digitale, care trebuie să respecte cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament, inclusiv cele referitoare la gestionarea vulnerabilităților, statele membre ar trebui să se asigure că aceste cerințe sunt luate în considerare în procesul de achiziții publice și că se ține seama și de capacitatea producătorilor de a aplica în mod eficace măsuri de securitate cibernetică și de a gestiona amenințările cibernetice.

---

[7] 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).

[8] 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).

În plus, Directiva (UE) 2022/2555 stabilește măsuri de gestionare a riscurilor în materie de securitate cibernetică pentru entitățile esențiale și importante menționate la articolul 3 din directiva respectivă, care ar putea implica măsuri de securitate a lanțului de aprovizionare care necesită utilizarea de către astfel de entități a unor produse cu elemente digitale care îndeplinesc cerințe de securitate cibernetică mai stricte decât cele prevăzute în prezentul regulament. Prin urmare, în conformitate cu Directiva (UE) 2022/2555 și cu principiul său de armonizare minimă, statele membre pot impune cerințe suplimentare în materie de securitate cibernetică pentru utilizarea produselor din domeniul tehnologiei informației și comunicațiilor (TIC) de către entitățile esențiale sau importante în temeiul directivei respective, pentru a asigura un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste cerințe să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii. Aspectele care nu sunt reglementate de prezentul regulament pot include factori fără caracter tehnic referitori la produsele cu elemente digitale și la producătorii acestora. Prin urmare, statele membre pot stabili măsuri naționale, inclusiv restricții privind produsele cu elemente digitale sau furnizorii de astfel de produse, care să țină seama de factori fără caracter tehnic. Măsurile naționale referitoare la astfel de factori trebuie să respecte dreptul Uniunii.

(14) Prezentul regulament ar trebui să nu aducă atingere responsabilității statelor membre de a lua măsuri de protejare a securității naționale, în conformitate cu dreptul Uniunii. Statele membre ar trebui să poată supune produsele cu elemente digitale care sunt achiziționate sau utilizate în scopuri de securitate națională sau de apărare unor măsuri suplimentare, cu condiția ca astfel de măsuri să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii.

(15) Prezentul regulament se aplică operatorilor economici numai în ceea ce privește produsele cu elemente digitale puse la dispoziție pe piață și, prin urmare, furnizate pentru distribuție sau utilizare pe piața Uniunii în cursul unei activități comerciale. Furnizarea în cadrul unei activități comerciale ar putea fi caracterizată nu numai prin perceperea unui preț pentru un produs cu elemente digitale, ci și prin perceperea unui preț pentru serviciile de asistență tehnică, în cazul în care acestea nu servesc doar la recuperarea costurilor reale, prin intenția de monetizare, de exemplu prin furnizarea unei platforme software prin intermediul căreia producătorul monetizează alte servicii, prin impunerea ca o condiție de utilizare a prelucrării datelor cu caracter personal din alte motive decât exclusiv pentru îmbunătățirea securității, compatibilității sau interoperabilității software-ului, sau prin acceptarea unor donații care depășesc costurile asociate cu proiectarea, dezvoltarea și furnizarea unui produs cu elemente digitale. Acceptarea de donații fără intenția de a realiza un profit nu ar trebui să fie considerată o activitate comercială.

(16) Produsele cu elemente digitale furnizate ca parte a furnizării unui serviciu pentru care se percepe o taxă exclusiv pentru recuperarea costurilor reale direct legate de funcționarea serviciului respectiv, cum ar fi cazul anumitor produse cu elemente digitale furnizate de entitățile administrației publice, nu ar trebui să fie considerate, exclusiv din aceste motive, o activitate comercială în sensul prezentului regulament. În plus, produsele cu elemente digitale care sunt elaborate sau modificate de o entitate a administrației publice exclusiv pentru uz propriu nu ar trebui considerate a fi puse la dispoziție pe piață în înțelesul prezentului regulament.

(17) 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. Pentru a favoriza dezvoltarea și utilizarea de software liber și cu sursă deschisă, în special de către microîntreprinderi și întreprinderi mici și mijlocii, inclusiv start-up-uri, persoane fizice, organizații fără scop lucrativ și organizații de cercetare academică, aplicarea prezentului regulament la produsele cu elemente digitale care se califică drept software liber și cu sursă deschisă furnizate în vederea distribuirii sau utilizării în cadrul unei activități comerciale ar trebui să țină seama de natura diferitelor modele de dezvoltare a software-ului distribuit și dezvoltat în temeiul licențelor de software liber și cu sursă deschisă.

(18) „Software liber și cu sursă deschisă” înseamnă un software al cărui cod sursă este partajat în mod deschis și care este pus la dispoziție sub licență liberă și cu sursă deschisă ce prevede toate drepturile necesare pentru ca software-ul să fie accesibil, utilizabil, modificabil și redistribuibil în mod gratuit. Software-ul liber și cu sursă deschisă este dezvoltat, menținut și distribuit în mod deschis prin platforme online. În ceea ce privește operatorii economici care intră în domeniul de aplicare al prezentului regulament, numai software-ul liber și cu sursă deschisă pus la dispoziție pe piață și, prin urmare, furnizat pentru distribuție sau utilizare în cursul unei activități comerciale ar trebui să intre în domeniul de aplicare al prezentului regulament. Circumstanțele în care a fost dezvoltat produsul cu elementele digitale sau modul în care a fost finanțată dezvoltarea nu ar trebui, prin urmare, să fie luate în considerare atunci când se stabilește natura comercială sau necomercială a activității respective. Mai precis, în sensul prezentului regulament și în ceea ce privește operatorii economici care intră în domeniul său de aplicare, pentru a se asigura că există o distincție clară între etapele de dezvoltare și de furnizare, furnizarea de produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care nu sunt monetizate de producătorii lor nu ar trebui să fie considerată a fi o activitate comercială. În plus, furnizarea de produse cu elemente digitale care se califică drept componente software gratuite și cu sursă deschisă destinate integrării de către alți producători în propriile produse cu elemente digitale ar trebui să fie considerată drept punere la dispoziție pe piață numai dacă componenta este monetizată de producătorul său inițial. De exemplu, simplul fapt că un produs software cu sursă deschisă cu elemente digitale primește sprijin financiar din partea producătorilor sau că producătorii contribuie la dezvoltarea unui astfel de produs nu ar trebui să determine în sine că activitatea este de natură comercială.

În plus, simpla prezență a diseminărilor periodice nu ar trebui, în sine, să ducă la concluzia că un produs cu elemente digitale este furnizat în cursul unei activități comerciale. În cele din urmă, în sensul prezentului regulament, dezvoltarea de produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă de către organizații non-profit nu ar trebui să fie considerată o activitate comercială, cu condiția ca organizația să fie înființată astfel încât să se asigure că toate veniturile după costuri sunt utilizate pentru a atinge obiective non-profit. Prezentul regulament nu se aplică persoanelor fizice sau juridice care contribuie cu cod sursă la produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care nu se află în responsabilitatea lor.

(19) Având în vedere importanța pentru securitatea cibernetică a multor produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care sunt publicate, dar nu sunt puse la dispoziție pe piață în înțelesul prezentului regulament, persoanele juridice care oferă sprijin susținut pentru dezvoltarea unor astfel de produse care sunt destinate activităților comerciale și care joacă un rol principal în asigurarea viabilității acestor produse (denumiți în continuare „administratori de software cu sursă deschisă”) ar trebui să fie supuse unui regim de reglementare facil și adaptat. Administratorii de software cu sursă deschisă includ anumite fundații, precum și entități care dezvoltă și publică software gratuit și cu sursă deschisă într-un context de afaceri, inclusiv entitățile fără scop lucrativ. Regimul de reglementare ar trebui să țină seama de natura lor specifică și de compatibilitatea lor cu tipul de obligații impuse. Acesta ar trebui să cuprindă numai produsele cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care sunt în cele din urmă destinate activităților comerciale, cum ar fi integrarea în servicii comerciale sau în produse monetizate cu elemente digitale. În sensul acestui regim de reglementare, intenția de integrare în produse monetizate cu elemente digitale include cazurile în care producătorii care integrează o componentă în propriile produse cu elemente digitale fie contribuie în mod regulat la dezvoltarea componentei respective, fie oferă asistență financiară periodică pentru a asigura continuitatea unui produs software. Furnizarea de asistență susținută pentru dezvoltarea unui produs cu elemente digitale include, fără a se limita la acestea, găzduirea și gestionarea platformelor de colaborare pentru dezvoltarea de software, găzduirea de coduri sursă sau software, reglementarea sau gestionarea produselor cu elemente digitale care se califică drept software gratuit și cu sursă deschisă, precum și coordonarea dezvoltării unor astfel de produse. Având în vedere că regimul de reglementare facil și adaptat nu îi supune pe cei care acționează ca administratori de software cu sursă deschisă acelorași obligații ca pe cei care acționează ca producători în temeiul prezentului regulament, acestora nu ar trebui să li se permită să aplice marcajul CE pe produsele cu elemente digitale a căror dezvoltare o sprijină.

(20) Simplul fapt de a găzdui produse cu elemente digitale în depozite deschise, inclusiv prin intermediul managerilor de pachete sau al platformelor de colaborare, nu constituie în sine punerea la dispoziție pe piață a unui produs cu elemente digitale. Furnizorii de astfel de servicii ar trebui să fie considerați distribuitori numai dacă pun la dispoziție pe piață un astfel de software și, prin urmare, îl furnizează pentru a fi distribuit sau utilizat pe piața Uniunii în cadrul unei activități comerciale.

(21) Pentru a sprijini și a facilita diligența necesară a producătorilor care integrează componente software libere și cu sursă deschisă care nu sunt supuși cerințelor esențiale de securitate cibernetică prevăzute în prezentul regulament în produsele lor cu elemente digitale, Comisia ar trebui să poată institui programe voluntare de atestare a securității, fie printr-un act delegat care completează prezentul regulament, fie solicitând un sistem european de certificare de securitate cibernetică în temeiul articolului 48 din Regulamentul (UE) 2019/881, care să țină seama de particularitățile modelelor de dezvoltare de software gratuite și cu sursă deschisă. Programele de atestare a securității ar trebui să fie concepute astfel încât nu numai persoanele fizice sau juridice care dezvoltă sau contribuie la dezvoltarea unui produs cu elemente digitale care se califică drept software liber și cu sursă deschisă să poată iniția sau finanța o atestare de securitate, ci și părți terțe, cum ar fi producătorii care integrează astfel de produse în propriile produse cu elemente digitale, utilizatorii sau administrațiile publice ale Uniunii și cele naționale.

(22) Având în vedere obiectivele publice în materie de securitate cibernetică ale prezentului regulament și pentru a îmbunătăți conștientizarea situației de către statele membre în ceea ce privește dependența Uniunii de componente software și, în special, de componente software potențial gratuite și cu sursă deschisă, un grup specific de cooperare administrativă (ADCO) instituit prin prezentul regulament ar trebui să poată decide să efectueze în comun o evaluare a dependenței Uniunii. Autoritățile de supraveghere a pieței ar trebui să poată solicita producătorilor de categorii de produse cu elemente digitale stabilite de ADCO să prezinte o listă a materialelor software (SBOM) pe care le-au generat în temeiul prezentului regulament. Pentru a proteja confidențialitatea SBOM, autoritățile de supraveghere a pieței ar trebui să transmită ADCO informații pertinente cu privire la dependențe într-un mod anonimizat și agregat.

(23) Eficacitatea punerii în aplicare a prezentului regulament va depinde, de asemenea, de disponibilitatea unor competențe adecvate în materie de securitate cibernetică. La nivelul Uniunii, diverse documente programatice și politice, inclusiv comunicarea Comisiei din 18 aprilie 2023 intitulată „Eliminarea deficitului de talente în materie de securitate cibernetică pentru a stimula competitivitatea, creșterea și reziliența UE” și concluziile Consiliului din 22 mai 2023 privind politica UE în domeniul apărării cibernetice au recunoscut lacunele în materie de competențe în materie de securitate cibernetică din Uniune și necesitatea de a aborda cu prioritate astfel de provocări, atât în sectorul public, cât și în cel privat. În vederea asigurării unei puneri în aplicare eficace a prezentului regulament, statele membre ar trebui să se asigure că sunt disponibile resurse adecvate pentru personalul corespunzător al autorităților de supraveghere a pieței și al organismelor de evaluare a conformității pentru a-și îndeplini sarcinile astfel cum sunt prevăzute în prezentul regulament. Aceste măsuri ar trebui să sporească mobilitatea forței de muncă în domeniul securității cibernetice și parcursurile lor profesionale asociate. Acestea ar trebui, de asemenea, să contribuie la creșterea rezilienței și a incluziunii forței de muncă din domeniul securității cibernetice, inclusiv în ceea ce privește genul. Prin urmare, statele membre ar trebui să ia măsuri pentru a se asigura că sarcinile respective sunt îndeplinite de profesioniști instruiți în mod adecvat, care dețin competențele necesare în materie de securitate cibernetică. În mod similar, producătorii ar trebui să se asigure că personalul lor are competențele necesare pentru a-și îndeplini obligațiile astfel cum sunt prevăzute în prezentul regulament. Statele membre și Comisia, în conformitate cu prerogativele și competențele lor și cu sarcinile specifice care le sunt conferite prin prezentul regulament, ar trebui să ia măsuri pentru a sprijini producătorii, în special microîntreprinderile și întreprinderile mici și mijlocii, inclusiv întreprinderile nou-înființate, inclusiv în domenii precum dezvoltarea competențelor, în scopul respectării obligațiilor care le revin astfel cum sunt prevăzute în prezentul regulament. În plus, întrucât Directiva (UE) 2022/2555 impune statelor membre să adopte politici de promovare și dezvoltare a instruirii privind competențele în materie de securitate cibernetică și competențele de securitate cibernetică, ca parte a strategiilor lor naționale de securitate cibernetică, statele membre pot, de asemenea, avea în vedere, atunci când adoptă astfel de strategii, să abordeze nevoile în materie de competențe în materie de securitate cibernetică care rezultă din prezentul regulament, inclusiv cele legate de recalificare și perfecționare.

(24) 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 astfel cum sunt menționate la articolul 3 din directiva respectivă, inclusiv de furnizori de infrastructură digitală care sprijină funcțiile de bază ale internetului deschis, asigură accesul la internet și furnizează 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.

(25) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului[9] stabilește norme privind dispozitivele medicale, iar Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului[10] stabilește norme privind dispozitivele medicale pentru diagnostic in vitro. Aceste 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, care le oferă producătorilor de dispozitive medicale, inclusiv de dispozitive pentru diagnostic in vitro, orientări privind modul de îndeplinire a tuturor cerințelor esențiale relevante prevăzute în 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.

---

[9] 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).

[10] 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).

(26) Produsele cu elemente digitale care sunt dezvoltate sau modificate exclusiv în scopuri de securitate națională sau de apărare sau produsele concepute în mod specific pentru prelucrarea informațiilor clasificate nu intră în domeniul de aplicare al prezentului regulament. Statele membre sunt încurajate să asigure același nivel de protecție sau un nivel mai ridicat de protecție pentru produsele respective față de nivelul de protecție pentru produsele cu elemente digitale care intră în domeniul de aplicare al prezentului regulament.

(27) Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului[11] 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, îndeosebi Regulamentul ONU nr. 155 – Dispoziții uniforme referitoare la omologarea vehiculelor în ceea ce privește securitatea cibernetică și sistemul de gestionare a securității cibernetice[12] și prevăzând proceduri specifice de evaluare a conformității.

---

[11] 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).

[12] JO L 82, 9.3.2021, p. 30.

În domeniul aviației, principalul obiectiv al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului[13] este stabilirea și menținerea unui nivel ridicat și uniform al siguranței aviației civile în Uniune. Regulamentul respectiv creează un cadru pentru cerințele esențiale de navigabilitate pentru produsele, piesele și echipamentele aeronautice, printre care și software-ul, care include obligațiile de protecție împotriva amenințărilor la adresa securității informațiilor. Procesul de certificare în temeiul Regulamentului (UE) 2018/1139 garantează nivelul de asigurare vizat de prezentul regulament. 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 ar trebui să facă obiectul cerințelor esențiale de securitate cibernetică și al procedurilor de evaluare a conformității prevăzute în prezentul regulament.

[13] 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).

(28) 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 vizate de cerințele esențiale de securitate cibernetică 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 vizate de cerințele esențiale de securitate cibernetică prevăzute în 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 cel puțin același nivel de protecție ca cel prevăzut de prezentul regulament. Comisia ar trebui să fie împuternicită să adopte acte delegate pentru a completa prezentul regulament prin identificarea produselor și a normelor respective. În ceea ce privește dreptul Uniunii în vigoare, în cazul în care o astfel de limitare sau excludere ar trebui să se aplice, prezentul regulament cuprinde dispoziții specifice pentru a clarifica relația sa cu dreptul Uniunii respectiv.

(29) Pentru a se asigura că produsele cu elemente digitale puse la dispoziție pe piață pot fi reparate în mod eficace și că durabilitatea lor poate fi prelungită, ar trebui să se prevadă o exceptare pentru piesele de schimb. Această exceptare ar trebui să cuprindă atât piesele de schimb care au scopul de a repara produsele preexistente puse la dispoziție înainte de data aplicării prezentului regulament, cât și piesele de schimb care au făcut deja obiectul unei proceduri de evaluare a conformității în temeiul prezentului regulament.

(30) Regulamentul delegat (UE) 2022/30 al Comisiei[14] precizează că anumitor echipamente radio li se aplică o serie de cerințe esențiale prevăzute la articolul 3 alineatul (3) literele (d), (e) și (f) din Directiva 2014/53/UE a Parlamentului European și a Consiliului[15], referitoare la prejudicierea rețelei și utilizarea abuzivă a resurselor rețelei, datele cu caracter personal și viața privată, precum și la fraudă. Decizia de punere în aplicare C(2022)5637 a Comisiei din 5 august 2022 privind o cerere de standardizare adresată Comitetului European de Standardizare și Comitetului European de Standardizare în Electrotehnică stabilește cerințe pentru elaborarea unor standarde specifice care să detalieze modul în care ar trebui să fie abordate respectivele cerințe esențiale. Cerințele esențiale de securitate cibernetică 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 de securitate cibernetică prevăzute de prezentul regulament sunt aliniate la obiectivele cerințelor pentru standardele specifice incluse în cererea de standardizare respectivă. Prin urmare, atunci când Comisia abrogă sau 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 atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a prezentului regulament. În cursul perioadei de tranziție pentru aplicarea prezentului regulament, Comisia ar trebui să ofere orientări producătorilor care sunt supuși prezentului regulament și, de asemenea, Regulamentului delegat (UE) 2022/30, pentru a facilita demonstrarea respectării celor două regulamente.

---

14 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).

15 Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62).

(31) Directiva (UE) 2024/... a Parlamentului European și a Consiliului[16+] este complementară prezentului regulament. Directiva respectivă 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.

---

16 Directiva (UE) 2024/... a Parlamentului European și a Consiliului din ... privind răspunderea pentru produsele cu defecte și de abrogare a Directivei 85/374/CEE a Consiliului (JO L, ..., ELI: ...).

\+ JO: a se introduce în text numărul directivei cuprinse în documentul PE CONS 7/24 (2022/0302(COD)) și a se introduce numărul, data și referința de publicare a respectivei directive în nota de subsol.

(32) Prezentul regulament nu ar trebui să aducă atingere Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului[17], 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 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 urmează, 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 aspectelor legate de securitatea cibernetică prin cooperarea dintre Comisie, organizațiile europene de standardizare, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Comitetul european pentru protecția datelor instituit prin Regulamentul (UE) 2016/679 și autoritățile naționale de supraveghere a protecției datelor. De asemenea, ar trebui să fie 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 aplicarea legislației Uniunii în materie de protecție a datelor.
De asemenea, acestea din urmă ar trebui să aibă acces la informațiile relevante pentru îndeplinirea sarcinilor lor.

---

[17] 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).

(33) În măsura în care produsele lor intră în domeniul de aplicare al prezentului regulament, furnizorii de portofele europene pentru identitatea digitală, astfel cum se menționează la articolul 5a alineatul (2) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului[18], ar trebui să respecte atât cerințele esențiale orizontale de securitate cibernetică prevăzute în prezentul regulament, cât și cerințele de securitate specifice prevăzute la articolul 5a din Regulamentul (UE) nr. 910/2014. Pentru a facilita conformitatea, furnizorii de portofele ar trebui să fie în măsură să demonstreze conformitatea portofelelor europene pentru identitatea digitală cu cerințele prevăzute în prezentul regulament și, respectiv, în Regulamentul (UE) nr. 910/2014, prin certificarea produselor lor în cadrul unui sistem european de certificare a securității cibernetice instituit în temeiul Regulamentului (UE) 2019/881 și pentru care Comisia a specificat, prin intermediul unor acte delegate, o prezumție de conformitate cu prezentul regulament, în măsura în care certificatul sau părți ale acestuia cuprind cerințele respective.

---

[18] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73).

(34) Atunci când integrează componente provenite de la părți terțe în produse cu elemente digitale în faza de proiectare și dezvoltare, producătorii ar trebui să exercite diligența necesară în ceea ce privește componentele respective, inclusiv componentele software gratuite și cu sursă deschisă care nu au fost puse la dispoziție pe piață, pentru a se asigura că produsele sunt proiectate, dezvoltate și produse în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament. Nivelul corespunzător de diligență necesară depinde de natura și de nivelul riscului de securitate cibernetică asociat cu o anumită componentă și, în acest scop, ar trebui să ia în considerare una sau mai multe dintre următoarele acțiuni: verificarea, după caz, a faptului că producătorul unei componente a demonstrat conformitatea cu prezentul regulament, inclusiv prin verificarea dacă componenta poartă deja marcajul CE; verificarea faptului că o componentă primește actualizări de securitate periodice, de exemplu prin verificarea istoricului actualizărilor sale de securitate; verificarea faptului că o componentă nu prezintă vulnerabilități înregistrate în baza de date europeană a vulnerabilităților instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555 sau în alte baze de date accesibile publicului privind vulnerabilitățile; sau efectuarea de teste de securitate suplimentare. Obligațiile de gestionare a vulnerabilităților prevăzute în prezentul regulament, pe care producătorii trebuie să le respecte atunci când introduc pe piață un produs cu elemente digitale și pentru perioada de asistență, se aplică tuturor produselor cu elemente digitale, inclusiv tuturor componentelor integrate. În cazul în care, în exercitarea diligenței necesare, producătorul produsului cu elemente digitale identifică o vulnerabilitate într-o componentă, inclusiv într-o componentă gratuită și cu sursă deschisă, acesta ar trebui să informeze persoana sau entitatea care produce sau întreține componenta, să abordeze și să remedieze vulnerabilitatea și, dacă este cazul, să furnizeze persoanei sau entității respective soluția de securitate aplicată.

(35) Imediat după perioada de tranziție pentru aplicarea prezentului regulament, este posibil ca un producător al unui produs cu elemente digitale care integrează una sau mai multe componente provenite de la părți terțe cărora li se aplică, de asemenea, prezentul regulament să nu fie în măsură să verifice, în cadrul obligației sale de diligență necesară, dacă producătorii componentelor respective au demonstrat conformitatea cu prezentul regulament prin verificarea, de exemplu, dacă componentele poartă deja marcajul CE. Acest lucru se poate întâmpla atunci când componentele au fost integrate înainte ca prezentul regulament să devină aplicabil producătorilor componentelor respective. Într-un astfel de caz, un producător care integrează astfel de componente ar trebui să exercite diligența necesară prin alte mijloace.

(36) 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 târguri comerciale, expoziții și demonstrații sau evenimente similare, statele membre nu ar trebui să împiedice prezentarea sau utilizarea unui produs cu elemente digitale care nu este conform cu prezentul regulament, inclusiv a prototipurilor sale, cu condiția ca un anunț vizibil să indice în mod clar că produsul nu este conform cu prezentul regulament și că nu poate fi pus la dispoziție pe piață înainte de asigurarea conformității.

(37) Pentru a se asigura că producătorii pot lansa software în scopuri de testare înainte de a-și supune produsele cu elemente digitale unei evaluări a conformității, statele membre nu ar trebui să împiedice punerea la dispoziție a software-ului nefinalizat, cum ar fi versiunile alfa, beta sau cele candidate la lansare, cu condiția ca software-ul nefinalizat să fie pus 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 prevăzute în 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.

(38) 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 de securitate cibernetică pentru astfel de produse. Respectivele cerințe esențiale de securitate cibernetică, inclusiv cerințele de gestionare a vulnerabilităților, se aplică fiecărui produs individual cu elemente digitale atunci când este introdus pe piață, indiferent dacă produsul cu elemente digitale este fabricat ca unitate individuală sau în serie. De exemplu, pentru un tip de produs, fiecare produs individual cu elemente digitale ar fi trebuit să primească toate corecțiile de securitate sau actualizările disponibile pentru a soluționa problemele de securitate relevante atunci când este introdus pe piață. În cazul în care produsele cu elemente digitale sunt modificate ulterior, prin mijloace fizice sau digitale, într-un mod care nu este prevăzut de producător în evaluarea inițială a riscurilor și care poate implica faptul că acestea nu mai îndeplinesc cerințele esențiale de securitate cibernetică relevante, modificarea ar trebui să fie considerată substanțială. De exemplu, reparațiile ar putea fi asimilate operațiunilor de întreținere, cu condiția ca acestea să nu modifice un produs cu elemente digitale deja introdus pe piață astfel încât să poată fi afectată conformitatea cu cerințele aplicabile sau să poată fi schimbată scopul preconizat pentru care a fost evaluat produsul.

(39) 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 scopul preconizat al produsului respectiv, iar aceste modificări nu au fost prevăzute de producător în evaluarea inițială a riscurilor sau dacă natura pericolului s-a schimbat sau nivelul de risc în materie de securitate cibernetică a crescut ca urmare a actualizării software-ului, iar versiunea actualizată a produsului este pusă la dispoziție pe piață. Dacă o actualizare de securitate, care este concepută pentru a reduce nivelul riscului în materie de securitate cibernetică al unui produs cu elemente digitale, nu modifică scopul preconizat al unui produs cu elemente digitale, aceasta nu este considerată a fi o modificare substanțială. Aceasta include, de obicei, situațiile în care o actualizare de securitate implică doar ajustări minore ale codului sursă. De exemplu, acesta ar putea fi cazul în care o actualizare de securitate abordează o vulnerabilitate cunoscută, inclusiv prin modificarea funcțiilor sau a performanței unui produs cu elemente digitale, cu unicul scop de a reduce nivelul riscului în materie de securitate cibernetică. În mod similar, o actualizare minoră a funcționalității, cum ar fi o îmbunătățire vizuală, adăugarea de noi pictograme sau versiuni lingvistice la interfața pentru utilizatori, nu ar trebui, în general, să fie considerată o modificare substanțială. În schimb, în cazul în care o actualizare de caracteristici modifică funcțiile inițiale preconizate sau tipul sau performanța unui produs cu elemente digitale și îndeplinesc criteriile menționate, aceasta ar trebui să fie considerată o modificare substanțială, deoarece adăugarea de noi caracteristici conduce, de regulă, la o suprafață de atac mai largă, sporind astfel riscul în materie de securitate cibernetică. Un exemplu ar putea fi cazul în care un nou element de intrare este adăugat unei aplicații, impunând producătorului să asigure o validare adecvată a datelor de intrare. Atunci când se evaluează dacă o actualizare a caracteristicilor este considerată a fi o modificare substanțială, nu este relevant dacă este furnizată ca actualizare separată sau în combinație, cu actualizare de securitate. Comisia ar trebui să emită orientări cu privire la modul de stabilire a ceea ce constituie o modificare substanțială.

(40) Ținând seama de caracterul iterativ al dezvoltării de software, producătorii care au introdus pe piață versiuni ulterioare ale unui produs software, ca urmare a unei modificări substanțiale ulterioare a produsului respectiv, ar trebui să poată furniza actualizări de securitate pentru perioada de asistență numai pentru versiunea produsului software pe care au introdus-o ultima dată pe piață. Aceștia ar trebui să poată face acest lucru numai dacă utilizatorii versiunilor anterioare relevante ale produsului au acces gratuit la ultima versiune a produsului introdusă pe piață și nu li se impută costuri suplimentare pentru a ajusta mediul hardware sau software în care utilizează produsul. Acesta ar putea fi, de exemplu, cazul în care o modernizare a sistemului de operare a unui calculator de tip desktop nu necesită hardware nou, cum ar fi o unitate centrală de procesare mai rapidă sau o memorie mai mare. Cu toate acestea, producătorul ar trebui să respecte în continuare, pentru perioada de asistență, alte cerințe de gestionare a vulnerabilităților, cum ar fi existența unei politici privind divulgarea coordonată a vulnerabilităților sau măsuri de facilitare a schimbului de informații cu privire la potențialele vulnerabilități pentru toate versiunile ulterioare modificate substanțial ale produsului software introdus pe piață. Producătorii ar trebui să poată furniza actualizări minore de securitate sau de funcționalitate care nu constituie o modificare substanțială numai pentru cea mai recentă versiune sau subversiune a unui produs software care nu a fost modificat substanțial. În același timp, dacă un produs hardware, cum ar fi un telefon inteligent, nu este compatibil cu cea mai recentă versiune a sistemului de operare cu care a fost livrat inițial, producătorul ar trebui să continue să furnizeze actualizări de securitate cel puțin pentru cea mai recentă versiune compatibilă a sistemului de operare pentru perioada de asistență.

(41) În conformitate cu conceptul stabilit de comun acord a modificării substanțiale pentru produsele reglementate de legislația de armonizare a Uniunii, atunci când apare o modificare substanțială care ar putea afecta conformitatea produsului cu elemente digitale 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, o modificare care ar putea duce la o modificare substanțială ar trebui să fie notificate părții terțe.

(42) Atunci când un produs cu elemente digitale face obiectul „recondiționării”, „întreținerii” și „reparării”, în sensul definiției de la articolul 2 punctele 18, 19 și 20 din Regulamentul (UE) 2024/1781 al Parlamentului European și al Consiliului[19], acestea nu conduc neapărat la o modificare substanțială a produsului, de exemplu în cazul în care scopul și funcționalitățile preconizate nu sunt modificate, iar nivelul de risc rămâne neafectat. Cu toate acestea, modernizarea unui produs cu elemente digitale de către producător ar putea duce la modificări ale proiectării și dezvoltării produsului respectiv și ar putea afecta, prin urmare, scopul pentru care a fost conceput și conformitatea produsului cu cerințele stabilite în prezentul regulament.

[19] Directiva (UE) 2024/1781 a Parlamentului European și a Consiliului din 13 iunie 2024 de instituire a unui cadru pentru stabilirea cerințelor în materie de proiectare ecologică pentru produsele sustenabile, de modificare a Directivei (UE) 2020/1828 și a Regulamentului (UE) 2023/1542 și de abrogare a Directivei 2009/125/CE (JO L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

(43) Produsele cu elemente digitale ar trebui considerate a fi importante 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 unei funcții care prezintă un risc semnificativ de efecte negative în ceea ce privește intensitatea și capacitatea de a perturba, controla sau cauza daune unui număr mare de alte produse sau în ceea ce privește sănătatea, securitatea sau siguranța utilizatorilor săi prin manipulare directă, cum ar fi o funcție de sistem central, inclusiv gestionarea rețelei, controlul configurației, virtualizarea sau prelucrarea datelor cu caracter personal. În special, vulnerabilitățile produselor cu elemente digitale care au o funcționalitate legată de securitatea cibernetică, de exemplu boot managers, 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, dacă produsul îndeplinește în primul rând o funcție de sistem central, inclusiv gestionarea rețelei, controlul configurației, virtualizarea sau prelucrarea datelor cu caracter personal.

(44) Anumite categorii de produse 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 importante cu elemente digitale ar trebui să fie împărțite în două clase, în funcție de nivelul de risc de securitate cibernetică legat de aceste categorii de produse. Un incident care implică produse importante cu elemente digitale care se încadrează în clasa II ar putea avea un impact negativ mai mare decât un incident care implică produse importante cu elemente digitale care se încadrează în clasa I, de exemplu din cauza naturii funcției lor legate de securitatea cibernetică sau a îndeplinirii unei alte funcții care prezintă un risc însemnat de efecte negative. Ca o indicație a acestor efecte negative mai mari, produsele cu elemente digitale care se încadrează în clasa II ar putea fie să îndeplinească o funcționalitate legată de securitatea cibernetică, fie o altă funcție care prezintă un risc semnificativ de efecte negative, mai mare decât pentru cele enumerate în clasa I, fie să îndeplinească ambele criterii menționate anterior. Produsele importante cu elemente digitale care se încadrează în clasa II ar trebui, prin urmare, să facă obiectul unei proceduri mai stricte de evaluare a conformității.

(45) Produsele importante cu elemente digitale, astfel cum sunt menționate în prezentul regulament ar trebui înțelese ca fiind produsele care au funcționalitatea de bază a unei categorii de produse importante cu elemente digitale care este prevăzută în prezentul regulament. De exemplu, prezentul regulament stabilește categorii de produse importante cu elemente digitale care sunt definite prin funcționalitatea lor de bază ca firewalls-urile sau sistemele de detectare sau prevenire a intruziunilor din clasa II. În consecință, firewalls-urile și sistemele de detectare sau prevenire a intruziunilor fac obiectul evaluării obligatorii de conformitate de către terți. Acest lucru nu este valabil pentru alte produse cu elemente digitale care nu sunt clasificate ca produse importante cu elemente digitale care pot integra firewalls-uri sau sisteme de detectare sau de prevenire a intruziunilor. Comisia ar trebui să adopte un act de punere în aplicare pentru a preciza descrierea tehnică a categoriilor de produse importante cu elemente digitale care se încadrează în clasele I și II, astfel cum sunt prevăzute în prezentul regulament.

(46) Categoriile de produse critice cu elemente digitale prevăzute în prezentul regulament au o funcționalitate legată de securitatea cibernetică și îndeplinesc o funcție care prezintă un risc semnificativ de efecte negative în ceea ce privește intensitatea și capacitatea de a perturba, controla sau cauza daune unui număr mare de alte produse cu elemente digitale prin manipulare directă. În plus, aceste categorii de produse cu elemente digitale sunt considerate dependențe critice pentru entitățile esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555. Categoriile de produse critice cu elemente digitale prevăzute într-o anexă la prezentul regulament, datorită importanței lor critice, folosesc deja pe scară largă diverse forme de certificare și fac, de asemenea, obiectul sistemului european de certificare de securitate cibernetică bazat pe criterii comune (EUCC), prevăzut de Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei[20]. Prin urmare, pentru a asigura o protecție adecvată comună în materie de securitate cibernetică a produselor critice cu elemente digitale în Uniune, ar putea fi adecvat și proporțional ca astfel de categorii de produse să fie supuse, prin intermediul unui act delegat, unei certificări europene obligatorii de securitate cibernetică dacă există deja un sistem european relevant de certificare a securității cibernetice privind produsele respective, iar Comisia a efectuat o evaluare a impactului potențial asupra pieței al certificării obligatorii preconizate. Evaluarea respectivă ar trebui să ia în considerare atât cererea, cât și oferta, inclusiv dacă există o cerere suficientă de produse cu elemente digitale în cauză atât din partea statelor membre, cât și a utilizatorilor pentru ca certificarea europeană de securitate cibernetică să fie necesară, precum și scopurile în care produsele cu elemente digitale sunt destinate a fi utilizate, inclusiv dependența critică de acestea a entităților esențiale astfel cum sunt menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555. Evaluarea ar trebui să analizeze, de asemenea, efectele potențiale ale certificării obligatorii asupra disponibilității acestor produse pe piața internă, precum și capacitățile și gradul de pregătire al statelor membre pentru introducerea sistemelor europene de certificare de securitate cibernetică relevante.

---

[20] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului și Consiliului, în ceea ce privește adoptarea sistemului european de certificare de securitate cibernetică bazat pe criterii comune (EUCC)(JO L, 2024/482, 07.02.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(47) Actele delegate care impun certificarea europeană obligatorie de securitate cibernetică ar trebui să stabilească produsele cu elemente digitale care au funcționalitatea de bază a unei categorii de produse critice cu elemente digitale, prevăzute în prezentul regulament, care urmează să facă obiectul certificării obligatorii, precum și nivelul de asigurare necesar, care ar trebui să fie cel puțin „substanțial”. Nivelul de asigurare necesar ar trebui să fie proporțional cu nivelul riscului în materie de securitate cibernetică asociat produsului cu elemente digitale. De exemplu, în cazul în care produsul cu elemente digitale are funcționalitatea de bază a unei categorii de produse critice cu elemente digitale prevăzute în prezentul regulament și este destinat utilizării într-un mediu sensibil sau critic, cum ar fi produsele destinate utilizării de către entitățile esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555, acesta poate necesita cel mai înalt nivel de asigurare.

(48) Pentru a asigura o protecție adecvată comună la nivelul Uniunii, în materie de securitate cibernetică a produselor cu elemente digitale care au funcționalitatea de bază a unei categorii de produse critice cu elemente digitale, prevăzută în prezentul regulament, Comisia ar trebui, de asemenea, să fie împuternicită să adopte acte delegate de modificare a prezentului regulament, prin adăugarea sau retragerea unor categorii de produse critice cu elemente digitale pentru care producătorii ar putea fi obligați să obțină un certificat european de securitate cibernetică, în cadrul unui sistem european de certificare de securitate cibernetică, în temeiul Regulamentului (UE) 2019/881, pentru a demonstra conformitatea cu prezentul regulament. O nouă categorie de produse critice cu elemente digitale poate fi adăugată la categoriile respective dacă există o dependență critică de acestea a entităților esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555 sau, în cazul în care sunt afectate de incidente sau conțin vulnerabilități exploatate, acest lucru ar putea duce la perturbări ale lanțurilor de aprovizionare critice. Atunci când evaluează necesitatea adăugării sau retragerii unor categorii de produse critice cu elemente digitale, prin intermediul unui act delegat, Comisia ar trebui să poată lua în considerare dacă statele membre au identificat la nivel național produsele cu elemente digitale care joacă un rol esențial pentru reziliența entităților esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555 și care se confruntă din ce în ce mai mult cu atacuri cibernetice asupra lanțului de aprovizionare, cu potențiale efecte perturbatoare grave. În plus, Comisia ar trebui să poată ține seama de rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate legate de lanțurile de aprovizionare critice, efectuate în conformitate cu articolul 22 din Directiva (UE) 2022/2555.

(49) Comisia ar trebui să se asigure că o gamă largă de părți interesate relevante sunt consultate în mod structurat și periodic atunci când pregătește măsurile pentru punerea în aplicare a prezentului regulament. Acest aspect ar trebui luat în considerare mai ales atunci când Comisia evaluează necesitatea unor eventuale actualizări ale listelor de categorii de produse importante sau critice cu elemente digitale, caz în care producătorii relevanți ar trebui să fie consultați și opiniile acestora ar trebui să fie avute în vedere, cu scopul de a analiza riscurile în materie de securitate cibernetică, precum și echilibrul dintre costurile și beneficiile desemnării unor astfel de categorii de produse ca fiind importante sau critice.

(50) 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 o consecință a unei încălcări a securității. Aceste riscuri ar trebui să fie reglementate în continuare de legislația relevantă de armonizare a Uniunii diferită de prezentul regulament. În cazul în care nu este aplicabil niciun alt act din legislația de armonizare a Uniunii, diferit de prezentul regulament, acestea ar trebui să facă obiectul Regulamentului (UE) 2023/988 al Parlamentului European și al Consiliului[21]. 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 legislația de armonizare a Uniunii diferită de prezentul regulament, în înțelesul articolului 3 punctul 27 din Regulamentul (UE) 2023/988.

---

[21] 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).

(51) Produsele cu elemente digitale clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul 6 din Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului[22] care intră în domeniul de aplicare al prezentului regulament ar trebui să respecte cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament. Dacă aceste sisteme de IA cu grad ridicat de risc îndeplinesc cerințele esențiale de securitate cibernetică ale prezentului regulament, ar trebui să se considere că acestea respectă cerințele de securitate cibernetică prevăzute la articolul 15 din Regulamentul (UE) 2024/1689, 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 acest scop, evaluarea riscurilor în materie de securitate cibernetică asociate unui produs cu elemente digitale clasificat drept sistem de IA cu grad ridicat de risc în temeiul Regulamentului (UE) 2024/1689 care urmează să fie avute în vedere în cursul etapelor de planificare, proiectare, dezvoltare, producție, livrare și mentenanță ale acestui produs, conform cerințelor prezentului regulament, ar trebui să țină cont de riscurile la adresa rezilienței cibernetice a unui sistem de IA în ceea ce privește tentativele unor părți terțe neautorizate de a-i schimba utilizarea, comportamentul sau performanța, inclusiv vulnerabilități specifice IA, cum ar fi „otrăvirea datelor” sau „atacurile contradictorii”, precum și, după caz, riscurile la adresa drepturilor fundamentale, în conformitate cu Regulamentul (UE) 2024/1689. În ceea ce privește procedurile de evaluare a conformității referitoare la cerințele esențiale de securitate cibernetică legate de un produs cu elemente digitale care se încadrează în domeniul de aplicare al prezentului regulament și este clasificat ca sistem de IA cu grad ridicat de risc, articolul 43 din Regulamentul (UE) 2024/1689 ar trebui să se aplice de regulă în locul dispozițiilor relevante din prezentul regulament.

---

[22] Regulamentul (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială)(JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

Totuși, această regulă nu ar trebui să conducă la o reducere a nivelului necesar de asigurare pentru produsele importante sau critice cu elemente digitale, astfel cum se menționează în prezentul 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 (UE) 2024/1689 sunt, de asemenea, produse importante sau critice cu elemente digitale, astfel cum se menționează în prezentul regulament și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa VI la Regulamentul (UE) 2024/1689 ar trebui să facă obiectul procedurilor privind evaluarea conformității prevăzute în prezentul regulament în ceea ce privește cerințele esențiale de securitate cibernetică ale prezentului regulament. În astfel de caz, pentru toate celelalte aspecte vizate de Regulamentul (UE) 2024/1689 ar trebui să se aplice dispozițiile relevante privind evaluarea conformității bazată pe control intern prevăzute în anexa VI la regulamentul respectiv.

(52) Pentru a îmbunătăți securitatea produselor cu elemente digitale introduse pe piața internă, este necesar să se stabilească cerințe esențiale de securitate cibernetică aplicabile unor astfel de produse. Aceste cerințe esențiale de securitate cibernetică nu ar trebui să aducă atingere evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate pentru lanțurile de aprovizionare critice prevăzute la articolul 22 din Directiva (UE) 2022/2555, care iau în considerare atât factori de risc tehnici, cât și, după caz, factori de risc fără caracter tehnic, cum ar fi influența nejustificată a unei țări terțe asupra furnizorilor. În plus, ele nu ar trebui să se aducă atingere prerogativelor statelor membre de a stabili cerințe suplimentare care să țină seama de factori fără caracter tehnic în scopul asigurării unui nivel ridicat de reziliență, inclusiv de cei definiți în Recomandarea (UE) 2019/534 a Comisiei[23], în evaluarea coordonată la nivelul UE a riscurilor legate de securitatea cibernetică a rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G convenit de Grupul de cooperare, instituit în conformitate cu articolul 14 din Directiva (UE) 2022/2555.

[23] Recomandarea (UE) 2019/534 a Comisiei din 26 martie 2019 intitulată „Securitatea cibernetică a rețelelor 5G” (JO L 88, 29.3.2019, p. 42).

(53) Producătorii de produse care intră în domeniul de aplicare al Regulamentului (UE) 2023/1230 al Parlamentului European și al Consiliului[24] care sunt și produse cu elemente digitale în sensul definiției din prezentul regulament ar trebui să respecte atât cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament și cerințele esențiale privind sănătatea și siguranța prevăzute în Regulamentul (UE) 2023/1230. Cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament și anumite cerințe esențiale prevăzute în Regulamentul (UE) 2023/1230 ar putea aborda riscuri similare în materie de securitate cibernetică. Prin urmare, respectarea cerințelor esențiale de securitate cibernetică prevăzute în prezentul regulament ar putea facilita respectarea cerințelor esențiale de securitate cibernetică care acoperă, de asemenea, anumite riscuri în materie de securitate cibernetică prevăzute în Regulamentul (UE) 2023/1230, în special cele privind protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control prevăzute în secțiunile 1.1.9 și 1.2.1 din anexa III la regulamentul respectiv. Astfel de sinergii trebuie să fie demonstrate de producător, de exemplu prin aplicarea, dacă sunt disponibile, a unor standarde armonizate sau a altor specificații tehnice care acoperă cerințele esențiale de securitate cibernetică relevante, în urma unei evaluări a riscurilor care acoperă respectivele riscuri în materie de securitate cibernetică. Producătorul ar trebui, de asemenea, să urmeze procedurile aplicabile de evaluare a conformității stabilite în prezentul regulament și în Regulamentul (UE) 2023/1230. În cadrul lucrărilor pregătitoare care sprijină punerea în aplicare a prezentului regulament și a Regulamentului (UE) 2023/1230 și a proceselor de standardizare aferente, Comisia și organizațiile europene de standardizare ar trebui să promoveze coerența în ceea ce privește modul în care trebuie să fie evaluate riscurile în materie de securitate cibernetică și modul în care riscurile respective urmează să facă obiectul unor standarde armonizate în privința cerințelor esențiale relevante.

---

[24] 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 Consiliului și a Directivei 73/361/CEE a Consiliului (JO L 165, 29.6.2023, p. 1).

În special, Comisia și organizațiile europene de standardizare ar trebui să țină cont de prezentul regulament în pregătirea și dezvoltarea standardelor armonizate pentru a facilita punerea în aplicare a Regulamentului (UE) 2023/1230 în ceea ce privește mai ales aspectele de securitate cibernetică legate de protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control, prevăzute în secțiunile 1.1.9 și 1.2.1 din Anexa III la regulamentul respectiv. Comisia ar trebui să ofere orientări pentru a sprijini producătorii cărora li se aplică prezentul regulament și, de asemenea, Regulamentul (UE) 2023/1230, în special pentru a facilita demonstrarea respectarea cerințelor esențiale relevante prevăzute în prezentul regulament și în Regulamentul (UE) 2023/1230.

(54) Pentru a se asigura faptul că produsele cu elemente digitale sunt sigure atât în momentul introducerii lor pe piață, cât și pe durata de utilizare preconizată a produsului cu elemente digitale, este necesar să se stabilească cerințe esențiale de securitate cibernetică 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 de securitate cibernetică legate de gestionarea vulnerabilităților pe întreaga perioadă de asistență, aceștia ar trebui să stabilească celelalte cerințe esențiale de securitate cibernetică legate de proprietățile produsului care sunt relevante pentru tipul de produs cu elemente digitale 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 de securitate cibernetică relevante pentru a pune la dispoziție produsele lor cu elemente digitale, 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 europene sau internaționale adecvate.

(55) În cazul în care anumite cerințe esențiale de securitate cibernetică nu sunt aplicabile unui produs cu elemente digitale, producătorul ar trebui să includă o justificare clară în evaluarea riscului în materie de securitate cibernetică în documentația tehnică. Acesta ar putea fi cazul în care o cerință esențială de securitate cibernetică este incompatibilă cu natura unui produs cu elemente digitale. De exemplu, scopul preconizat al unui produs cu elemente digitale poate impune producătorului să respecte standarde de interoperabilitate recunoscute pe scară largă, chiar dacă elementele sale de securitate nu mai sunt considerate a fi de ultimă generație. În mod similar, alte acte legislative ale Uniunii impun producătorilor să aplice cerințe specifice de interoperabilitate. În cazul în care o cerință esențială de securitate cibernetică nu se aplică unui produs cu elemente digitale, dar producătorul a identificat riscuri în materie de securitate cibernetică în legătură cu cerința esențială de securitate cibernetică respectivă, acesta ar trebui să ia măsuri pentru a aborda riscurile respective prin alte mijloace, de exemplu prin limitarea scopului preconizat al produsului la medii sigure sau prin informarea utilizatorilor cu privire la riscurile respective.

(56) Una dintre cele mai importante măsuri pe care utilizatorii trebuie să le ia pentru a-și proteja produsele cu elemente digitale împotriva atacurilor cibernetice este instalarea celor mai recente actualizări de securitate disponibile cât mai curând posibil. Prin urmare, producătorii ar trebui să își proiecteze produsele și să instituie procese pentru a se asigura că produsele cu elemente digitale includ funcții care permit notificarea, distribuirea, descărcarea și instalarea automată a actualizărilor de securitate, în special în cazul produselor de consum. Acestea ar trebui, de asemenea, să ofere posibilitatea de a aproba descărcarea și instalarea actualizărilor de securitate ca etapă finală. Utilizatorii ar trebui să își păstreze capacitatea de a dezactiva actualizările automate, printr-un mecanism clar și ușor de utilizat, însoțit de instrucțiuni clare despre modul în care utilizatorii pot renunța la actualizări. Cerințele referitoare la actualizările automate astfel cum sunt prevăzute într-o anexă la prezentul regulament nu se aplică produselor cu elemente digitale destinate în principal să fie integrate drept componente în alte produse. De asemenea, ele nu se aplică produselor cu elemente digitale pentru care utilizatorii nu s-ar aștepta în mod rezonabil la actualizări automate, inclusiv produselor cu elemente digitale destinate a fi utilizate în rețele TIC profesionale și, în special, în medii critice și industriale în care o actualizare automată ar putea cauza interferențe cu operațiunile. Indiferent dacă un produs cu elemente digitale este conceput sau nu pentru a primi actualizări automate, producătorul acestuia ar trebui să informeze utilizatorii despre vulnerabilități și să pună la dispoziție fără întârziere actualizările de securitate. În cazul în care un produs cu elemente digitale are o interfață pentru utilizatori sau mijloace tehnice similare care permit interacțiunea directă cu utilizatorii săi, producătorul ar trebui să utilizeze astfel de caracteristici pentru a informa utilizatorii că produsul său cu elemente digitale a ajuns la sfârșitul perioadei de asistență. Notificările ar trebui să se limiteze la ceea ce este necesar pentru a asigura primirea eficace a acestor informații și nu ar trebui să aibă un impact negativ asupra experienței utilizatorilor produsului cu elemente digitale.

(57) Pentru a îmbunătăți transparența proceselor de gestionare a vulnerabilităților și pentru a se asigura că utilizatorii nu sunt obligați să instaleze noi actualizări de funcționalitate cu unicul scop de a primi cele mai recente actualizări de securitate, producătorii ar trebui să se asigure, în cazul în care acest lucru este fezabil din punct de vedere tehnic, că noile actualizări de securitate sunt furnizate separat de actualizările de funcționalitate.

(58) Comunicarea comună a Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate din 20 iunie 2023 intitulată „Strategia europeană de securitate economică” a afirmat că Uniunea trebuie să maximizeze beneficiile deschiderii sale economice, reducând în același timp la minimum riscurile generate de dependența economică de furnizorii cu grad ridicat de risc, prin intermediul unui cadru strategic comun privind securitatea economică a Uniunii. Dependențele de furnizorii cu risc ridicat de produse cu elemente digitale ar putea prezenta un risc strategic care trebuie abordat la nivelul Uniunii, în special atunci când produsele cu elemente digitale sunt destinate utilizării de către entitățile esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555. Astfel de riscuri pot fi legate, dar nu în mod exclusiv, de jurisdicția aplicabilă producătorului, de caracteristicile acționariatului său și de legăturile de control cu guvernul unei țări terțe în care este stabilit producătorul, în special în cazul în care o țară terță este implicată în spionaj economic sau are un comportament de stat iresponsabil în spațiul cibernetic, iar legislația sa îi permite accesul arbitrar la orice tip de operațiuni sau date ale întreprinderilor, inclusiv la 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 unor mecanisme de supraveghere, respectarea normelor privind un proces echitabil sau a dreptului de a introduce o cale de atac în fața unei instanțe independente. Atunci când evaluează importanța unui risc de securitate cibernetică în înțelesul prezentului regulament, Comisia și autoritățile de supraveghere a pieței, conform responsabilităților lor prevăzute în prezentul regulament, ar trebui să ia în considerare și factorii de risc fără caracter tehnic, în special cei stabiliți după evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate ale lanțurilor de aprovizionare critice, efectuate în conformitate cu articolul 22 din Directiva (UE) 2022/2555.

(59) Pentru a asigura securitatea produselor cu elemente digitale după introducerea lor pe piață, producătorii ar trebui să stabilească perioada de asistență, care să reflecte durata preconizată pentru utilizarea produsului cu elemente digitale. La stabilirea unei perioade de asistență, un producător ar trebui să țină seama mai ales de așteptările rezonabile ale utilizatorilor, de natura produsului, precum și de dreptul relevant al Uniunii care stabilește durata de viață a produselor cu elemente digitale. Producătorii ar trebui, de asemenea, să poată lua în considerare alți factori relevanți. Criteriile ar trebui să fie aplicate într-un mod care să asigure proporționalitatea în ceea ce privește stabilirea perioadei de asistență. La cerere, un producător ar trebui să furnizeze autorităților de supraveghere a pieței informațiile care au fost luate în considerare pentru a stabili perioada de asistență a unui produs cu elemente digitale.

(60) Perioada de asistență pentru care producătorul asigură gestionarea eficace a vulnerabilităților ar trebui să fie de cel puțin cinci ani, cu excepția cazului în care durata de viață a produsului cu elemente digitale este mai mică de cinci ani, caz în care producătorul ar trebui să asigure gestionarea vulnerabilităților pe durata de viață respectivă. În cazul în care se preconizează în mod rezonabil că produsul cu elemente digitale va fi utilizat mai mult de cinci ani, așa cum se întâmplă adesea în cazul componentelor hardware, cum ar fi plăcile de bază sau microprocesoarele, dispozitivele de rețea, cum ar fi routerele, modemurile sau comutatoarele, precum și software-ul, cum ar fi sistemele de operare sau instrumentele de editare video, producătorii ar trebui să asigure, în consecință, perioade de asistență mai lungi. În special, produsele cu elemente digitale destinate utilizării în medii industriale, cum ar fi sistemele industriale de control, sunt adesea utilizate pentru perioade semnificativ mai lungi de timp. Un producător ar trebui să poată defini o perioadă de asistență mai mică de cinci ani numai dacă acest lucru este justificat de natura produsului cu elemente digitale în cauză și dacă se preconizează că produsul respectiv va fi utilizat mai puțin de cinci ani, caz în care perioada de asistență ar trebui să corespundă duratei de utilizare preconizate. De exemplu, durata de viață a unei aplicații de depistare a contacților, destinată utilizării în timpul unei pandemii, ar putea fi limitată la durata pandemiei. În plus, anumite aplicații software pot fi puse la dispoziție, prin natura lor, numai pe baza unui abonament, în special în cazul în care aplicația nu mai este disponibilă pentru utilizator și, prin urmare, nu mai este în uz după expirarea abonamentului.

(61) Atunci când produsele cu elemente digitale ajung la sfârșitul perioadelor lor de asistență, pentru a se asigura că vulnerabilitățile pot fi gestionate după sfârșitul perioadei de asistență, producătorii ar trebui să ia în considerare divulgarea codului sursă al unor astfel de produse cu elemente digitale fie altor întreprinderi care se angajează să extindă furnizarea de servicii de gestionare a vulnerabilităților, fie publicului. În cazul în care producătorii divulgă codul sursă altor întreprinderi, ar trebui să fie în măsură să protejeze proprietatea asupra produsului cu elemente digitale și să împiedice diseminarea codului sursă către public, de exemplu prin acorduri contractuale.

(62) Pentru a se asigura că producătorii din întreaga Uniune stabilesc perioade de asistență similare pentru produse comparabile cu elemente digitale, ADCO ar trebui să publice statistici privind perioadele medii de asistență stabilite de producători pentru categoriile de produse cu elemente digitale și să emită orientări care să indice perioadele de asistență adecvate pentru astfel de categorii. În plus, în vederea asigurării unei abordări armonizate la nivelul pieței interne, Comisia ar trebui să poată adopta acte delegate în vederea precizării perioadelor minime de asistență pentru anumite categorii de produse dacă datele furnizate de autoritățile de supraveghere a pieței sugerează că perioadele de asistență stabilite de producători fie nu sunt în mod sistematic conforme cu criteriile de stabilire a perioadelor de asistență prevăzute în prezentul regulament, fie că producătorii din state membre diferite stabilesc în mod nejustificat perioade de asistență diferite.

(63) Producătorii ar trebui să înființeze un ghișeu unic care să le permită utilizatorilor să comunice cu ușurință cu aceștia, inclusiv în scopul raportării și primirii de informații despre vulnerabilitățile produsului cu elemente digitale. Ei ar trebui să facă ghișeul unic ușor accesibil pentru utilizatori și să indice în mod clar disponibilitatea acestuia, menținând aceste informații actualizate. În cazul în care producătorii aleg să ofere instrumente automatizate, de exemplu chat box, ar trebui să ofere, de asemenea, un număr de telefon sau alte mijloace digitale de contact, cum ar fi o adresă de e-mail sau un formular de contact. Ghișeul unic nu ar trebui să se bazeze exclusiv pe instrumente automatizate.

(64) Producătorii ar trebui să pună la dispoziție pe piață produsele lor cu elemente digitale cu o configurație securizată implicită și să furnizeze utilizatorilor actualizări de securitate în mod gratuit. Producătorii ar trebui să se poată abate de la aceste cerințe esențiale de securitate cibernetică numai în ceea ce privește produsele personalizate care sunt montate într-un anumit scop pentru un anumit furnizor, prin servicii de intermediere online și în cazul în care atât producătorul, cât și utilizatorul au convenit în mod explicit asupra unui set diferit de clauze contractuale.

(65) Producătorii ar trebui să anunțe simultan, prin intermediul platformei unice de raportare, atât echipa de răspuns la incidente de securitate cibernetică (CSIRT), desemnată drept coordonator, cât și ENISA, cu privire la vulnerabilitățile exploatate activ conținute în produsele cu elemente digitale, precum și cu privire la incidentele grave care au un impact asupra securității produselor respective. Notificările ar trebui să fie transmise utilizând punctul terminal de notificare electronică al unei CSIRT desemnate drept coordonator și ar trebui să fie simultan accesibile ENISA.

(66) Producătorii ar trebui să notifice vulnerabilitățile exploatate activ pentru a se asigura că CSIRT desemnate drept coordonatori și ENISA au o imagine de ansamblu adecvată a acestor vulnerabilități și primesc informațiile necesare pentru îndeplinirea sarcinilor lor prevăzute în Directiva (UE) 2022/2555 și pentru creșterea nivelului general de securitate cibernetică a entităților esențiale și importante menționate la articolul 3 din directiva respectivă, precum și pentru a asigura funcționarea eficace a autorităților de supraveghere a pieței. Întrucât majoritatea produselor cu elemente digitale sunt comercializate pe întreaga piață internă, orice vulnerabilitate exploatată activ a unui produs cu elemente digitale ar trebui considerată a fi o amenințare la adresa funcționării pieței interne. ENISA ar trebui, în acord cu producătorul, să divulge vulnerabilitățile fixe bazei de date europene a vulnerabilităților instituite în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555. Baza de date europeană a vulnerabilităților va ajuta producătorii să depisteze vulnerabilitățile exploatabile din produsele lor, pentru a garanta punerea la dispoziție pe piață a unor produse sigure.

(67) Producătorii ar trebui, de asemenea, să informeze CSIRT desemnată drept coordonator și ENISA cu privire la orice incident grav care are un impact asupra securității produsului cu elemente digitale. Pentru a se asigura că utilizatorii pot reacționa rapid la incidentele grave 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 în materie de securitate cibernetică justifică acest lucru, prin contactarea directă a utilizatorilor.

(68) Vulnerabilitățile exploatate în mod activ se referă la cazurile în care un producător stabilește că o încălcare a securității care îi afectează utilizatorii sau orice altă persoană fizică sau juridică a fost cauzată de un actor rău-intenționat care a utilizat o deficiență a unuia dintre produsele cu elemente digitale puse la dispoziție pe piață de producător. Exemple de astfel de vulnerabilități ar putea fi deficiențele în ceea ce privește funcțiile de identificare și de autentificare ale unui produs. 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 unei notificări obligatorii. Incidentele grave care au un impact asupra securității produsului cu elemente digitale se referă, pe de altă parte, la situațiile în care un incident de securitate cibernetică afectează procesele de dezvoltare, producție sau întreținere ale producătorului într-un mod în care ar putea duce la un risc crescut de securitate cibernetică pentru utilizatori sau pentru alte persoane. Un astfel de incident grav ar putea include o situație în care un atacator a introdus cu succes un cod dăunător în canalul de lansare prin care producătorul eliberează actualizări de securitate utilizatorilor.

(69) Pentru a se asigura că notificările pot fi diseminate rapid tuturor CSIRT relevante desemnate drept coordonatori și pentru a permite producătorilor să transmită o notificare unică în fiecare etapă a procesului de notificare, ENISA ar trebui să instituie o platformă unică de raportare cu puncte terminale naționale de notificare electronică. Operațiunile curente ale platformei unice de raportare ar trebui să fie gestionate și întreținute de ENISA. CSIRT desemnate drept coordonatori ar trebui să își informeze autoritățile de supraveghere a pieței cu privire la vulnerabilitățile sau incidentele notificate. Platforma unică de raportare ar trebui să fie concepută într-un mod în care să asigure confidențialitatea notificărilor, în special în ceea ce privește vulnerabilitățile pentru care nu este încă disponibilă o actualizare de securitate. În plus, ENISA ar trebui să stabilească proceduri pentru a gestiona informațiile în mod securizat și confidențial. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal referitor la tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită grupului de cooperare creat în conformitate cu articolul 14 din Directiva (UE) 2022/2555.

(70) În circumstanțe excepționale și în special la cererea producătorului, CSIRT desemnată drept coordonator care primește inițial o notificare ar trebui să poată decide să amâne diseminarea acesteia către celelalte CSIRT relevante desemnate drept coordonatori prin intermediul platformei unice de raportare, în cazul în care acest lucru se poate justifica din motive legate de securitatea cibernetică și pentru o perioadă strict necesară. CSIRT desemnată drept coordonator ar trebui să informeze imediat ENISA cu privire la decizia de a amâna diseminarea, la motivele care stau la baza acesteia, precum și cu privire la momentul în care intenționează să continue diseminarea. Comisia ar trebui să elaboreze, printr-un act delegat, specificații privind termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică și ar trebui să coopereze cu rețeaua CSIRT creată în temeiul articolului 15 din Directiva (UE) 2022/2555 și cu ENISA la pregătirea proiectului de act delegat. Printre exemplele de motive legate de securitatea cibernetică se numără o procedură coordonată de divulgare a vulnerabilităților aflată în curs sau situațiile în care producătorul ar trebui să furnizeze în scurt timp o măsură de atenuare, iar riscurile în materie de securitate cibernetică ale unei diseminări imediate prin intermediul platformei unice de raportare depășesc beneficiile acesteia. La cererea CSIRT desemnată drept coordonator, ENISA ar trebui să fie în măsură să sprijine CSIRT respectivă să aplice motivele legate de securitatea cibernetică pentru a amâna diseminarea notificării pe baza informațiilor pe care ENISA le-a primit de la această CSIRT cu privire la decizia de a nu disemina o notificare din aceste motive legate de securitate cibernetică. În plus, în circumstanțe excepționale, ENISA nu ar trebui să primească simultan toate detaliile unei notificări privind o vulnerabilitate exploatată activ.

Acest lucru este valabil atunci când producătorul indică în notificarea sa că vulnerabilitatea notificată a fost exploatată în mod activ de către un actor rău-intenționat și că, potrivit informațiilor disponibile, aceasta nu a fost exploatată în niciun alt stat membru decât cel al CSIRT desemnate drept coordonator căreia producătorul i-a notificat vulnerabilitatea, atunci când orice diseminare ulterioară imediată a vulnerabilității notificate ar putea avea ca rezultat furnizarea de informații a căror divulgare ar fi contrară intereselor esențiale ale statului membru respectiv sau atunci când vulnerabilitatea notificată prezintă un risc iminent ridicat în materie de securitate cibernetică care decurge din diseminarea sa ulterioară. În astfel de cazuri, ENISA va primi acces simultan numai la informațiile conform cărora producătorul a efectuat o notificare, la informațiile generale cu privire la produsul cu elemente digitale în cauză, la informațiile privind natura generală a exploatării și la informațiile referitoare la faptul că respectivele motive de securitate au fost invocate de producător și că, prin urmare, conținutul complet al notificării nu este divulgat. Notificarea completă ar trebui apoi să fie pusă la dispoziția ENISA și a altor CSIRT relevante desemnate drept coordonatori atunci când CSIRT desemnată drept coordonator, care primește inițial notificarea, constată că respectivele motive de securitate care reflectă în special circumstanțele excepționale stabilite în prezentul regulament încetează să existe. În cazul în care, pe baza informațiilor disponibile, ENISA consideră că există un risc sistemic care afectează securitatea pe piața internă, ENISA ar trebui să recomande CSIRT destinatare să disemineze notificarea completă celorlalte CSIRT desemnate drept coordonatori și ENISA.

(71) Atunci când producătorii notifică o vulnerabilitate exploatată activ sau un incident grav care are un impact asupra securității produsului cu elemente digitale, aceştia ar trebui să indice în ce măsură consideră că informațiile notificate sunt sensibile. CSIRT desemnată drept coordonator care primește inițial notificarea ar trebui să țină seama de aceste informații atunci când evaluează dacă notificarea generează circumstanțe excepționale care justifică o întârziere în diseminarea sa către celelalte CSIRT relevante desemnate drept coordonatori, din motive justificate legate de securitatea cibernetică. De asemenea, aceasta ar trebui să țină seama de aceste informații atunci când evaluează dacă notificarea unei vulnerabilități exploatate activ dă naștere unor circumstanțe excepționale care justifică ca notificarea completă să nu fie pusă simultan la dispoziția ENISA. În cele din urmă, CSIRT desemnate drept coordonatori ar trebui să fie în măsură să țină seama de aceste informații atunci când stabilesc măsurile adecvate de atenuare a riscurilor care decurg din astfel de vulnerabilități și incidente.

(72) Pentru a simplifica raportarea informațiilor solicitate în temeiul prezentului regulament, având în vedere celelalte cerințe de raportare complementare prevăzute în dreptul Uniunii, cum ar fi Regulamentul (UE) 2016/679, Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului[25], Directiva 2002/58/CE a Parlamentului European și a Consiliului[26] și Directiva (UE) 2022/2555, precum și pentru a reduce sarcina administrativă pentru entități, statele membre sunt încurajate să ia în considerare crearea, la nivel național, a unor puncte unice de intrare pentru astfel de cerințe de raportare. Utilizarea unor astfel de puncte unice de intrare la nivel național pentru raportarea incidentelor de securitate în temeiul Regulamentului (UE) 2016/679 și al Directivei 2002/58/CE nu ar trebui să afecteze aplicarea dispozițiilor Regulamentului (UE) 2016/679 și ale Directivei 2002/58/CE, în special a celor referitoare la independența autorităților menționate în aceste acte. Atunci când instituie platforma unică de raportare menționată în prezentul regulament, ENISA ar trebui să ia în considerare posibilitatea ca punctele terminale naționale de notificare electronică menționate în prezentul regulament să fie integrate în punctele unice de intrare la nivel național care pot integra și alte notificări necesare în temeiul dreptului Uniunii.

---

[25] 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).

[26] 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).

(73) Atunci când creează platforma unică de raportare menționată în prezentul regulament și pentru a beneficia de experiența anterioară, ENISA ar trebui să consulte alte instituții sau agenții ale Uniunii care gestionează platforme sau baze de date care fac obiectul unor cerințe de securitate stricte, cum ar fi Agenția Uniunii Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (eu-LISA). ENISA ar trebui să analizeze și complementaritățile potențiale cu baza de date europeană a vulnerabilităților creată în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555.

(74) Producătorii și alte persoane fizice și juridice ar trebui să fie în măsură să notifice unei CSIRT desemnate drept coordonator sau ENISA, în mod voluntar, orice vulnerabilitate conținută într-un produs cu elemente digitale, amenințările cibernetice care ar putea afecta profilul de risc al unui produs cu elemente digitale, orice incident care are un impact asupra securității produsului cu elemente digitale, precum și incidentele evitate la limită care ar fi putut duce la un astfel de incident.

(75) Statele membre ar trebui să își propună să facă față, în măsura posibilului, provocărilor cu care se confruntă cercetătorii în domeniul vulnerabilității, inclusiv expunerea potențială a acestora la răspunderea penală, în conformitate cu dreptul intern. Având în vedere faptul că persoanele fizice și juridice care cercetează vulnerabilități ar putea fi expuse, în unele state membre, răspunderii penale și civile, statele membre sunt încurajate să adopte orientări în ceea ce privește neurmărirea penală a cercetătorilor în domeniul securității informațiilor și exonerarea de răspundere civilă pentru activitățile desfășurate de aceștia.

(76) 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 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. În plus, producătorii ar trebui, de asemenea, să aibă în vedere publicarea politicilor lor de securitate într-un format care poate fi citit automat. 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. Aceasta se referă la așa-numitele „programe de stimulare a identificării bug-urilor”.

(77) 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 de securitate cibernetică nou apărute cunoscute. Este deosebit de important ca producătorii să se asigure că produsele lor cu elemente digitale nu conțin componente vulnerabile dezvoltate de terți. Producătorii nu ar trebui să fie obligați să publice SBOM.

(78) În cadrul noilor modele de afaceri complexe legate de vânzările online, o societate care își desfășoară activitatea online poate furniza o varietate de servicii. În funcție de natura serviciilor furnizate în legătură cu un anumit produs cu elemente digitale, aceeași entitate se poate încadra în categorii diferite de modele de afaceri sau de operatori economici. În cazul în care o entitate prestează numai servicii de intermediere online pentru un produs cu elemente digitale și este doar un furnizor al unei piețe online, în sensul definiției de la articolul 3 punctul 14 din Regulamentul (UE) 2023/988, aceasta nu se califică drept unul dintre tipurile de operatori economici definiți în prezentul regulament. În cazul în care aceeași entitate este un furnizor al unei piețe online și acționează și în calitate de operator economic, astfel cum este definit în prezentul regulament, pentru vânzarea anumitor produse cu elemente digitale, aceasta ar trebui să fie supusă obligațiilor stabilite în prezentul regulament pentru acest tip de operator economic. De exemplu, dacă furnizorul unei piețe online distribuie, de asemenea, un produs cu elemente digitale, atunci acesta ar fi considerat distribuitor în ceea ce privește vânzarea produsului respectiv. În mod similar, dacă entitatea în cauză își vinde propriile produse de marcă cu elemente digitale, aceasta ar fi considerată drept producător și, prin urmare, ar trebui să respecte cerințele aplicabile producătorilor. De asemenea, unele entități pot fi considerate drept furnizori de servicii de logistică, în sensul definiției de la articolul 3 punctul 11 din Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[27], dacă oferă astfel de servicii. Astfel de cazuri ar trebui să fie evaluate individual. 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 cu scopul de a contribui la garantarea faptului că produsele cu elemente digitale achiziționate prin intermediul piețelor online respectă cerințele de securitate cibernetică prevăzute în prezentul regulament.

---

[27] Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011 (JO L 169, 25.6.2019, p. 1).

(79) 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 de securitate cibernetică prevăzute în prezentul regulament în specificații tehnice detaliate și care sunt adoptate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[28]. Regulamentul respectiv prevede o procedură pentru formularea de obiecții cu privire la standardele armonizate în cazul în care standardele respective nu îndeplinesc în totalitate cerințele prevăzute în prezentul regulament. Procesul de standardizare ar trebui să asigure o reprezentare echilibrată a intereselor și participarea efectivă a părților interesate din cadrul societății civile, inclusiv a organizațiilor de consumatori. Standardele internaționale care sunt conforme cu nivelul de protecție în materie de securitate cibernetică vizat de cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament ar trebui să fie luate, de asemenea, în considerare cu scopul de a facilita elaborarea de standarde armonizate și punerea în aplicare a prezentului regulament, precum și de a înlesni asigurarea conformității pentru întreprinderi, în special microîntreprinderi și întreprinderile mici și mijlocii și cele care își desfășoară activitatea la nivel mondial.

---

28 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).

(80) Elaborarea în timp util de standarde armonizate în cursul perioadei de tranziție pentru aplicarea prezentului regulament și disponibilitatea acestora înainte de data aplicării prezentului regulament vor fi deosebit de importante pentru punerea sa în aplicare efectivă. Acesta este, în special, cazul produselor importante cu elemente digitale care se încadrează în clasa I. Disponibilitatea standardelor armonizate va permite producătorilor acestor produse să efectueze evaluările conformității prin procedura de control intern și, prin urmare, aceasta poate evita blocajele și întârzierile în activitățile organismelor de evaluare a conformității.

(81) Regulamentul (UE) 2019/881 stabilește un cadru european voluntar de certificare de securitate cibernetică pentru produsele TIC, procesele TIC și serviciile TIC. Sistemele europene de certificare de securitate cibernetică oferă un cadru comun de încredere pentru utilizatori, care le permite să utilizeze produsele cu elemente digitale care fac obiectul prezentului regulament. Prezentul regulament ar trebui, prin urmare, să 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 european de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 care a fost identificat de Comisie într-un act de punere în aplicare sunt considerate a fi conforme cu cerințele esențiale de securitate cibernetică stabilite în prezentul regulament în măsura în care certificatul european de securitate cibernetică sau declarația de conformitate ori anumite părți ale acestora acoperă cerințele respective. În lumina prezentului regulament ar trebui să fie evaluată necesitatea unor noi sisteme europene de certificare de securitate cibernetică pentru produsele cu elemente digitale, inclusiv atunci când se pregătește programul de lucru etapizat la nivelul Uniunii în conformitate cu Regulamentul (UE) 2019/881. În cazul în care este necesar un nou sistem care să acopere produsele cu elemente digitale, inclusiv pentru a facilita respectarea prezentului regulament, Comisia poate solicita ENISA să pregătească propuneri de sisteme în conformitate cu articolul 48 din Regulamentul (UE) 2019/881. 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 de securitate cibernetică și de procedurile de evaluare a conformității prevăzute în prezentul regulament și să faciliteze respectarea prezentului regulament. Pentru sistemele europene de certificare de securitate cibernetică care intră în vigoare înainte de intrarea în vigoare a prezentului regulament ar putea fi nevoie de precizări suplimentare cu privire la modalitățile detaliate potrivit cărora se poate aplica prezumția de conformitate.

Comisia ar trebui să fie împuternicită să precizeze, prin intermediul unor acte delegate, condițiile în care sistemele europene de certificare de securitate cibernetică pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament. În plus, pentru a evita sarcinile administrative nejustificate 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, dacă a fost emis un certificat de securitate cibernetică în conformitate cu aceste sisteme europene de certificare de securitate cibernetică la un nivel cel puțin „substanțial”.

(82) La intrarea în vigoare a Regulamentului de punere în aplicare (UE) 2024/482 care se referă la produsele care fac obiectul prezentului regulament, cum ar fi modulele de securitate hardware și microprocesoarele, Comisia ar trebui să fie în măsură să precizeze, prin intermediul unui act delegat, modul în care EUCC oferă o prezumție de conformitate cu cerințele esențiale de securitate cibernetică stabilite în prezentul regulament sau cu anumite părți ale acestora. În plus, un astfel de act delegat poate preciza modul în care un certificat emis în temeiul EUCC elimină obligația producătorilor de a efectua o evaluare de către terți, astfel cum se prevede în prezentul regulament pentru cerințele corespunzătoare.

(83) Actualul cadru european de standardizare, care se bazează pe principiile noii abordări stabilite în Rezoluția Consiliului din 7 mai 1985 privind o nouă abordare în ceea ce privește armonizarea tehnică și standardizarea și pe Regulamentul (UE) nr. 1025/2012, reprezintă cadrul implicit pentru elaborarea de standarde care să prevadă o prezumție de conformitate cu cerințele esențiale de securitate cibernetică relevante stabilite în prezentul regulament. Standardele europene ar trebui să fie orientate către piață, să țină seama de interesul public, precum și de obiectivele de politică enunțate în mod clar în solicitarea Comisiei adresată uneia sau mai multor organizații europene de standardizare de a elabora standarde armonizate, într-un termen stabilit și să se bazeze pe consens. Totuși, în absența unor trimiteri pertinente la standarde armonizate, Comisia ar trebui să poată adopta acte de punere în aplicare de stabilire a unor specificații comune pentru cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament, ca soluție de rezervă excepțională pentru a facilita îndeplinirea de către producător a obligației de a respecta respectivele cerințe esențiale de securitate cibernetică, atunci când procesul de standardizare este blocat sau când există întârzieri în stabilirea unor standarde armonizate adecvate, cu condiția ca, procedând astfel, să respecte în mod corespunzător rolul și funcțiile organizațiilor de standardizare europene. În cazul în care întârzierea se datorează complexității tehnice a standardului în cauză, Comisia ar trebui să ia în considerare acest aspect înainte de a analiza dacă să stabilească specificații comune.

(84) Pentru a stabili, în modul cel mai eficient, specificații comune care să răspundă cerințelor esențiale de securitate cibernetică stabilite în prezentul regulament, Comisia ar trebui să implice în acest proces părțile interesate relevante.

(85) „Termen rezonabil” înseamnă, în ceea ce privește publicarea trimiterilor la standardele armonizate în *Jurnalul Oficial al Uniunii Europene* în conformitate cu Regulamentul (UE) nr. 1025/2012, un termen în care se preconizează publicarea în *Jurnalul Oficial al Uniunii Europene* a trimiterii la standard, rectificarea sau modificarea acesteia și care nu ar trebui să depășească un an de la termenul-limită pentru elaborarea unui standard european stabilit în conformitate cu Regulamentul (UE) nr. 1025/2012.

(86) Pentru a facilita evaluarea conformității cu cerințele esențiale de securitate cibernetică stabilite 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.

(87) Aplicarea standardelor armonizate, a specificațiilor comune sau a sistemelor europene de certificare a securității cibernetice adoptate în temeiul Regulamentului (UE) 2019/881 care prevăd prezumția de conformitate în ceea ce privește cerințele esențiale de securitate cibernetică aplicabile produselor cu elemente digitale va facilita evaluarea conformității de către producători. În cazul în care producătorul alege să nu aplice aceste modalități pentru anumite cerințe, acesta trebuie să indice în documentația sa tehnică modul în care se realizează conformitatea prin alte mijloace. În plus, aplicarea standardelor armonizate, a specificațiilor comune sau a sistemelor europene de certificare a securității cibernetice adoptate în temeiul Regulamentului (UE) 2019/881 care prevăd prezumția de conformitate de către producători, ar facilita verificarea conformității produselor cu elemente digitale de către autoritățile de supraveghere a pieței. Prin urmare, producătorii de produse cu elemente digitale sunt încurajați să aplice aceste standarde armonizate, specificații comune sau sisteme europene de certificare a securității cibernetice.

(88) 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 de securitate cibernetică stabilite în prezentul regulament și, după caz, ale altor acte relevante din legislația de armonizare a Uniunii sub incidența cărora intră produsul cu elemente digitale. De asemenea, producătorilor li se poate impune, în temeiul altor acte juridice 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 juridice 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.

(89) 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[29] stabilește principiile generale care reglementează marcajul CE. 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 stabilite în prezentul regulament.

---

[29] 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).

(90) Pentru a permite operatorilor economici să demonstreze conformitatea cu cerințele esențiale de securitate cibernetică stabilite 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[30] 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 de securitate cibernetică prevăzute în prezentul regulament ar trebui să se bazeze 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 cu elemente digitale.

[30] 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).

(91) Evaluarea conformității produselor cu elemente digitale care nu sunt enumerate ca produse importante sau critice cu elemente digitale în prezentul regulament poate fi efectuată de producător pe propria răspundere, urmând procedura de control intern bazată pe modulul A din Decizia nr. 768/2008/CE, în conformitate cu prezentul regulament. Acest lucru este valabil și în cazurile în care un producător alege să nu aplice, integral sau parțial, un standard armonizat, o specificație comună sau un sistem european de certificare a securității cibernetice aplicabil. Producătorul păstrează flexibilitatea de a alege o procedură mai strictă de evaluare a conformității care să implice o parte terță. În cadrul procedurii de evaluare a conformității controlului intern, producătorul se asigură și declară pe răspunderea sa exclusivă că produsul cu elemente digitale și procesele producătorului îndeplinesc cerințele esențiale de securitate cibernetică aplicabile prevăzute în prezentul regulament. În cazul în care un produs important cu elemente digitale se încadrează în clasa I, este necesară o asigurare suplimentară pentru a demonstra conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament. Producătorul ar trebui să aplice standardele armonizate, specificațiile comune sau sistemele europene de certificare a securității cibernetice adoptate în conformitate cu Regulamentul (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 europene de certificare a securității cibernetice, producătorul ar trebui să fie supus unei evaluări a conformității care implică o parte terță (pe baza modulelor B și C sau a modulului H). 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 și C sau pe modulul H din Decizia nr. 768/2008/CE au fost alese ca fiind cele mai adecvate pentru evaluarea conformității produselor importante 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 importante cu elemente digitale care se încadrează în clasa II, evaluarea conformității ar trebui să implice întotdeauna o parte terță, chiar și în cazul în care produsul respectă integral sau parțial standardele armonizate, specificațiile comune sau sistemele europene de certificare a securității cibernetice. Producătorii de produse importante cu elemente digitale care se califică drept software liber și cu sursă deschisă ar trebui să poată urma procedura de control intern bazată pe modulul A, cu condiția de a pune documentația tehnică la dispoziția publicului.

(92) 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 a fi activități echivalente cu producția atunci când se aplică modulele relevante de evaluare a conformității pentru a verifica conformitatea produsului cu cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament în etapele de proiectare, dezvoltare și producție.

(93) În ceea ce privește microîntreprinderile și întreprinderile mici, pentru a asigura proporționalitatea, este oportun să se reducă costurile administrative fără a afecta nivelul de protecție a securității cibernetice a produselor cu elemente digitale care intră în domeniul de aplicare al prezentului regulament sau condițiile de concurență echitabile între producători. Prin urmare, este oportun ca Comisia să stabilească un formular simplificat de documentație tehnică care să vizeze nevoile microîntreprinderilor și ale întreprinderilor mici. Formularul simplificat de documentație tehnică adoptat de Comisie ar trebui să acopere toate elementele aplicabile legate de documentația tehnică prevăzute în prezentul regulament și să precizeze modul în care o microîntreprindere sau o întreprindere mică poate furniza în mod concis elementele solicitate, cum ar fi descrierea proiectării, dezvoltării și fabricării produsului cu elemente digitale. Astfel, formularul ar contribui la reducerea sarcinii administrative de asigurare a conformității, oferind întreprinderilor în cauză securitate juridică cu privire la amploarea și nivelul de detaliere a informațiilor care trebuie furnizate. Microîntreprinderile și întreprinderile mici ar trebui să poată alege să furnizeze într-o formă cuprinzătoare elementele aplicabile legate de documentația tehnică și să nu recurgă la formularul simplificat de documentație tehnică aflat la dispoziția lor.

(94) Pentru a promova și a proteja inovarea, este important să se țină seama de interesele producătorilor care sunt microîntreprinderi sau întreprinderi mici sau mijlocii, în special ale microîntreprinderilor și întreprinderilor mici, inclusiv ale întreprinderilor nou-înființate. În acest scop, statele membre ar putea elabora inițiative care să vizeze producătorii care sunt microîntreprinderi sau întreprinderi mici, în special în ceea ce privește formarea, sensibilizarea, comunicarea și informațiilor, testarea și activitățile de evaluare a conformității de către terți, precum și crearea unor spații de testare. Costurile de traducere legate de documentația obligatorie, cum ar fi documentația tehnică și informațiile și instrucțiunile pentru utilizator solicitate în temeiul prezentului regulament, precum și comunicarea cu autoritățile, pot constitui un cost semnificativ pentru producători, în special pentru cei de dimensiuni mai mici. Prin urmare, statele membre ar trebui să fie în măsură să prevadă ca una dintre limbile pe care le stabilesc și le acceptă pentru documentația pertinentă a producătorilor și pentru comunicarea cu producătorii să fie o limbă larg înțeleasă de un număr cât mai mare de utilizatori.

(95) Cu scopul de a asigura buna aplicare a prezentului regulament, statele membre ar trebui să depună eforturi pentru a se asigura, înainte de data aplicării prezentului regulament, că este disponibil un număr suficient de organisme notificate pentru a efectua evaluări ale conformității de către terți. Comisia ar trebui să urmărească să sprijine statele membre și celelalte părți pertinente în acest demers, pentru a evita blocajele și obstacolele în calea intrării pe piață a producătorilor. Activitățile de formare specifice conduse de statele membre, inclusiv, după caz, cu sprijinul Comisiei, pot contribui la disponibilitatea unor profesioniști calificați, inclusiv pentru a sprijini activitățile organismelor notificate în temeiul prezentului regulament. În plus, având în vedere costurile pe care le poate implica evaluarea conformității de către terți, ar trebui avute în vedere inițiative de finanțare la nivelul Uniunii și la nivel național care să urmărească să atenueze astfel de costuri pentru microîntreprinderi și întreprinderile mici.

(96) Pentru a asigura proporționalitatea, organismele de evaluare a conformității, atunci când stabilesc taxele pentru procedurile de evaluare a conformității, ar trebui să țină seama de interesele și nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii, inclusiv ale întreprinderilor nou-înființate. În special, organismele de evaluare a conformității ar trebui să aplice procedura de examinare și testele pertinente prevăzute în prezentul regulament numai dacă este cazul și urmând o abordare bazată pe riscuri.

(97) Spațiile de testare în materie de reglementare ar trebui să aibă drept obiectiv stimularea inovării și a competitivității pentru întreprinderi prin stabilirea unor medii de testare controlate înainte de introducerea pe piață a produselor cu elemente digitale. Spațiile de testare în materie de reglementare ar trebui să contribuie la îmbunătățirea securității juridice pentru toți actorii care intră în domeniul de aplicare al prezentului regulament și să faciliteze și să accelereze accesul la piața Uniunii al produselor cu elemente digitale, în special atunci când sunt furnizate de microîntreprinderi și întreprinderi mici, inclusiv de întreprinderi nou-înființate.

(98) 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.

(99) 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 să fie utilizată și în vederea notificării.

(100) Organismele de evaluare a conformității care au fost acreditate și notificate în temeiul unui act legislativ al Uniunii care stabilește cerințe similare cu cele prevăzute în prezentul regulament, cum ar fi un organism de evaluare a conformității care a fost notificat pentru un sistem european de certificare a securității cibernetice adoptat în temeiul Regulamentului (UE) 2019/881 sau notificat în temeiul Regulamentului delegat (UE) 2022/30, ar trebui să fie evaluate și notificate din nou în temeiul prezentului regulament. Cu toate acestea, autoritățile pertinente pot defini sinergii în ceea ce privește eventualele suprapuneri ale cerințelor, pentru a preveni o sarcină financiară și administrativă inutilă și pentru a asigura un proces de notificare fără probleme și în timp util.

(101) 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.

(102) 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.

(103) Notificarea unui organism de evaluare a conformității ar trebui să fie 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). Sistemul informațional NANDO este instrumentul de notificare electronică dezvoltat și gestionat de Comisie, în care se găsește o listă a tuturor organismelor notificate.

(104) 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.

(105) 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. 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 să fie realizat cel mai bine printr-o coordonare și o cooperare adecvată între organismele notificate.

(106) Supravegherea pieței este un instrument esențial, deoarece asigură aplicarea corespunzătoare și uniformă a dreptului 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 se aplică produselor cu elemente digitale care intră în domeniul de aplicare al prezentului regulament.

(107) În conformitate cu Regulamentul (UE) 2019/1020, o autoritate de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru care o desemnează. Prezentul regulament nu ar trebui să împiedice statele membre să aleagă autoritățile competente pentru îndeplinirea sarcinilor de supraveghere a pieței. Fiecare stat membru ar trebui să desemneze una sau mai multe autorități de supraveghere a pieței pe teritoriul său. Statele membre ar trebui să poată alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile competente desemnate sau instituite în temeiul articolului 8 din Directiva (UE) 2022/2555, autoritățile naționale de certificare a securității cibernetice desemnate în temeiul articolului 58 din Regulamentul (UE) 2019/881 sau autoritățile de supraveghere a pieței desemnate în sensul Directivei 2014/53/UE. 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 a pieței 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.

(108) Ar trebui să fie instituit un grup specific ADCO pentru reziliența cibernetică a produselor cu elemente digitale cu scopul de a asigura aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. 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 conformitate cu articolul 29 din Regulamentul (UE) 2019/1020 și alcătuită din reprezentanți ai fiecărui stat membru, inclusiv un reprezentant al fiecărui birou unic de legătură astfel cum se menționează la articolul 10 din regulamentul respectiv și un expert național opțional, președinții ADCO și reprezentanți ai Comisiei. Comisia ar trebui să participe la reuniunile Rețelei Uniunii pentru conformitatea produselor, ale subgrupurilor sale și ale ADCO. Aceasta ar trebui, de asemenea, să asiste ADCO prin intermediul unui secretariat executiv care să ofere sprijin tehnic și logistic. ADCO poate invita, de asemenea, experți independenți să participe și poate colabora cu alte ADCO, cum ar fi cel instituit în temeiul Directivei 2014/53/UE.

(109) Autoritățile de supraveghere a pieței, prin intermediul ADCO instituit în temeiul prezentului regulament, ar trebui să coopereze îndeaproape și ar trebui să fie în măsură să elaboreze documente de orientare cu scopul de a facilita activitățile de supraveghere a pieței la nivel național, de exemplu prin elaborarea de bune practici și de indicatori pentru a verifica în mod eficace conformitatea cu prezentul regulament a produselor cu elemente digitale.

(110) 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.

(111) 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 menționate la articolul 3 alineatul (1) din 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 sau să îl recheme ori să îl retragă, în funcție de risc. De îndată ce o autoritate de supraveghere a pieței restricționează sau interzice libera circulație a unui produs cu elemente digitale 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 cu elemente digitale 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 a fi justificată, Comisia ar trebui, de asemenea, să analizeze dacă este oportun să adopte propuneri de revizuire a legislației relevante a Uniunii.

(112) 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, riscuri de nerespectare a obligațiilor în temeiul dreptului Uniunii și al dreptului intern menite să protejeze drepturile fundamentale sau riscuri la adresa disponibilității, autenticității, integrității sau confidențialității serviciilor oferite prin utilizarea unui sistem informatic electronic de către entități esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555, Comisia ar trebui să poată solicita ENISA să efectueze o evaluare. Pe baza evaluării respective, Comisia ar trebui să poată adopta, prin intermediul unor acte de punere în aplicare, măsuri corective sau restrictive la nivelul Uniunii, inclusiv măsuri prin care se impune retragerea de pe piață sau rechemarea produselor în cauză, într-un termen rezonabil, proporțional cu natura riscului. Comisia ar trebui să poată 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 a pieței nu au luat măsuri eficace pentru remedierea situației. Astfel de circumstanțe excepționale pot fi situații de urgență în care, de exemplu, un produs neconform cu elemente digitale 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 (UE) 2022/2555, acesta conținând vulnerabilități cunoscute care sunt exploatate de actori rău-intenționați și pentru care producătorul nu oferă corecții disponibile. Comisia ar trebui să poată interveni în astfel de situații de urgență numai pe durata circumstanțelor excepționale și dacă nerespectarea prezentului regulament sau riscurile importante prezentate persistă.

(113) Atunci când 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.

(114) 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 să fie efectuate acțiuni de verificare atunci când tendințele pieței, reclamațiile consumatorilor sau alte indicii sugerează că anumite categorii de produse cu elemente digitale sunt adesea considerate ca prezentând riscuri de securitate cibernetică. În plus, atunci când stabilesc categoriile de produse care urmează să fie supuse acțiunilor de verificare, autoritățile de supraveghere a pieței ar trebui să țină seama și de circumstanțele legate de factorii de risc fără caracter tehnic. În acest scop, autoritățile de supraveghere a pieței ar trebui să poată ține seama de rezultatele evaluărilor coordonate la nivelul Uniunii ale riscurilor de securitate legate de lanțurile de aprovizionare critice, efectuate în conformitate cu articolul 22 din Directiva (UE) 2022/2555, inclusiv de circumstanțele legate de factorii de risc fără caracter tehnic. ENISA ar trebui să prezinte autorităților de supraveghere a pieței propuneri de categorii de produse cu elemente digitale pentru care ar putea fi organizate acțiuni de verificare, bazate, printre altele, pe notificările pe care le primește cu privire la vulnerabilități și la incidente.

(115) 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, ENISA 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 să fie organizate acțiuni de verificare. În circumstanțe excepționale, ENISA ar trebui, la cererea Comisiei, 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.

(116) Prezentul regulament conferă ENISA anumite sarcini care necesită resurse adecvate, atât în ceea ce privește expertiza, cât și resursele umane, pentru a permite ENISA să își îndeplinească sarcinile respective în mod eficace. La elaborarea proiectului de buget general al Uniunii, Comisia va propune resursele bugetare necesare pentru schema de personal a ENISA, în conformitate cu procedura prevăzută la articolul 29 din Regulamentul (UE) 2019/881. În cursul acestui proces, Comisia va lua în considerare resursele globale de care ENISA are nevoie pentru a-și îndeplini sarcinile, inclusiv cele care îi sunt conferite în temeiul prezentului regulament.

(117) Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene (TFUE) ar trebui să fie delegată Comisiei în ceea ce privește actualizarea listei produselor importante cu elemente digitale dintr-o anexă la prezentul regulament. 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 în cadrul unui sistem european de certificare de securitate cibernetică a produselor critice cu elemente digitale enumerate într-o anexă la prezentul regulament, precum și pentru actualizarea listei produselor critice cu elemente digitale pe baza criteriilor referitoare la caracterul critic prevăzute în prezentul regulament și pentru specificarea sistemelor europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale de securitate cibernetică sau cu părți ale acestora, astfel cum se prevede într-o anexă la prezentul regulament. Competența de a adopta acte ar trebui să fie delegată Comisiei și pentru a specifica perioada minimă de asistență pentru anumite categorii de produse pentru care datele de supraveghere a pieței sugerează perioade de asistență inadecvate, precum și pentru a specifica termenele și condițiile de aplicare a motivelor legate de securitatea cibernetică în ceea ce privește întârzierea difuzării notificărilor privind vulnerabilitățile exploatate activ.

În plus, competența de a adopta acte ar trebui să fie delegată Comisiei pentru a institui programe voluntare de atestare a securității pentru evaluarea conformității produselor cu elemente digitale care se califică drept software gratuit și cu sursă deschisă cu toate sau cu anumite cerințe esențiale de securitate cibernetică sau cu alte obligații prevăzute în prezentul regulament, precum și pentru a preciza conținutul minim al declarației de conformitate UE și a completa elementele care trebuie incluse în documentația tehnică. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare[31]. 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. Competența de a adopta acte delegate menționată în prezentul regulament se conferă Comisiei pe o perioadă de cinci ani de la ... [data intrării în vigoare a prezentului regulament]. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

[31] JO L 123, 12.5.2016, p. 1.

(118) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui să fie conferite competențe de executare Comisiei pentru a preciza descrierea tehnică a categoriilor de produse importante cu elemente digitale enumerate într-o anexă la prezentul regulament, pentru a specifica formatul și elementele listei materialelor software, pentru a preciza mai detaliat formatul și procedura notificărilor privind vulnerabilitățile exploatate activ și incidentele grave care au un impact asupra securității produselor cu elemente digitale prezentate de producători, pentru a stabili specificații comune privind cerințele tehnice care oferă un mijloc de respectare a cerințelor esențiale de securitate cibernetică prevăzute într-o anexă la prezentul regulament, pentru a stabili specificații tehnice pentru etichete, pictograme sau orice alte marcaje legate de securitatea produselor cu elemente digitale, perioada de asistență a acestora și mecanisme de promovare a utilizării lor și de creștere a gradului de sensibilizare a publicului cu privire la securitatea produselor cu elemente digitale, pentru a preciza formularul de documentație simplificat adaptat nevoilor microîntreprinderilor și ale întreprinderilor mici și 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 să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[32].

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

---

[32] 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), ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj).

(120) 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 să fie stabilite niveluri maxime ale amenzilor administrative, care să fie prevăzute în dreptul intern, 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 sau o întreprindere mică sau mijlocie, inclusiv o întreprindere nou-înființată și dacă aceleași sau alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiași operator economic pentru încălcări similare. Aceste circumstanțe ar putea fi fie agravante, în situațiile în care încălcarea săvârșită de același operator economic 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. Având în vedere că amenzile administrative nu se aplică microîntreprinderilor sau întreprinderilor mici pentru nerespectarea termenului de 24 de ore pentru notificarea timpurie a vulnerabilităților exploatate activ sau a incidentelor grave care au un impact asupra securității produsului cu elemente digitale, nici administratorilor de software cu sursă deschisă pentru orice încălcare a prezentului regulament, și sub rezerva principiului conform căruia sancțiunile ar trebui să fie eficace, proporționale și disuasive, statele membre nu ar trebui să le impună entităților respective alte tipuri de sancțiuni cu caracter pecuniar.

(121) În cazul în care se impun amenzi administrative unei persoane care nu este o întreprindere, 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 fie supuse unor amenzi administrative ar trebui să le revină statelor membre.

(122) Statele membre ar trebui să analizeze, ținând seama de circumstanțele naționale, posibilitatea de a utiliza veniturile provenite din sancțiunile prevăzute în prezentul regulament sau echivalentul financiar al acestora pentru a sprijini politicile de securitate cibernetică și pentru a crește nivelul de securitate cibernetică în Uniune, printre altele, prin mărirea numărului de specialiști calificați în domeniul securității cibernetice, prin consolidarea capacităților microîntreprinderilor și ale întreprinderilor mici și mijlocii și printr-o mai mare sensibilizare a publicului cu privire la amenințările cibernetice.

(123) În relațiile sale cu țările terțe, Uniunea 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. Aceste acorduri 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 cu mai multe țări terțe. Acordurile respective sunt încheiate într-o serie de sectoare specifice, care pot varia de la o țară terță 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 terțe 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 Uniunii.

(124) Consumatorilor ar trebui să li se permită să își exercite drepturile în legătură cu obligațiile impuse operatorilor economici în temeiul prezentului regulament prin intermediul acțiunilor în reprezentare în temeiul Directivei (UE) 2020/1828 a Parlamentului European și a Consiliului[33]. În acest scop, prezentul regulament ar trebui să prevadă că Directiva (UE) 2020/1828 se aplică acțiunilor în reprezentare introduse împotriva încălcărilor dispozițiilor prezentului regulament care aduc atingere sau pot aduce atingere intereselor colective ale consumatorilor. Prin urmare, anexa I la directiva menționată ar trebui modificată în consecință. Statele membre sunt cele care trebuie să se asigure că modificările respective sunt reflectate în măsurile de transpunere pe care le adoptă în temeiul directivei menționate, chiar dacă adoptarea de măsuri naționale de transpunere în această privință nu este o condiție pentru aplicabilitatea directivei respective în cazul acelor acțiuni în reprezentare. Directiva respectivă ar trebui să poată fi aplicată acțiunilor în reprezentare introduse împotriva încălcărilor dispozițiilor prezentului regulament de către operatori economici care prejudiciază sau pot prejudicia interesele colective ale consumatorilor începând de la ... [36 de luni de la data intrării în vigoare a prezentului regulament].

(125) Comisia ar trebui să evalueze și să reexamineze periodic prezentul regulament, consultându-se cu părțile interesate relevante, în special pentru a stabili dacă este necesară efectuarea unor modificări ca urmare a evoluției condițiilor societale, politice, tehnologice sau de piață. Prezentul regulament va facilita respectarea obligațiilor privind securitatea lanțului de aprovizionare de către entitățile care intră în domeniul de aplicare al Regulamentului (UE) 2022/2554 și al Directivei (UE) 2022/2555 și care utilizează produse cu elemente digitale. Comisia ar trebui să evalueze, în cadrul reexaminării periodice, efectele combinate ale cadrului de securitate cibernetică al Uniunii.

---

[33] 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).

(126) Operatorilor economici ar trebui să li se acorde suficient timp pentru a se adapta la cerințele prevăzute în prezentul regulament. Prezentul regulament ar trebui să se aplice de la ... [36 de luni de la data intrării în vigoare a prezentului regulament], cu excepția obligațiilor de raportare privind vulnerabilitățile exploatate activ și incidentele grave care au un impact asupra securității produselor cu elemente digitale, care ar trebui să se aplice de la ... **[**21 de luni de la data intrării în vigoare a prezentului regulament] și a dispozițiilor privind notificarea organismelor de evaluare a conformității, care ar trebui să se aplice de la ... [18 luni de la data intrării în vigoare a prezentului regulament].

(127) Este important să se ofere sprijin microîntreprinderilor și întreprinderilor mici și mijlocii, inclusiv întreprinderilor nou-înființate, la punerea în aplicare a prezentului regulament și să se reducă la minimum riscurile legate de punerea în aplicare care rezultă din lipsa de cunoștințe și de expertiză de pe piață, precum și pentru a facilita respectarea de către producători a obligațiilor care le revin în temeiul prezentului regulament. Programul Europa digitală și alte programe relevante ale Uniunii oferă sprijin financiar și tehnic care le permite întreprinderilor respective să contribuie la creșterea economiei Uniunii și la consolidarea nivelului comun de securitate cibernetică în Uniune. Centrul european de competențe în materie de securitate cibernetică și centrele naționale de coordonare, precum și centrele europene de inovare digitală stabilite de Comisie și de statele membre la nivelul Uniunii sau la nivel național ar putea, de asemenea, să sprijine întreprinderile și organizațiile din sectorul public și ar putea contribui la punerea în aplicare a prezentului regulament. În cadrul misiunilor și domeniilor lor de competență respective, acestea ar putea oferi sprijin tehnic și științific microîntreprinderilor și întreprinderilor mici și mijlocii, de exemplu, pentru activitățile de testare și evaluările conformității de către terți. Acestea ar putea, de asemenea, să promoveze implementarea de instrumente care să faciliteze punerea în aplicare a prezentului regulament.

(128) În plus, statele membre ar trebui să ia în considerare acțiuni complementare pentru a oferi orientări și sprijin microîntreprinderilor și întreprinderilor mici și mijlocii, cum ar fi înființarea de spații de testare în materie de reglementare și de canale speciale de comunicare. Pentru a consolida nivelul de securitate cibernetică în Uniune, statele membre pot lua în considerare, de asemenea, acordarea de asistență pentru dezvoltarea capacității și a competențelor legate de securitatea cibernetică a produselor cu elemente digitale, îmbunătățirea rezilienței cibernetice a operatorilor economici, în special a microîntreprinderilor și a întreprinderilor mici și mijlocii, și promovarea sensibilizării publicului cu privire la securitatea cibernetică a produselor cu elemente digitale.

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

(130) 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[34] și a emis un aviz la 9 noiembrie 2022[35],

ADOPTĂ PREZENTUL REGULAMENT:

---

[34] 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).

[35] JO C 452, 29.11.2022, p. 23.

Capitolul I
Dispoziții generale

Articolul 1

Obiect

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 de securitate cibernetică 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 de securitate cibernetică pentru procesele de gestionare a vulnerabilităților instituite de producători pentru a asigura securitatea cibernetică a produselor cu elemente digitale pe durata în care se preconizează că produsele vor fi utilizate, precum și obligațiile operatorilor economici în legătură cu aceste procese;

(d) normele privind supravegherea pieței, inclusiv monitorizarea, și asigurarea respectării normelor și cerințelor menționate la prezentul articol.

Articolul 2

Domeniul de aplicare

(1) Prezentul regulament se aplică produselor cu elemente digitale puse la dispoziție pe piață al căror scop preconizat sau a căror utilizare previzibilă în mod rezonabil include o conexiune de date logică sau fizică 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 juridice 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.

(4) Prezentul regulament nu se aplică echipamentelor care intră în domeniul de aplicare al Directivei 2014/90/UE a Parlamentului European și a Consiliului[36].

[36] Directiva 2014/90/UE a Parlamentului European și a Consiliului din 23 iulie 2014 privind echipamentele maritime și de abrogare a Directivei 96/98/CE a Consiliului (JO L 257, 28.8.2014, p. 146).

(5) 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 de securitate cibernetică prevăzute în anexa I poate fi limitată sau exclusă dacă:

(a) o astfel de limitare sau excludere este în concordanță cu cadrul general de reglementare care se aplică produselor respective; și

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

Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a completa 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.

(6) Prezentul regulament nu se aplică pieselor de schimb care sunt puse la dispoziție pe piață pentru a înlocui componente identice din produse cu elemente digitale și care sunt fabricate în conformitate cu aceleași specificații ca și componentele pe care sunt destinate să le înlocuiască.

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

(8) Obligațiile prevăzute în prezentul regulament nu implică furnizarea de informații a căror divulgare ar contraveni intereselor esențiale ale statelor membre în materie de securitate națională, siguranță publică sau apărare.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

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

2. „prelucrare de date la distanță” înseamnă prelucrarea 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 vreuna dintre funcții;

3. „securitate cibernetică” înseamnă securitate cibernetică în sensul definiției de la articolul 2 alineatul (1) din Regulamentul (UE) 2019/881;

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

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

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

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

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

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

10. „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;

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

12. „operator economic” înseamnă producătorul, reprezentantul autorizat, importatorul sau distribuitorul, sau o altă persoană fizică sau juridică care este supusă obligațiilor privind fabricarea produselor cu elemente digitale sau punerea la dispoziție a produselor cu elemente digitale pe piață în conformitate cu prezentul regulament;

13. „producător” înseamnă o 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;

14. „administrator de software cu sursă deschisă” înseamnă o persoană juridică, alta decât un producător, care are scopul sau obiectivul de a oferi în mod sistematic și durabil sprijin pentru dezvoltarea de produse specifice cu elemente digitale, care se califică drept software gratuit și cu sursă deschisă și sunt destinate unor activități comerciale, și care asigură viabilitatea produselor respective;

15. „reprezentant autorizat” înseamnă o persoană fizică sau juridică stabilită în Uniune, care a primit din partea unui producător un mandat scris de a acționa în numele său pentru îndeplinirea unor sarcini determinate;

16. „importator” înseamnă o 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;

17. „distribuitor” înseamnă o 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;

18. „consumator” înseamnă o persoană fizică care acționează în scopuri care nu sunt legate de activitățile sale comerciale, de afaceri, artizanale sau profesionale;

19. „microîntreprinderi”, „întreprinderi mici” și „întreprinderi mijlocii” înseamnă, respectiv, microîntreprinderi, întreprinderi mici și întreprinderi mijlocii în sensul definiției din anexa la Recomandarea 2003/361/CE;

20. „perioadă de asistență” înseamnă perioada în care un producător trebuie să se asigure că vulnerabilitățile unui produs cu elemente digitale sunt gestionate în mod eficace și în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II;

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

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

23. „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;

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

25. „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;

26. „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;

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

28. „organism de evaluare a conformității” înseamnă un organism de evaluare a conformității în sensul definiției de la articolul 2 punctul 13 din Regulamentul (CE) nr. 765/2008;

29. „organism notificat” înseamnă un organism de evaluare a conformității desemnat în conformitate cu articolul 43 și cu legislația relevantă de armonizare a Uniunii;

30. „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 de securitate cibernetică prevăzute în anexa I partea I sau care are ca rezultat o modificare a scopului preconizat pentru care a fost evaluat respectivul produs cu elemente digitale;

31. „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 de securitate cibernetică prevăzute în anexa I și în alte acte legislative de armonizare aplicabile ale Uniunii care prevăd aplicarea acestuia;

32. „legislație de armonizare a Uniunii” înseamnă legislația Uniunii enumerată în anexa I la Regulamentul (UE) 2019/1020 și orice alte acte legislative ale Uniunii care armonizează condițiile de comercializare a produselor cărora li se aplică regulamentul respectiv;

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

34. „standard internațional” înseamnă un standard internațional în sensul definiției de la articolul 2 punctul 1 litera (a) din Regulamentul (UE) nr. 1025/2012;

35. „standard european” înseamnă un standard european în sensul definiției de la articolul 2 punctul 1 litera (b) din Regulamentul (UE) nr. 1025/2012;

36. „standard armonizat” înseamnă un standard armonizat în sensul definiției de la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012;

37. „risc de securitate cibernetică” înseamnă potențialul de pierderi sau perturbări cauzate de un incident și se exprimă ca o combinație între amploarea unei astfel de pierderi sau perturbări și probabilitatea producerii incidentului respectiv;

38. „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;

39. „listă a materialelor software” 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;

40. „vulnerabilitate” înseamnă un punct slab, o susceptibilitate sau o deficiență a unui produs cu elemente digitale care poate fi exploatată de o amenințare cibernetică;

41. „vulnerabilitate exploatabilă” înseamnă o vulnerabilitate care poate fi utilizată în mod eficace de un adversar în condiții operaționale practice;

42. „vulnerabilitate exploatată activ” înseamnă o vulnerabilitate în privința căreia există dovezi fiabile că a fost exploatată de un actor rău-intenționat într-un sistem fără permisiunea proprietarului sistemului;

43. „incident” înseamnă un incident în sensul definiției de la articolul 6 punctul 6 din Directiva (UE) 2022/2555;

44. „incident care are un impact asupra securității produsului cu elemente digitale” înseamnă un incident care afectează în mod negativ sau poate afecta în mod negativ capacitatea unui produs cu elemente digitale de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea unor date sau funcții;

45. „incident evitat la limită” înseamnă un incident evitat la limită în sensul definiției de la articolul 6 punctul 5 din Directiva (UE) 2022/2555;

46. „amenințare cibernetică” înseamnă o amenințare cibernetică în sensul definiției de la articolul 2 punctul 8 din Regulamentul (UE) 2019/881;

47. „date cu caracter personal” înseamnă date cu caracter personal în sensul definiției de la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;

48. „software liber și cu sursă deschisă” înseamnă un software al cărui cod sursă este partajat în mod deschis și care este pus la dispoziție sub licență liberă și cu sursă deschisă ce prevede toate drepturile necesare pentru ca software-ul să fie accesibil, utilizabil, modificabil și redistribuibil în mod liber;

49. „rechemare” înseamnă o rechemare în sensul definiției de la articolul 3 punctul 22 din Regulamentul (UE) 2019/1020;

50. „retragere” înseamnă o retragere în sensul definiției de la articolul 3 punctul 23 din Regulamentul (UE) 2019/1020;

51. „CSIRT desemnată drept coordonator” înseamnă o CSIRT desemnată drept coordonator în temeiul articolului 12 alineatul (1) din Directiva (UE) 2022/2555.

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) La târguri comerciale, expoziții, demonstrații sau evenimente similare, statele membre nu împiedică prezentarea sau utilizarea unui produs cu elemente digitale care nu este conform cu prezentul regulament, inclusiv a prototipurilor sale, cu condiția ca un anunț vizibil să indice în mod clar că produsul nu este conform cu prezentul regulament și că nu poate fi pus la dispoziție pe piață până când nu va fi conform.

(3) Statele membre nu împiedică punerea la dispoziție pe piață 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 ca un anunț vizibil să indice în mod clar că produsul nu este conform cu prezentul regulament și că nu va fi disponibil pe piață în alte scopuri decât pentru testare.

(4) Alineatul (3) nu se aplică componentelor de siguranță menționate în legislația de armonizare a Uniunii diferită de prezentul regulament.

Articolul 5

Achizițiile sau utilizarea de produse cu elemente digitale

(1) Prezentul regulament nu împiedică statele membre să supună produsele cu elemente digitale unor cerințe suplimentare în materie de securitate cibernetică pentru achiziționarea sau utilizarea produselor respective în scopuri specifice, inclusiv în cazul în care produsele respective sunt achiziționate sau utilizate în scopuri de securitate națională sau apărare, cu condiția ca aceste cerințe să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii și să fie necesare și proporționale pentru realizarea scopurilor respective.

(2) Fără a aduce atingere Directivelor 2014/24/UE și 2014/25/UE, atunci când sunt achiziționate produse cu elemente digitale care intră în domeniul de aplicare al prezentului regulament, statele membre se asigură că respectarea cerințelor esențiale de securitate cibernetică prevăzute în anexa I la prezentul regulament, inclusiv capacitatea producătorilor de a gestiona în mod eficace vulnerabilitățile, este luată în considerare în procesul de achiziție.

Articolul 6

Cerințe pentru produsele cu elemente digitale

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

(a) îndeplinesc cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I, 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, au fost instalate actualizările de securitate necesare, și

(b) procesele instituite de producător respectă cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

Articolul 7

Produsele importante cu elemente digitale

(1) Produsele cu elemente digitale care au funcționalitatea de bază a unei categorii de produse prevăzute în anexa III sunt considerate produse importante cu elemente digitale și fac obiectul procedurilor de evaluare a conformității menționate la articolul 32 alineatele (2) și (3). Integrarea unui produs cu elemente digitale care are funcționalitatea de bază a unei categorii de produse prevăzute în anexa III nu implică, în sine, faptul că produsul în care acesta este integrat face obiectul procedurilor de evaluare a conformității menționate la articolul 32 alineatele (2) și (3).

(2) Categoriile de produse cu elemente digitale menționate la alineatul (1) din prezentul articol, împărțite în clasele I și II astfel cum sunt prevăzute în anexa III, îndeplinesc cel puțin unul dintre următoarele criterii:

(a) produsul cu elemente digitale îndeplinește în primul rând funcții esențiale pentru securitatea cibernetică a altor produse, rețele sau servicii, inclusiv securizarea autentificării și a accesului, prevenirea și detectarea intruziunilor, securizarea punctelor terminale sau protejarea rețelei;

(b) produsul cu elemente digitale îndeplinește o funcție care prezintă un risc semnificativ de efecte negative în ceea ce privește intensitatea și capacitatea sa de a perturba, controla sau cauza daune unui număr mare de alte produse sau în ceea ce privește sănătatea, securitatea sau siguranța utilizatorilor săi prin manipulare directă, cum ar fi o funcție de sistem central, inclusiv gestionarea rețelei, controlul configurației, virtualizarea sau prelucrarea datelor cu caracter personal.

(3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a modifica anexa III prin includerea în listă a unei noi categorii în cadrul fiecărei clase de categorii de produse cu elemente digitale și prin stabilirea definiției sale, prin mutarea unei categorii de produse dintr-o clasă în alta sau prin retragerea unei categorii existente din lista respectivă. Atunci când evaluează necesitatea de a modifica lista din anexa III, Comisia ține seama de funcționalitățile legate de securitatea cibernetică sau de funcția și de nivelul riscului de securitate cibernetică prezentat de produsele cu elemente digitale, astfel cum se prevede în criteriile menționate la alineatul (2) de la prezentul articol.

Actele delegate menționate la primul paragraf de la prezentul alineat prevăd, după caz, o perioadă de tranziție minimă de 12 luni, în special dacă o nouă categorie de produse importante cu elemente digitale este adăugată în clasa I sau II sau este mutată din clasa I în clasa II, astfel cum se prevede în anexa III, înainte de începerea aplicării procedurilor relevante de evaluare a conformității astfel cum se menționează la articolul 32 alineatele (2) și (3), cu excepția cazului în care se justifică o perioadă de tranziție mai scurtă din motive imperative de urgență.

(4) Până la ... [12 luni de la data intrării în vigoare a prezentului regulament], Comisia adoptă un act de punere în aplicare care precizează descrierea tehnică a categoriilor de produse cu elemente digitale din clasa I și clasa II, astfel cum sunt prevăzute în anexa III, și descrierea tehnică a categoriilor de produse cu elemente digitale astfel cum sunt prevăzute în anexa IV. Acest act de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

Articolul 8

Produsele critice cu elemente digitale

(1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a completa prezentul regulament cu scopul de a stabili ce produse cu elemente digitale care au funcționalitatea de bază a unei categorii de produse ce este prevăzută în anexa IV la prezentul regulament trebuie să obțină un certificat european de securitate cibernetică cu un nivel de asigurare cel puțin „substanțial”, emis în cadrul unui sistem european de certificare a securității cibernetice adoptat în temeiul Regulamentului (UE) 2019/881, pentru a demonstra conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în anexa I la prezentul regulament sau cu părți ale acestora, cu condiția să fi fost adoptat un sistem european de certificare a securității cibernetice care să acopere aceste categorii de produse cu elemente digitale în temeiul Regulamentului (UE) 2019/881 și ca un astfel de sistem să fie disponibil pentru producători. Actele delegate respective specifică nivelul de asigurare necesar care este proporțional cu nivelul riscului de securitate cibernetică asociat produselor cu elemente digitale și ține seama de scopul preconizat al acestora, inclusiv de dependența critică de acestea a entităților esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555.

Înainte de adoptarea unor astfel de acte delegate, Comisia efectuează o evaluare a impactului potențial asupra pieței al măsurilor avute în vedere și desfășoară consultări cu părțile interesate relevante, inclusiv cu Grupul european pentru certificarea securității cibernetice instituit prin Regulamentul (UE) 2019/881. Evaluarea ține seama de gradul de pregătire și de capacitatea statelor membre pentru punerea în aplicare a sistemului european de certificare a securității cibernetice relevant. În cazul în care nu au fost adoptate acte delegate, astfel cum se menționează la primul paragraf al prezentului alineat, produsele cu elemente digitale care au funcționalitatea de bază a unei categorii de produse prevăzute în anexa IV fac obiectul procedurilor de evaluare a conformității menționate la articolul 32 alineatul (3).

Actele delegate menționate la primul paragraf prevăd o perioadă minimă de tranziție de șase luni, cu excepția cazului în care se justifică o perioadă de tranziție mai scurtă din motive imperative de urgență.

(2) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a modifica anexa IV prin adăugarea sau retragerea unor categorii de produse critice cu elemente digitale. La determinarea acestor categorii de produse critice cu elemente digitale și a nivelului de asigurare necesar, în conformitate cu alineatul (1) de la prezentul articol, Comisia ține seama de criteriile menționate la articolul 7 alineatul (2) și asigură faptul că cel puțin unul dintre următoarele criterii este îndeplinit de categoria de produse cu elemente digitale:

(a) există o dependență critică a entităților esențiale menționate la articolul 3 din Directiva (UE) 2022/2555 de categoria de produse cu elemente digitale;

(b) incidentele și vulnerabilitățile exploatate în ceea ce privește categoria de produse cu elemente digitale ar putea duce la perturbări grave ale lanțurilor de aprovizionare critice de pe piața internă.

Înainte de adoptarea unor astfel de acte delegate, Comisia efectuează o evaluare a tipului menționat la alineatul (1).

Actele delegate menționate la primul paragraf prevăd o perioadă minimă de tranziție de șase luni, cu excepția cazului în care se justifică o perioadă de tranziție mai scurtă din motive imperative de urgență.

Articolul 9

Consultarea părților interesate

(1) Atunci când pregătește măsurile de punere în aplicare a prezentului regulament, Comisia consultă părțile interesate relevante și ține seama de opiniile acestora, spre exemplu de ale autorităților relevante ale statelor membre, ale întreprinderile din sectorul privat, inclusiv de ale microîntreprinderilor și ale întreprinderilor mici și mijlocii, ale comunității de software cu sursă deschisă, ale asociațiilor de consumatori, ale mediului academic și ale agențiilor și organelor relevante ale Uniunii, precum și de ale grupurilor de experți instituite la nivelul Uniunii. În special, Comisia consultă și solicită punctele de vedere ale părților interesate respective, într-un mod structurat, după caz, atunci când:

(a) elaborează orientările menționate la articolul 26;

(b) pregătește descrierile tehnice ale categoriilor de produse prevăzute în anexa III în conformitate cu articolul 7 alineatul (4), evaluează necesitatea unor eventuale actualizări ale listei categoriilor de produse în conformitate cu articolul 7 alineatul (3) și cu articolul 8 alineatul (2) sau efectuează evaluarea impactului potențial asupra pieței menționat la articolul 8 alineatul (1), fără a aduce atingere articolului 61;

(c) desfășoară activități pregătitoare pentru evaluarea și revizuirea prezentului regulament.

(2) Comisia organizează sesiuni periodice de consultare și informare, cel puțin o dată pe an, pentru a colecta opiniile părților interesate menționate la alineatul (1) cu privire la punerea în aplicare a prezentului regulament.

Articolul 10

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

În sensul prezentului regulament și pentru a răspunde nevoilor profesioniștilor în sprijinul punerii în aplicare a prezentului regulament, statele membre, cu sprijinul, după caz, al Comisiei, al Centrului european de competențe în materie de securitate cibernetică și al ENISA, respectând pe deplin responsabilitatea statelor membre în domeniul educației, promovează măsuri și strategii care vizează:

(a) dezvoltarea competențelor în materie de securitate cibernetică și crearea de instrumente organizaționale și tehnologice pentru a asigura disponibilitatea unui număr suficient de profesioniști calificați, cu scopul de a sprijini activitățile autorităților de supraveghere a pieței și ale organismelor de evaluare a conformității;

(b) intensificarea colaborării dintre sectorul privat, operatorii economici, inclusiv prin recalificarea sau perfecționarea profesională a angajaților producătorilor, consumatori, furnizorii de formare, precum și administrațiile publice, extinzând astfel opțiunile de care dispun tinerii de a avea acces la locuri de muncă în sectorul securității cibernetice.

Articolul 11

Siguranța generală a produselor

Prin derogare de la articolul 2 alineatul (1) al treilea paragraf litera (b) din Regulamentul (UE) 2023/988, capitolul III, secțiunea 1, capitolele V și VII și capitolele IX-XI din regulamentul respectiv se aplică produselor cu elemente digitale în ceea ce privește aspectele și riscurile sau categoriile de riscuri care nu sunt acoperite de prezentul regulament, în cazul în care produsele respective nu fac obiectul unor cerințe de siguranță specifice prevăzute în alte acte din „legislația de armonizare a Uniunii” în sensul definiției de la articolul 3 punctul 27 din Regulamentul (UE) 2023/988.

Articolul 12

Sistemele de IA cu grad ridicat de risc

(1) Fără a aduce atingere cerințelor privind acuratețea și robustețea prevăzute la articolul 15 din Regulamentul (UE) 2024/1689, 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 temeiul articolului 6 din regulamentul respectiv sunt considerate conforme cu cerințele de securitate cibernetică prevăzute la articolul 15 din regulamentul respectiv în cazul în care:

(a) produsele respective îndeplinesc cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I;

(b) procesele instituite de producător respectă cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II; și

(c) atingerea nivelului de protecție în materie de securitate cibernetică necesar în temeiul articolului 15 din Regulamentul (UE) 2024/1689 este demonstrată în declarația de conformitate a UE emisă în temeiul prezentului regulament.

(2) Pentru produsele cu elemente digitale și cerințele de securitate cibernetică menționate la alineatul (1) din prezentul articol, se aplică procedura relevantă de evaluare a conformității prevăzută la articolul 43 din Regulamentul (UE) 2024/1689. În scopul efectuării acestei evaluări, organismele notificate care au competența de a verifica conformitatea sistemelor de IA cu grad ridicat de risc în temeiul Regulamentului (UE) 2024/1689 au, de asemenea, competența de a verifica 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 39 din prezentul regulament să fi fost evaluată în contextul procedurii de notificare în temeiul Regulamentului (UE) 2024/1689.

(3) Prin derogare de la alineatul (2) de la prezentul articol, produsele importante cu elemente digitale enumerate în anexa III la prezentul regulament, care fac obiectul procedurilor de evaluare a conformității menționate la articolul 32 alineatul (2) literele (a) și (b) și la articolul 32 alineatul (3) din prezentul regulament și produsele critice cu elemente digitale astfel cum sunt enumerate în anexa IV la prezentul regulament, în cazul cărora trebuie să fie obținut un certificat european de securitate cibernetică în temeiul articolului 8 alineatul (1) din prezentul regulament, sau, dacă această obligație nu este aplicabilă, care fac obiectul procedurilor de evaluare a conformității menționate la articolul 32 alineatul (3) din prezentul regulament și care sunt clasificate ca sisteme de IA cu grad ridicat de risc în temeiul articolului 6 din Regulamentul (UE) 2024/1689 și cărora li se aplică procedura de evaluare a conformității bazată pe control intern menționată în anexa VI la Regulamentul (UE) 2024/1689, fac obiectul procedurilor de evaluare a conformității prevăzute de prezentul regulament în ceea ce privește cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament.

(4) Producătorii de produse cu elemente digitale astfel cum sunt menționate la alineatul (1) de la prezentul articol pot participa la spațiile de testare în materie de reglementare a IA menționate la articolul 57 din Regulamentul (UE) 2024/1689.

Capitolul II
Obligațiile operatorilor economici și dispoziții privind software-ul liber și cu sursă deschisă

Articolul 13

Obligațiile producătorilor

(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 de securitate cibernetică prevăzute în anexa I partea I.

(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 și de a reduce cât mai mult impactul acestora, inclusiv în ceea ce privește sănătatea și siguranța utilizatorilor.

(3) Evaluarea riscurilor de securitate cibernetică este documentată și actualizată, după caz, pe parcursul unei perioade de asistență care urmează să fie stabilită în conformitate cu alineatul (8) din prezentul articol. Respectiva evaluare a riscurilor de securitate cibernetică cuprinde cel puțin o analiză a riscurilor în materie de securitate cibernetică, efectuată pe baza scopului preconizat și a utilizării previzibile în mod rezonabil, precum și a condițiilor de utilizare a produsului cu elemente digitale, cum ar fi mediul operațional sau activele care urmează să fie protejate, ținând seama de perioada de timp în care se preconizează că produsul va fi în uz. Evaluarea riscurilor de securitate cibernetică indică dacă și, în caz afirmativ, în ce mod cerințele de securitate prevăzute în partea I punctul 2 din anexa I sunt aplicabile produsului relevant cu elemente digitale și modul în care aceste cerințe sunt puse în aplicare, în conformitate cu prevederile evaluării riscurilor de securitate cibernetică. Aceasta indică, de asemenea, modul în care producătorul trebuie să aplice partea I punctul 1 din anexa I, precum și cerințele de gestionare a vulnerabilităților prevăzute în anexa I partea II.

(4) Atunci când introduce pe piață un produs cu elemente digitale, producătorul include o evaluare a riscurilor de securitate cibernetică menționate la alineatul (3) din prezentul articol în documentația tehnică solicitată în temeiul articolului 31 și în anexa VII. În cazul produselor cu elemente digitale astfel cum sunt menționate la articolul 12 care fac, de asemenea, obiectul altor acte juridice ale Uniunii, evaluarea riscurilor de securitate cibernetică poate face parte din evaluarea riscurilor impusă de respectivele acte juridice ale Uniunii. În cazul în care anumite cerințe esențiale de securitate cibernetică nu sunt aplicabile produsului cu elemente digitale, producătorul include o justificare clară în acest sens în documentația tehnică respectivă.

(5) În scopul respectării obligației prevăzute la alineatul (1), producătorii exercită diligența necesară atunci când integrează componente obținute de la terți, astfel încât respectivele componente să nu compromită securitatea cibernetică a produsului cu elemente digitale, inclusiv atunci când integrează componente ale unui software liber și cu sursă deschisă care nu au fost puse la dispoziție pe piață în cursul unei activități comerciale.

(6) La identificarea vulnerabilității unei componente, inclusiv a unei componente cu sursă deschisă, care este integrată în produsul cu elemente digitale, producătorii raportează vulnerabilitatea respectivă persoanei sau entității care produce sau întreține componenta în cauză și abordează și remediază vulnerabilitatea în conformitate cu cerințele privind gestionarea vulnerabilităților prevăzute în anexa I partea II. În cazul în care producătorii au realizat o modificare a software-ului sau a hardware-ului pentru a aborda vulnerabilitatea componentei respective, aceștia partajează codul sau documentația relevantă cu persoana sau entitatea care produce sau întreține componenta, după caz, într-un format care poate fi citit automat.

(7) Producătorii documentează în mod sistematic, într-un mod proporțional cu natura și cu riscurile de securitate cibernetică, aspectele de securitate cibernetică relevante ale produselor cu elemente digitale, inclusiv vulnerabilitățile de care iau cunoștință și orice informații relevante furnizate de terți, și, după caz, actualizează evaluarea riscurilor de securitate cibernetică pentru produsele respective.

(8) Producătorii se asigură, atunci când introduc pe piață un produs cu elemente digitale, precum și pe parcursul perioadei de asistență, că vulnerabilitățile produsului respectiv, inclusiv ale componentelor sale, sunt gestionate în mod eficace și în conformitate cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

Producătorii stabilesc perioada de asistență astfel încât aceasta să reflecte perioada de timp în care se preconizează că produsul va fi în uz, ținând seama, în special, de așteptările rezonabile ale utilizatorilor, de natura produsului, inclusiv de scopul său preconizat, precum și de dreptul relevant al Uniunii care stabilește durata de viață a produselor cu elemente digitale. Atunci când stabilesc perioada de asistență, producătorii pot lua în considerare, de asemenea, perioadele de asistență aferente produselor cu elemente digitale care oferă o funcționalitate similară introduse pe piață de alți producători, disponibilitatea mediului de operare, perioadele de asistență aferente componentelor integrate care oferă funcții de bază și care sunt furnizate de părți terțe, precum și orientările relevante furnizate de grupul specific de cooperare administrativă (ADCO) instituit în temeiul articolului 52 alineatul (15) și de către Comisie. Aspectele de care trebuie să se țină seama pentru a determina perioada de asistență sunt luate în considerare într-un mod care să asigure proporționalitatea.

Fără a aduce atingere celui de-al doilea paragraf, perioada de asistență este de cel puțin cinci ani. În cazul în care se preconizează că produsul cu elemente digitale va fi utilizat mai puțin de cinci ani, perioada de asistență trebuie să corespundă duratei de utilizare preconizate.

Ținând seama de recomandările ADCO menționate la articolul 52 alineatul (16), Comisia poate adopta acte delegate în conformitate cu articolul 61 pentru a completa prezentul regulament prin specificarea perioadei minime de asistență pentru anumite categorii de produse în cazul în care datele de supraveghere a pieței sugerează perioade de asistență inadecvate.

Producătorii includ în documentația tehnică informațiile care au fost luate în considerare pentru a stabili perioada de asistență a unui produs cu elemente digitale, astfel cum se prevede în anexa VII.

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

(9) Producătorii se asigură că fiecare actualizare de securitate, astfel cum se menționează în partea II punctul 8 din anexa I, care a fost pusă la dispoziția utilizatorilor în cursul perioadei de asistență, rămâne disponibilă după ce a fost emisă pentru o perioadă de cel puțin 10 ani sau pentru restul perioadei de asistență, oricare dintre acestea este mai lungă.

(10) În cazul în care un producător a introdus pe piață versiuni ulterioare modificate substanțial ale unui produs software, producătorul respectiv poate asigura conformitatea cu cerința esențială de securitate cibernetică prevăzută în partea II punctul 2 din anexa I numai pentru versiunea pe care producătorul a introdus-o ultima dată pe piață, cu condiția ca utilizatorii versiunilor introduse anterior pe piață să aibă acces gratuit la ultima versiune introdusă pe piață și să nu suporte costuri suplimentare pentru a ajusta echipamentele hardware și programele software în care utilizează versiunea originală a produsului respectiv.

(11) Producătorii pot întreține arhive software publice care să îmbunătățească accesul utilizatorilor la versiunile istorice. În aceste cazuri, utilizatorii sunt informați într-un mod clar și ușor accesibil, cu privire la riscurile asociate utilizării software-ului care nu beneficiază de asistență.

(12) Înainte de a introduce pe piață un produs cu elemente digitale, producătorii întocmesc documentația tehnică menționată la articolul 31.

Aceștia efectuează procedurile alese de evaluare a conformității astfel cum sunt menționate la articolul 32 sau dispun efectuarea acestora.

În cazul în care conformitatea produsului cu elemente digitale cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și a proceselor instituite de producător cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II fost demonstrată prin respectiva procedură de evaluare a conformității, producătorii întocmesc declarația de conformitate UE în conformitate cu articolul 28 și aplică marcajul CE în conformitate cu articolul 30.

(13) Producătorii păstrează documentația tehnică și declarația de conformitate UE la dispoziția autorităților de supraveghere a pieței timp de cel puțin 10 ani de la introducerea pe piață a produsului cu elemente digitale sau pe parcursul perioadei de asistență, oricare dintre acestea este mai lungă.

(14) Producătorii se asigură că există proceduri care să garanteze conformitatea continuă cu prezentul regulament a produselor cu elemente digitale care fac parte dintr-o producție în serie. Producătorii țin 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 astfel cum sunt menționate la articolul 27 în raport cu care se declară conformitatea produsului cu elemente digitale sau prin aplicarea cărora este verificată conformitatea acestuia.

(15) Producătorii se asigură de faptul că produsele lor cu elemente digitale poartă tipul, lotul sau numărul de serie sau un alt element de identificare sau, în cazul în care acest lucru nu este posibil, că informațiile respective sunt furnizate pe ambalaj sau într-un document care însoțește produsul cu elemente digitale.

(16) Producătorii indică pe produsul cu elemente digitale, pe ambalajul acestuia sau într-un document care însoțește produsul cu elemente digitale numele, denumirea comercială înregistrată sau marca înregistrată a producătorului, precum și adresa poștală, adresa de e-mail și alte date de contact digitale, precum și, dacă este cazul, site-ul web la care pot fi contactați. Aceste informații se includ, de asemenea, în informațiile și instrucțiunile pentru utilizator prevăzute în anexa II. Datele de contact sunt redactate într-o limbă ușor de înțeles de către utilizatori și autoritățile de supraveghere a pieței.

(17) În sensul prezentului regulament, producătorii desemnează un ghișeu unic pentru a le permite utilizatorilor să comunice direct și rapid cu aceștia, inclusiv pentru a facilita raportarea vulnerabilităților produsului cu elemente digitale.

Producătorii se asigură că ghișeul unic este ușor de identificat de către utilizatori. Aceștia includ, de asemenea, ghișeul unic în informațiile și instrucțiunile pentru utilizatori prevăzute în anexa II.

Ghișeul unic permite utilizatorilor să își aleagă mijloacele de comunicare preferate și nu limitează aceste mijloace la instrumente automatizate.

(18) Producătorii se asigură că produsele cu elemente digitale sunt însoțite de informațiile și instrucțiunile pentru utilizatori prevăzute în anexa II, în format electronic sau pe hârtie. Aceste informații și instrucțiuni trebuie să fie furnizate într-o limbă ușor de înțeles de către utilizatori și autoritățile de supraveghere a pieței. 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. Producătorii păstrează informațiile și instrucțiunile pentru utilizatori stabilite în anexa II la dispoziția utilizatorilor și a autorităților de supraveghere a pieței timp de cel puțin 10 ani de la introducerea pe piață a produsului cu elemente digitale sau pe parcursul perioadei de asistență, oricare dintre acestea este mai lungă. În cazul în care aceste informații și instrucțiuni sunt furnizate online, producătorii se asigură că ele sunt accesibile, prezentate într-un format ușor de utilizat și disponibile online timp de cel puțin 10 ani după introducerea pe piață a produsului cu elemente digitale sau pe parcursul perioadei de asistență, oricare dintre acestea este mai lungă.

(19) Producătorii se asigură că data de încheiere a perioadei de asistență menționate la alineatul (8), incluzând cel puțin luna și anul, este specificată în mod clar și inteligibil la momentul achiziției într-un mod ușor accesibil și, după caz, pe produsul cu elemente digitale, pe ambalajul acestuia sau prin mijloace digitale.

În cazul în care acest lucru este fezabil din punct de vedere tehnic, având în vedere natura produsului cu elemente digitale, producătorii afișează o notificare adresată utilizatorilor prin care îi informează că produsul lor cu elemente digitale a ajuns la sfârșitul perioadei sale de asistență.

(20) Producătorii fie prezintă o copie a declarației de conformitate UE, fie prezintă o declarație de conformitate simplificată a UE împreună cu produsul cu elemente digitale. În cazul în care este pusă la dispoziție o declarație de conformitate simplificată a UE, aceasta conține adresa de internet exactă la care poate fi accesată declarația de conformitate UE completă.

(21) De la introducerea pe piață și pe parcursul perioadei 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 de securitate cibernetică prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor producătorului sau pentru a retrage ori a rechema produsul, după caz.

(22) 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 autoritatea respectivă, 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 de securitate cibernetică prevăzute în anexa I. Producătorii 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.

(23) Un producător care își încetează activitatea și, în consecință, nu este în măsură să respecte 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 produselor cu elemente digitale relevante introduse pe piață cu privire la încetarea iminentă a activității.

(24) Comisia poate specifica, prin intermediul actelor de punere în aplicare care țin seama de standardele și de bunele practici europene sau internaționale, formatul și elementele listei materialelor software menționate în partea II punctul 1 din anexa I. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

(25) Pentru a evalua dependența statelor membre și a Uniunii în ansamblu de componentele software și, în special, de componentele care se califică drept software liber și cu sursă deschisă, ADCO poate decide să efectueze o evaluare a dependenței la nivelul Uniunii pentru anumite categorii de produse cu elemente digitale. În acest scop, autoritățile de supraveghere a pieței pot solicita producătorilor acestor categorii de produse cu elemente digitale să furnizeze listele relevante ale materialelor software, astfel cum se menționează în partea II punctul 1 din anexa I. Pe baza acestor informații, autoritățile de supraveghere a pieței pot furniza ADCO informații anonimizate și agregate cu privire la dependențele de software. ADCO prezintă grupului de cooperare instituit în temeiul articolului 14 din Directiva (UE) 2022/2555 un raport privind rezultatele evaluării dependenței.

Articolul 14

Obligațiile de raportare ale producătorilor

(1) Un producător notifică orice vulnerabilitate exploatată activ conținută în produsul cu elemente digitale de care ia cunoștință simultan către CSIRT desemnată drept coordonator, în conformitate cu alineatul (7) din prezentul articol, precum și către ENISA. Producătorul notifică vulnerabilitatea exploatată activ prin intermediul platformei unice de raportare instituite în temeiul articolului 16.

(2) În sensul notificării menționate la alineatul (1), producătorul prezintă:

(a) o notificare de alertă timpurie cu privire la o vulnerabilitate exploatată activ, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care producătorul a luat cunoștință de aceasta, indicând, după caz, statele membre pe teritoriul cărora producătorul are cunoștință că produsul său cu elemente digitale a fost pus la dispoziție;

(b) cu excepția cazului în care informațiile relevante au fost deja furnizate, 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 activ, care furnizează informații generale, după caz, cu privire la produsul cu elemente digitale în cauză, la natura generală a exploatării și a vulnerabilității în cauză, precum și la orice măsuri corective sau de atenuare luate și la orice măsuri corective sau de atenuare pe care utilizatorii le pot lua și care indică, de asemenea, dacă este cazul, gradul de sensibilitate pe care producătorul îl atribuie informațiilor notificate;

(c) cu excepția cazului în care informațiile relevante au fost deja furnizate, un raport final, în termen de cel mult 14 zile de la data la care este disponibilă o măsură corectivă sau de atenuare, care să includă cel puțin următoarele elemente:

(i) o descriere a vulnerabilității, inclusiv gravitatea și impactul acesteia;

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

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

(3) Un producător notifică orice incident sever care afectează securitatea produsului cu elemente digitale de care a luat cunoștință simultan către CSIRT desemnată drept coordonator, în conformitate cu alineatul (7) de la prezentul articol, precum și către ENISA. Producătorul notifică incidentul respectiv prin intermediul platformei unice de raportare instituite în temeiul articolului 16.

(4) În sensul notificării menționate la alineatul (3), producătorul prezintă:

(a) o notificare de alertă timpurie cu privire la un incident grav care are un impact asupra securității produsului cu elemente digitale, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la data la care producătorul a luat cunoștință de acesta, inclusiv, cel puțin, dacă se suspectează că incidentul este cauzat de acte ilegale sau răuvoitoare, notificarea indicând, de asemenea, după caz, statele membre pe teritoriul cărora producătorul are cunoștință de faptul că produsul său cu elemente digitale a fost pus la dispoziție;

(b) cu excepția cazului în care informațiile relevante au fost deja furnizate, o notificare a incidentului, fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la data la care producătorul a luat cunoștință de incident, notificarea conținând informații generale, dacă sunt disponibile, cu privire la natura incidentului, o evaluare inițială a incidentului, precum și orice măsuri corective sau de atenuare care au fost adoptate și măsuri corective sau de atenuare pe care utilizatorii le pot lua și care indică, de asemenea, după caz, gradul de sensibilitate atribuit de producător informațiilor notificate;

(c) cu excepția cazului în care informațiile relevante au fost deja furnizate, un raport final, în termen de o lună de la transmiterea notificării incidentului 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 cauza principală care este probabil că a declanșat incidentul;

(iii) măsurile de atenuare aplicate și în curs.

(5) În sensul alineatului (3), un incident care are un impact asupra securității produsului cu elemente digitale este considerat grav în cazul în care:

(a) afectează în mod negativ sau poate afecta în mod negativ capacitatea unui produs cu elemente digitale de a proteja disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor sau a funcțiilor sensibile sau importante; sau

(b) a condus sau poate conduce la introducerea sau executarea unui cod dăunător într-un produs cu elemente digitale sau în rețeaua și sistemele informatice ale unui utilizator al produsului cu elemente digitale.

(6) În cazul în care este necesar, CSIRT desemnată drept coordonator care primește inițial notificarea poate solicita producătorilor să furnizeze un raport intermediar privind actualizările relevante ale statutului în ceea ce privește vulnerabilitatea exploatată activ sau privind incidentul grav care are un impact asupra securității produsului cu elemente digitale.

(7) Notificările menționate la alineatele (1) și (3) din prezentul articol se transmit prin intermediul platformei unice de raportare menționate la articolul 16, utilizând unul dintre punctele terminale de notificare electronică menționate la articolul 16 alineatul (1). Notificarea se transmite utilizând punctul terminal de notificare electronică al CSIRT desemnate drept coordonator a statului membru în care producătorii își au sediul principal în Uniune și este accesibilă simultan ENISA.

În sensul prezentului regulament, se consideră că un producător are sediul principal în Uniune în statul membru în care sunt luate în mod preponderent deciziile legate de securitatea cibernetică a produselor sale cu elemente digitale. Dacă un astfel de stat membru nu poate fi stabilit, sediul principal este considerat a fi în statul membru în care producătorul în cauză are sediul cu cel mai mare număr de angajați din Uniune.

În cazul în care un producător nu are sediul principal în Uniune, acesta transmite notificările menționate la alineatele (1) și (3) utilizând punctul terminal de notificare electronică a CSIRT desemnate drept coordonator din statul membru stabilit pe baza următoarei ordini a criteriilor și pe baza informațiilor aflate la dispoziția producătorului:

(a) statul membru în care este stabilit reprezentantul autorizat care acționează în numele producătorului pentru cel mai mare număr de produse cu elemente digitale ale producătorului respectiv;

(b) statul membru în care este stabilit importatorul care introduce pe piață cel mai mare număr de produse cu elemente digitale ale producătorului respectiv;

(c) statul membru în care este stabilit distribuitorul care pune la dispoziție pe piață cel mai mare număr de produse cu elemente digitale ale producătorului respectiv;

(d) statul membru în care se află cel mai mare număr de utilizatori de produse cu elemente digitale ale producătorului respectiv.

În ceea ce privește al treilea paragraf litera (d), un producător poate transmite notificări referitoare la orice vulnerabilitate ulterioară exploatată activ sau la orice incident grav ulterior care are un impact asupra securității produsului cu elemente digitale către aceeași CSIRT desemnată drept coordonator căreia i-a transmis notificarea inițială.

(8) După ce a luat cunoștință de o vulnerabilitate exploatată activ sau de un incident grav care are un impact asupra securității produsului cu elemente digitale, producătorul informează utilizatorii afectați ai produsului cu elemente digitale și, după caz, toți utilizatorii cu privire la vulnerabilitatea sau la incidentul respectiv și, dacă este necesar, cu privire la atenuarea riscurilor și la orice măsuri corective pe care utilizatorii le pot aplica pentru a atenua impactul vulnerabilității sau al incidentului respectiv, după caz, într-un format structurat, ușor de prelucrat automat și care poate fi citit automat. În cazul în care producătorul nu informează utilizatorii produsului cu elemente digitale în timp util, CSIRT notificate desemnate drept coordonatori pot furniza astfel de informații utilizatorilor atunci când ele sunt considerate a fi proporționale și necesare pentru prevenirea sau atenuarea impactului incidentului sau al vulnerabilității respective.

(9) Până la ... [12 luni de la data intrării în vigoare a prezentului regulament], Comisia adoptă acte delegate în conformitate cu articolul 61 din prezentul regulament pentru a completa prezentul regulament prin specificarea termenelor și condițiilor de aplicare a motivelor legate de securitatea cibernetică în legătură cu întârzierea difuzării notificărilor, astfel cum se menționează la articolul 16 alineatul (2) din prezentul regulament. Comisia cooperează cu rețeaua CSIRT instituită în temeiul articolului 15 din Directiva (UE) 2022/2555 și cu ENISA la pregătirea proiectelor de acte delegate.

(10) Comisia poate, prin intermediul unor acte de punere în aplicare, să precizeze mai detaliat formatul notificărilor și procedurile de efectuare a notificărilor la care se face referire în prezentul articol, precum și la articolele 15 și 16. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2). Comisia cooperează cu rețeaua CSIRT și cu ENISA la pregătirea acestor proiecte de acte de punere în aplicare.

Articolul 15

Raportarea voluntară

(1) Producătorii, precum și alte persoane fizice sau juridice pot notifica, în mod voluntar, unei CSIRT desemnate drept coordonator sau ENISA, orice vulnerabilitate conținută într-un produs cu elemente digitale, precum și orice amenințări cibernetice care ar putea afecta profilul de risc al unui produs cu elemente digitale.

(2) Producătorii, precum și alte persoane fizice sau juridice pot notifica, în mod voluntar, unei CSIRT desemnate drept coordonator sau ENISA, orice incident care are un impact asupra securității produsului cu elemente digitale, precum și incidentele evitate la limită care ar fi putut avea drept rezultat un astfel de incident.

(3) CSIRT desemnată drept coordonator sau ENISA prelucrează notificările menționate la alineatele (1) și (2) din prezentul articol în conformitate cu procedura prevăzută la articolul 16.

CSIRT desemnată drept coordonator poate acorda prioritate prelucrării notificărilor obligatorii în detrimentul notificărilor voluntare.

(4) În cazul în care o persoană fizică sau juridică, alta decât producătorul, notifică o vulnerabilitate exploatată activ sau un incident grav care are un impact asupra securității unui produs cu elemente digitale în conformitate cu alineatul (1) sau (2), CSIRT desemnată drept coordonator informează producătorul fără întârzieri nejustificate.

(5) CSIRT desemnate drept coordonatori, precum și ENISA asigură confidențialitatea și protecția adecvată a informațiilor furnizate de o persoană fizică sau juridică care face notificarea. Fără a aduce atingere prevenirii, investigării, depistării și urmăririi penale a infracțiunilor, raportarea voluntară nu are ca rezultat impunerea niciunei obligații suplimentare unei persoane fizice sau juridice care face notificarea și căreia nu i s-ar fi aplicat această obligație dacă nu ar fi transmis notificarea.

Articolul 16

Instituirea unei platforme unice de raportare

(1) În scopul notificărilor menționate la articolul 14 alineatele (1) și (3) și la articolul 15 alineatele (1) și (2) și pentru a simplifica obligațiile de raportare ale producătorilor, ENISA instituie o platformă unică de raportare. Operațiunile curente ale respectivei platforme unice de raportare sunt gestionate și întreținute de ENISA. Arhitectura platformei unice de raportare permite statelor membre și ENISA să instituie propriile puncte terminale de notificare electronică.

(2) După primirea unei notificări, CSIRT desemnată drept coordonator care a primit inițial notificarea difuzează fără întârziere notificarea prin intermediul platformei unice de raportare către CSIRT desemnate drept coordonatori pe teritoriul cărora producătorul a indicat că produsul cu elemente digitale a fost pus la dispoziție.

În circumstanțe excepționale și, în special, la cererea producătorului și având în vedere nivelul de sensibilitate a informațiilor notificate indicat de producător în temeiul articolului 14 alineatul (2) litera (a) din prezentul regulament, diseminarea notificării poate fi amânată din motive justificate legate de securitatea cibernetică pentru o perioadă de timp strict necesară, inclusiv în cazul în care o vulnerabilitate face obiectul unei proceduri coordonate de divulgare a vulnerabilităților, astfel cum se menționează la articolul 12 alineatul (1) din Directiva (UE) 2022/2555. În cazul în care CSIRT decide să refuze o notificare, aceasta informează imediat ENISA cu privire la decizie și furnizează atât o justificare pentru refuzul notificării, cât și o indicație cu privire la momentul în care va difuza notificarea în conformitate cu procedura de diseminare prevăzută la prezentul alineat. ENISA poate sprijini CSIRT cu privire la aplicarea motivelor legate de securitatea cibernetică în ceea ce privește întârzierea difuzării notificării.

În circumstanțe excepționale, atunci când producătorul indică în notificarea menționată la articolul 14 alineatul (2) litera (b):

(a) că vulnerabilitatea notificată a fost exploatată în mod activ de un actor rău-intenționat și, conform informațiilor disponibile, nu a fost exploatată în niciun alt stat membru decât cel al CSIRT desemnate drept coordonator căruia producătorul i-a notificat vulnerabilitatea;

(b) că orice diseminare ulterioară imediată a vulnerabilității notificate ar conduce probabil la furnizarea de informații a căror divulgare ar fi contrară intereselor esențiale ale statului membru respectiv; sau

(c) că vulnerabilitatea notificată prezintă un risc iminent ridicat în materie de securitate cibernetică care decurge din diseminarea ulterioară;

numai informațiile conform cărora producătorul a efectuat o notificare, informațiile generale cu privire la produs, informațiile privind natura generală a exploatării și informațiile cu privire la faptul că au fost invocate motive legate de securitate sunt puse simultan la dispoziția ENISA până când notificarea completă este transmisă către CSIRT în cauză și ENISA. În cazul în care, pe baza informațiilor respective, ENISA consideră că există un risc sistemic care afectează securitatea pe piața internă, aceasta recomandă CSIRT destinatare să disemineze notificarea completă celorlalte CSIRT desemnate drept coordonatori și ENISA.

(3) După primirea unei notificări privind o vulnerabilitate exploatată activ a unui produs cu elemente digitale sau privind un incident grav care are un impact asupra securității unui produs cu elemente digitale, CSIRT desemnate drept coordonatori furnizează autorităților de supraveghere a pieței din statele lor membre informațiile notificate necesare autorităților de supraveghere a pieței pentru a-și îndeplini obligațiile care le revin în temeiul prezentului regulament.

(4) ENISA ia măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității platformei unice de raportare și informațiile transmise sau difuzate prin intermediul platformei unice de raportare. Aceasta notifică fără întârzieri nejustificate orice incident de securitate care afectează platforma unică de raportare rețelei CSIRT, precum și Comisiei.

(5) ENISA, în cooperare cu rețeaua CSIRT, furnizează și pune în aplicare specificații privind măsurile tehnice, operaționale și organizatorice referitoare la instituirea, întreținerea și funcționarea sigură a platformei unice de raportare menționate la alineatul (1), inclusiv cel puțin mecanismele de securitate legate de instituirea, funcționarea și întreținerea platformei unice de raportare, precum și punctele terminale de notificare electronică instituite de echipele CSIRT desemnate drept coordonatori la nivel național și de ENISA la nivelul Uniunii, inclusiv aspectele procedurale pentru a se asigura că, în cazul în care o vulnerabilitate notificată nu dispune de măsuri corective sau de atenuare, informațiile cu privire la vulnerabilitatea respectivă sunt partajate în conformitate cu protocoale stricte de securitate și pe baza principiului necesității de a cunoaște.

(6) În cazul în care CSIRT desemnată drept coordonator a fost informată cu privire la o vulnerabilitate exploatată activ în cadrul unei proceduri coordonate de divulgare a vulnerabilităților, astfel cum se menționează la articolul 12 alineatul (1) din Directiva (UE) 2022/2555, CSIRT desemnată drept coordonator care primește inițial notificarea poate întârzia diseminarea notificării relevante prin intermediul platformei unice de raportare, pe baza unor motive justificate legate de securitatea cibernetică, pentru o perioadă care nu depășește ceea ce este strict necesar și până când părțile implicate în divulgarea coordonată a vulnerabilităților își dau consimțământul. Această cerință nu împiedică producătorii să notifice o astfel de vulnerabilitate în mod voluntar, în conformitate cu procedura prevăzută la prezentul articol.

Articolul 17

Alte dispoziții referitoare la raportare

(1) ENISA poate 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 articolului 14 alineatele (1) și (3) și articolului 15 alineatele (1) și (2) din prezentul regulament dacă aceste informații sunt relevante pentru gestionarea coordonată la nivel operațional a incidentelor și crizelor de securitate cibernetică de mare amploare. Pentru a stabili această relevanță, ENISA poate lua în considerare analizele tehnice efectuate de rețeaua CSIRT, dacă sunt disponibile.

(2) În cazul în care sensibilizarea publicului este necesară pentru a preveni sau a atenua un incident grav care are un impact asupra securității produsului cu elemente digitale sau pentru a gestiona un incident în curs sau în cazul în care divulgarea incidentului este în alt mod în interesul public, CSIRT desemnată drept coordonator a statului membru relevant poate, după consultarea producătorului în cauză și, după caz, în cooperare cu ENISA, să informeze publicul cu privire la incident sau să solicite producătorului să facă acest lucru.

(3) Pe baza notificărilor primite în temeiul articolului 14 alineatele (1) și (3) și articolului 15 alineatele (1) și (2) din prezentul regulament, ENISA pregătește, la fiecare 24 de luni, un raport tehnic 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 articolul 14 alineatele (1) și (3) din prezentul regulament. 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.

(4) Simplul act de notificare în conformitate cu articolul 14 alineatele (1) și (3) sau cu articolul 15 alineatele (1) și (2) nu presupune o răspundere mai mare pentru persoana fizică sau juridică care face notificarea.

(5) După ce este disponibilă o actualizare de securitate sau o altă formă de măsură corectivă sau de atenuare, ENISA, de comun acord cu producătorul produsului cu elemente digitale în cauză, adaugă vulnerabilitatea cunoscută public notificată în temeiul articolului 14 alineatul (1) sau al articolului 15 alineatul (1) din prezentul regulament în baza de date europeană privind vulnerabilitățile instituită în temeiul articolului 12 alineatul (2) din Directiva (UE) 2022/2555.

(6) CSIRT desemnate drept coordonatori oferă asistență tehnică în ceea ce privește obligațiile de raportare în temeiul articolului 14 producătorilor și, în special, producătorilor care se califică drept microîntreprinderi sau întreprinderi mici sau mijlocii.

Articolul 18

Reprezentanți autorizați

(1) Un fabricant poate numi, prin mandat scris, un reprezentant autorizat.

(2) Obligațiile stabilite la articolul 13 alineatul (1)-(11), la articolul 13 alineatul (12) primul paragraf și la articolul 13 alineatul (14) nu fac parte din mandatul reprezentantului autorizat.

(3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la producător. Reprezentantul autorizat furnizează, la cerere, 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 28 și documentația tehnică menționată la articolul 31 la dispoziția autorităților de supraveghere a pieței timp de cel puțin 10 ani de la introducerea pe piață a produsului cu elemente digitale sau pe durata perioadei de asistență, oricare din ele este mai lungă;

(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 riscurilor reprezentate de produsul cu elemente digitale acoperit de mandatul reprezentantului autorizat.

Articolul 19

Obligațiile importatorilor

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

(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 astfel cum sunt menționate la articolul 32;

(b) producătorul a întocmit documentația tehnică;

(c) produsul cu elemente digitale poartă marcajul CE menționat la articolul 30 și este însoțit de declarația de conformitate UE menționată la articolul 13 alineatul (20) și de informațiile și instrucțiunile de utilizare prevăzute în anexa II, într-o limbă ușor de înțeles de către utilizatori și autoritățile de supraveghere a pieței;

(d) fabricantul a respectat cerințele prevăzute la articolul 13 alineatele (15), (16) și (19).

În sensul prezentului alineat, importatorii sunt în măsură să furnizeze documentele necesare care dovedesc îndeplinirea cerințelor prevăzute la prezentul articol.

(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 prezentul regulament, importatorul nu introduce produsul pe piață până când produsul respectiv sau procesele instituite de producător nu au fost aduse în conformitate cu prezentul regulament. 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.

În cazul în care un importator are motive să creadă că un produs cu elemente digitale poate prezenta un risc semnificativ de securitate cibernetică având în vedere factori de risc fără caracter tehnic, importatorul informează autoritățile de supraveghere a pieței în acest sens. La primirea acestor informații, autoritățile de supraveghere a pieței urmează procedurile menționate la articolul 54 alineatul (2).

(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, adresa de e-mail sau orice alte date digitale de contact, 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 care știu sau au motive să creadă că un produs cu elemente digitale pe care l-au introdus pe piață nu este conform prezentului regulament, iau de îndată măsurile corective necesare pentru a asigura conformitatea produsului cu prezentul regulament sau pentru a retrage sau a rechema produsul, după caz.

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.

(6) Importatorii păstrează o copie a declarației de conformitate UE la dispoziția autorităților de supraveghere a pieței timp de cel puțin zece ani de la introducerea pe piață a produsului sau pe durata perioadei de asistență, oricare din ele este mai lungă și se asigură că documentația tehnică poate fi pusă la dispoziția acestor autorități, la cerere.

(7) 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 de securitate cibernetică prevăzute în anexa I partea I și a proceselor instituite de producător cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II. 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.

(8) 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 20

Obligațiile distribuitorilor

(1) În cazul în care pun la dispoziție pe piață un produs cu elemente digitale, distribuitorii acordă o atenție deosebită cerințelor stabilite în prezentul 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 13 alineatele (15), (16), (18), (19) și (20) și la articolul 19 alineatul (4) și dacă au furnizat distribuitorului toate documentele necesare.

(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 de securitate cibernetică 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 cu prezentul regulament. În plus, atunci când produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, distribuitorul informează, fără întârzieri nejustificate, 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 prezentul regulament se asigură că se iau 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.

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 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 prezentul regulament. 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) Atunci când distribuitorul unui produs cu elemente digitale constată, pe baza informațiilor pe care le deține, că producătorul produsului respectiv și-a încetat activitatea și, în consecință, nu este în măsură să respecte obligațiile prevăzute în prezentul regulament, distribuitorul informează, fără întârzieri nejustificate, 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 21

Situațiile în care obligațiile producătorilor se aplică importatorilor și distribuitorilor

Importatorul sau distribuitorul este considerat producător în sensul prezentului regulament și i se aplică articolele 13 și 14 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 unui produs cu elemente digitale deja introdus pe piață.

Articolul 22

Alte cazuri în care se aplică obligațiile producătorilor

(1) O persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul, care efectuează o modificare substanțială a unui produs cu elemente digitale și pune produsul respectiv la dispoziție pe piață este considerată producător în sensul prezentului regulament.

(2) Persoana menționată la alineatul (1) de la prezentul articol este supusă obligațiilor prevăzute la articolele 13 și 14 pentru partea produsului cu elemente digitale 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 23

Identificarea operatorilor economici

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

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

(b) dacă sunt disponibile, 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 10 ani de la data la care le-a fost furnizat produsul cu elemente digitale și timp de 10 ani de la data la care aceștia au furnizat produsul, după caz.

Articolul 24

Obligațiile administratorilor de software cu sursă deschisă

(1) Administratorii de software cu sursă deschisă instituie și documentează în mod verificabil o politică de securitate cibernetică pentru a încuraja dezvoltarea unui produs securizat cu elemente digitale, precum și gestionarea eficace a vulnerabilităților de către dezvoltatorii produsului respectiv. Politica respectivă încurajează, de asemenea, raportarea voluntară a vulnerabilităților, astfel cum se prevede la articolul 15, de către dezvoltatorii produsului respectiv și ține seama de natura specifică a administratorului software-ului cu sursă deschisă și de modalitățile juridice și organizatorice care i se aplică. Politica respectivă include, în special, aspecte legate de documentarea, abordarea și remedierea vulnerabilităților și promovează schimbul de informații privind vulnerabilitățile descoperite în cadrul comunității cu sursă deschisă.

(2) Administratorii de software cu sursă deschisă cooperează cu autoritățile de supraveghere a pieței, la cererea acestora, în vederea atenuării riscurilor în materie de securitate cibernetică prezentate de un produs cu elemente digitale care se consideră software liber și cu sursă deschisă.

În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, administratorii de software cu sursă deschisă furnizează autorității respective, într-o limbă ușor de înțeles de către autoritatea respectivă, documentația menționată la alineatul (1), pe suport de hârtie sau în format electronic.

(3) Obligațiile prevăzute la articolul 14 alineatul (1) se aplică administratorilor de software cu sursă deschisă, în măsura în care aceștia sunt implicați în dezvoltarea produselor cu elemente digitale. Obligațiile prevăzute la articolul 14 alineatele (3) și (8) se aplică administratorilor de software cu sursă deschisă în măsura în care incidentele grave care au un impact asupra securității produselor cu elemente digitale afectează rețelele și sistemele informatice furnizate de administratorii de software cu sursă deschisă pentru dezvoltarea unor astfel de produse.

Articolul 25

Atestare de securitate a software-ului liber și cu sursă deschisă

Pentru a facilita obligația de diligență prevăzută la articolul 13 alineatul (5), în special în ceea ce privește producătorii care integrează componente de software liber și cu sursă deschisă în produsele lor cu elemente digitale, Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a completa prezentul regulament prin instituirea unor programe voluntare de atestare a securității care să le permită dezvoltatorilor sau utilizatorilor de produse cu elemente digitale care sunt considerate software gratuit și cu sursă deschisă, precum și altor părți terțe să evalueze conformitatea acestor produse cu toate sau cu anumite cerințe esențiale de securitate cibernetică sau cu alte obligații prevăzute în prezentul regulament.

Articolul 26

Orientări

(1) Pentru a facilita punerea în aplicare și pentru a asigura coerența acestei puneri în aplicare, Comisia publică orientări pentru a ajuta operatorii economici în aplicarea prezentului regulament, acordând o atenție deosebită facilitării respectării sale de către microîntreprinderi și întreprinderile mici și mijlocii.

(2) În cazul în care intenționează să ofere orientări, astfel cum se menționează la alineatul (1), Comisia abordează cel puțin următoarele aspecte:

(a) domeniul 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) aplicarea perioadelor de asistență în legătură cu anumite categorii de produse cu elemente digitale;

(c) orientări destinate producătorilor cărora li se aplică prezentul regulament și cărora li se aplică, de asemenea, legislația de armonizare a Uniunii diferită de prezentul regulament, sau alte acte juridice conexe ale Uniunii;

(d) conceptul de modificare substanțială.

Comisia păstrează, de asemenea, o listă ușor de accesat a actelor delegate și a actelor de punere în aplicare adoptate în temeiul prezentului regulament.

(3) La elaborarea orientărilor în temeiul prezentului articol, Comisia consultă părțile interesate relevante.

Capitolul III

Conformitatea produsului cu elementele digitale

Articolul 27

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 de securitate cibernetică 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 de securitate cibernetică prevăzute în anexa I la prezentul regulament. Atunci când elaborează cererile de standardizare pentru prezentul regulament, Comisia depune eforturi pentru a ține seama de standardele europene și internaționale existente în materie de securitate cibernetică, care sunt în vigoare sau în curs de elaborare, pentru a simplifica elaborarea de standarde armonizate, în conformitate cu Regulamentul (UE) nr. 1025/2012.

(2) 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 de securitate cibernetică prevăzute în anexa I pentru produsele cu elemente digitale care intră în domeniul de aplicare al prezentului regulament.

Aceste acte de punere în aplicare se adoptă numai 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 de securitate cibernetică prevăzute în anexa I și:

(i) cererea nu a fost acceptată;

(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

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

Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

(3) Înainte de a pregăti proiectul de act de punere în aplicare menționat la alineatul (2) de la prezentul articol, Comisia informează comitetul menționat la articolul 22 din Regulamentul (UE) nr. 1025/2012 că, în opinia sa, condițiile de la alineatul (2) de la prezentul articol sunt îndeplinite.

(4) La elaborarea proiectului de act de punere în aplicare menționat la alineatul (2), Comisia ține seama de opiniile organismelor relevante și consultă în mod corespunzător toate părțile interesate relevante.

(5) Produsele cu elemente digitale și procesele instituite de producător care sunt conforme cu specificațiile comune stabilite prin acte de punere în aplicare menționate la alineatul (2) de la prezentul articol sau cu părți din acestea sunt considerate a fi conforme cu cerințele esențiale de securitate cibernetică prevăzute în anexa I acoperite de specificațiile comune respective sau de părți din acestea.

(6) 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 (2) de la prezentul articol sau acele părți ale lor care vizează aceleași cerințe esențiale de securitate cibernetică precum cele vizate de respectivul standard armonizat.

(7) În cazul în care un stat membru consideră că o specificație comună nu satisface în totalitate cerințele esențiale de securitate cibernetică prevăzute în anexa I, acesta informează Comisia, prezentând o explicație detaliată. Comisia analizează respectiva explicație detaliată și, dacă este cazul, poate modifica actul de punere în aplicare prin care se stabilește specificația comună în cauză.

(8) 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 sunt considerate a fi conforme cu cerințele esențiale de securitate cibernetică prevăzute în anexa I în măsura în care declarația de conformitate UE sau certificatul european de securitate cibernetică sau părți ale acestora acoperă cerințele respective.

(9) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 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 de securitate cibernetică sau cu anumite părți ale acestora, astfel cum sunt prevăzute în anexa I. În plus, emiterea unui certificat european de securitate cibernetică în cadrul unor astfel de sisteme, la un nivel de asigurare cel puțin „substanțial”, elimină obligația unui producător de a efectua o evaluare a conformității de către terți pentru cerințele corespunzătoare, astfel cum se prevede la articolul 32 alineatul (2) literele (a) și (b) și articolul 32 alineatul (3) literele (a) și (b) din prezentul regulament.

Articolul 28

Declarația de conformitate UE

(1) Declarația de conformitate UE este întocmită de producători în conformitate cu articolul 13 alineatul (12) și prevede faptul că îndeplinirea cerințelor esențiale de securitate cibernetică aplicabile prevăzute în anexa I a fost demonstrată.

(2) Declarația de conformitate UE trebuie să fie structurată după modelul prevăzut în anexa V și să conțină elementele specificate în procedurile relevante de evaluare a conformității stabilite în anexa VIII. O astfel de declarație trebuie să fie 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 pe piață.

Declarația de conformitate UE menționată la articolul 13 alineatul (20) trebuie să fie structurată după modelul prevăzut în anexa VI. 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 pe piață.

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

(4) Prin redactarea declarației de conformitate UE, producătorul își asumă responsabilitatea pentru conformitatea produsului cu elemente digitale.

(5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 61 pentru a completa prezentul regulament prin adăugarea de elemente la conținutul minim al declarației de conformitate UE prevăzute în anexa V, pentru a ține seama de evoluțiile tehnologice.

Articolul 29

Principii generale ale marcajului CE

Marcajul CE este supus principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.

Articolul 30

Norme și condiții pentru 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 28 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 28, fie pe site-ul web care însoțește produsul software. În această ultimă situație, secțiunea relevantă a site-ului web 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 de securitate cibernetică sau o utilizare specială prevăzută 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 32.

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 este supus legislației de armonizare a Uniunii, diferită de prezentul regulament, care prevede și aplicarea marcajului CE, marcajul indică faptul că produsul îndeplinește și cerințele prevăzute de respectiva legislație de armonizare a Uniunii.

(6) Comisia poate stabili, prin intermediul unor acte de punere în aplicare, specificații tehnice pentru etichete, pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale și perioadele lor de asistență tehnică, precum și mecanisme de promovare a utilizării acestora și pentru a îmbunătăți conștientizarea în rândul publicului cu privire la securitatea produselor cu elemente digitale. Atunci când pregătește proiectele de acte de punere în aplicare, Comisia consultă părțile interesate relevante și, dacă a fost deja instituit în temeiul articolului 52 alineatul (15), ADCO. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

Articolul 31

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 de securitate cibernetică prevăzute în anexa I. Aceasta conține cel puțin elementele prevăzute în anexa VII.

(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 asistență.

(3) Pentru produsele cu elemente digitale menționate la articolul 12, care fac, de asemenea, obiectul altor acte juridice ale Uniunii care prevăd documentația tehnică, se întocmește o singură documentație tehnică care conține informațiile menționate în anexa VII la prezentul regulament și informațiile prevăzute în respectivele acte juridice 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 61 pentru a completa prezentul regulament prin adăugarea elementelor care trebuie incluse în documentația tehnică prevăzută în anexa VII, pentru a ține seama de evoluțiile tehnologice, precum și de situațiile întâlnite în procesul de punere în aplicare a prezentului regulament. În acest scop, Comisia depune eforturi pentru a se asigura că sarcina administrativă pentru microîntreprinderi și întreprinderile mici și mijlocii are un caracter proporționat.

Articolul 32

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 de securitate cibernetică prevăzute în anexa I. Producătorul demonstrează conformitatea cu cerințele esențiale de securitate cibernetică utilizând oricare dintre procedurile următoare:

(a) procedura controlului intern (pe baza modulului A) prevăzută în anexa VIII;

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

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

(d) în cazul în care este disponibil și aplicabil, un sistem european de certificare de securitate cibernetică în temeiul articolului 27 alineatul (9).

(2) În cazul în care, la evaluarea conformității produsului important cu elemente digitale care se încadrează la clasa I prevăzută în anexa III și a proceselor instituite de producătorul său cu cerințele esențiale de securitate cibernetică prevăzute în anexa I, producătorul nu a aplicat sau a aplicat doar parțial standardele armonizate, specificațiile comune sau sistemele europene de certificare de securitate cibernetică cu nivelul de asigurare cel puțin „substanțial” menționate la articolul 27 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 de securitate cibernetică respective, oricăreia dintre procedurile următoare:

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

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

(3) În cazul în care produsul este un produs important cu elemente digitale care se încadrează la clasa II prevăzută în anexa III, producătorul demonstrează conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în anexa I utilizând oricare dintre procedurile următoare:

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

(b) evaluarea conformității bazată pe asigurarea totală a calității (pe baza modulului H) prevăzută în anexa VIII; sau

(c) în cazul în care este disponibil și aplicabil, un sistem european de certificare de securitate cibernetică în temeiul articolului 27 alineatul (9) din prezentul regulament la un nivel de asigurare cel puțin „substanțial” în conformitate cu Regulamentul (UE) 2019/881.

(4) Produsele critice cu elemente digitale enumerate în anexa IV demonstrează conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în anexa I utilizând una dintre procedurile următoare:

(a) un sistem european de certificare de securitate cibernetică în conformitate cu articolul 8 alineatul (1); sau

(b) în cazul în care condițiile prevăzute la articolul 8 alineatul (1) nu sunt îndeplinite, oricare dintre procedurile menționate la alineatul (3) din prezentul articol.

(5) Producătorii de produse cu elemente digitale care se califică drept software liber și cu sursă deschisă, care se încadrează în categoriile prevăzute în anexa III, sunt în măsură să demonstreze conformitatea cu cerințele esențiale de securitate cibernetică prevăzute în anexa I utilizând una dintre procedurile menționate la alineatul (1) din prezentul articol, cu condiția ca documentația tehnică menționată la articolul 31 să fie pusă la dispoziția publicului în momentul introducerii pe piață a produselor respective.

(6) Interesele și nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii, inclusiv ale întreprinderilor nou-înființate, sunt luate în considerare la stabilirea taxelor pentru procedurile de evaluare a conformității, iar taxele respective se reduc proporțional cu interesele și nevoile specifice ale acestora.

Articolul 33

Măsuri de asistență pentru microîntreprinderi
și întreprinderile mici și mijlocii, inclusiv pentru întreprinderile nou-înființate

(1) Statele membre întreprind, după caz, următoarele acțiuni, adaptate la nevoile microîntreprinderilor și ale întreprinderilor mici:

(a) organizează activități specifice de sensibilizare și formare cu privire la aplicarea prezentului regulament;

(b) instituie un canal specific de comunicare cu microîntreprinderile și întreprinderile mici și, după caz, cu autoritățile publice locale pentru a oferi consiliere și a răspunde la întrebări cu privire la punerea în aplicare a prezentului regulament;

(c) sprijină activitățile de testare și de evaluare a conformității, inclusiv, după caz, cu sprijinul Centrului european de competențe în materie de securitate cibernetică.

(2) Statele membre pot, după caz, să instituie spații de testare în materie de reglementare a rezilienței cibernetice. Astfel de spații de testare în materie de reglementare prevăd medii de testare controlate pentru produse inovatoare cu elemente digitale, pentru a facilita dezvoltarea, proiectarea, validarea și testarea acestora în scopul respectării prezentului regulament pentru o perioadă limitată de timp înainte de introducerea pe piață. Comisia și, după caz, ENISA pot oferi sprijin tehnic, consiliere și instrumente pentru instituirea și operarea spațiilor de testare în materie de reglementare. Spațiile de testare în materie de reglementare sunt instituite sub supravegherea, îndrumarea și sprijinul directe ale autorităților de supraveghere a pieței. Statele membre informează Comisia și celelalte autorități de supraveghere a pieței cu privire la instituirea unui spațiu de testare în materie de reglementare prin intermediul ADCO. Spațiile de testare în materie de reglementare nu afectează competențele de supraveghere și atribuțiile corective ale autorităților competente. Statele membre asigură accesul deschis, echitabil și transparent la spațiile de testare în materie de reglementare și, în special, facilitează accesul microîntreprinderilor și al întreprinderilor mici, inclusiv al întreprinderilor nou-înființate.

(3) În conformitate cu articolul 26, Comisia oferă orientări microîntreprinderilor și întreprinderilor mici și mijlocii în ceea ce privește punerea în aplicare a prezentului regulament.

(4) Comisia promovează public sprijinul financiar disponibil în cadrul de reglementare al programelor existente ale Uniunii, în special pentru a ușura sarcina financiară asupra microîntreprinderilor și a întreprinderilor mici și mijlocii.

(5) Microîntreprinderile și întreprinderile mici pot furniza toate elementele documentației tehnice specificate în anexa VII utilizând un format simplificat. În acest scop, Comisia specifică, prin intermediul unor acte de punere în aplicare, formularul simplificat de documentație tehnică destinat nevoilor microîntreprinderilor și ale întreprinderilor mici, inclusiv modul în care trebuie furnizate elementele prevăzute în anexa VII. În cazul în care o microîntreprindere sau o întreprindere mică optează să furnizeze informațiile prevăzute în anexa VII într-un mod simplificat, aceasta utilizează formularul menționat la prezentul alineat. Organismele notificate acceptă formularul respectiv în scopul evaluării conformității.

Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

Articolul 34

Acorduri de recunoaștere reciprocă

Ținând seama de nivelul de dezvoltare tehnică și de abordarea privind evaluarea conformității unei țări terțe, Uniunea poate încheia acorduri de recunoaștere reciprocă cu țări terțe, în conformitate cu articolul 218 din TFUE, pentru a promova și a facilita comerțul internațional.

Capitolul IV

Notificarea organismelor de evaluare a conformității

Articolul 35

Notificarea

(1) Statele membre notifică Comisiei și celorlalte state membre organismele autorizate să efectueze evaluări ale conformității în conformitate cu prezentul regulament.

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

Articolul 36

Autoritățile de notificare

(1) Fiecare stat membru desemnează o autoritate de notificare care este responsabilă cu instituirea și efectuarea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora, inclusiv în ceea ce privește respectarea articolului 41.

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

(3) În cazul în care autoritatea de notificare deleagă sau încredințează în alt mod evaluarea, notificarea sau monitorizarea menționate la alineatul (1) din prezentul articol unui organism care nu reprezintă o entitate guvernamentală, respectivul organism este o entitate juridică și îndeplinește *mutatis mutandis* cerințele prevăzute la articolul 37. În plus, acesta dispune de modalități de compensare a răspunderilor care decurg din activitățile sale.

(4) Autoritatea de notificare își asumă întreaga răspundere pentru sarcinile îndeplinite de organismul menționat la alineatul (3).

Articolul 37

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.

Articolul 38

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.

(2) Comisia pune la dispoziția publicului informațiile menționate la alineatul (1).

Articolul 39

Cerințe referitoare la organismele 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 cu elemente digitale 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 terț, 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, importator, distribuitor, 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, importul, distribuirea, comercializarea, instalarea, utilizarea sau întreținerea produselor cu elemente digitale pe care le evaluează, 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 de natură financiară, 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 VIII 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) personal având cunoștințe tehnice și experiență suficientă și adecvată pentru a îndeplini sarcinile de evaluare a conformității;

(b) descrierile procedurilor în conformitate cu care urmează să se realizeze 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 de securitate cibernetică stabilite în anexa I, a standardelor armonizate și a specificațiilor comune 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.

(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 în cazul în care răspunderea nu este asumată de statul membru respectiv în conformitate cu dreptul intern sau în cazul în care statul membru 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 VIII sau al oricărei dispoziții de punere în aplicare a acesteia din dreptul intern, excepție făcând relația cu autoritățile de supraveghere a pieței ale statului membru în care își desfășoară activitățile. Drepturile de autor sunt protejate. 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 51 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, proporționale și rezonabile, evitând în același timp sarcinile inutile pentru operatorii economici, ținând seama în mod special de interesele microîntreprinderilor și ale întreprinderilor mici și mijlocii în ceea ce privește taxele.

Articolul 40

Prezumția de conformitate a organismelor notificate

În cazul în care un organism de evaluare a conformității poate demonstra conformitatea sa cu criteriile prevăzute în standardele armonizate relevante sau în părți din acestea, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, se consideră că acesta este în conformitate cu prevederile articolului 39 în măsura în care standardele armonizate aplicabile reglementează aceste cerințe.

Articolul 41

Filialele organismelor notificate și subcontractarea de către organismele notificate

(1) În cazul în care un organism notificat subcontractează anumite sarcini legate de evaluarea conformității sau recurge la o filială, acesta se asigură că subcontractantul sau filiala îndeplinește cerințele prevăzute la articolul 39 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 stabilite.

(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 aceasta în temeiul prezentului regulament.

Articolul 42

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 cu elemente digitale pentru care organismul se consideră a fi competent, precum și, dacă este cazul, 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 39.

(3) În cazul în care un organism de evaluare a conformității nu poate prezenta un certificat de acreditare, acesta prezintă autorității de notificare toate documentele justificative necesare pentru verificarea, recunoașterea și monitorizarea periodică a conformității acestuia cu cerințele de la articolul 39.

Articolul 43

Procedura de notificare

(1) Autoritățile de notificare notifică numai organismele de evaluare a conformității care au satisfăcut cerințele prevăzute la articolul 39.

(2) Autoritatea de notificare notifică Comisia și celelalte state membre utilizând sistemul informațional 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 cu elemente digitale în cauză, precum și atestarea relevantă a competenței.

(4) În cazul în care notificarea nu se bazează pe certificatul de acreditare menționat la articolul 42 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 39.

(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 a fi un organism notificat în sensul prezentului regulament.

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

Articolul 44

Numerele de identificare și lista organismelor 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 juridice 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 45

Modificări ale notificărilor

(1) Dacă o autoritate de notificare a constatat sau a fost informată că un organism notificat nu mai respectă cerințele prevăzute la articolul 39 sau că acesta nu își îndeplinește obligațiile, autoritatea de notificare restricționează, suspendă sau retrage notificarea, după caz, în funcție de gravitatea nerespectării cerințelor sau de gravitatea neîndeplinirii obligațiilor respective. 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 46

Contestarea competenței organismelor notificate

(1) Comisia investighează toate cazurile în care are îndoieli sau în care 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 47

Obligațiile operaționale ale organismelor notificate

(1) Organismele notificate efectuează evaluări ale conformității în conformitate cu procedurile de evaluare a conformității prevăzute la articolul 32 și în anexa VIII.

(2) Evaluările conformității sunt 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, în special în ceea ce privește microîntreprinderile și întreprinderile mici și mijlocii, de domeniul de activitate și structura acestora, de gradul lor de complexitate și de nivelul de risc în materie de securitate cibernetică al produselor cu elemente digitale și al tehnologiei în cauză, 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 produselor cu elemente digitale cu prezentul regulament.

(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 27 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 cu elemente digitale 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 48

Căi de atac împotriva deciziilor organismelor notificate

Statele membre se asigură că este disponibilă o cale de atac împotriva deciziilor organismelor notificate.

Articolul 49

Obligația de informare care revine 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 cu elemente digitale informații relevante privind aspecte legate de rezultatele negative și, la cerere, de rezultatele pozitive ale evaluării conformității.

Articolul 50

Schimbul de experiență

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

Articolul 51

Coordonarea organismelor notificate

(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.

(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 52

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) Autoritățile de supraveghere a pieței desemnate în temeiul alineatului (2) de la prezentul articol sunt, de asemenea, responsabile de desfășurarea activităților de supraveghere a pieței în legătură cu obligațiile administratorilor de software cu sursă deschisă prevăzute la articolul 24. În cazul în care o autoritate de supraveghere a pieței constată că un administrator de software cu sursă deschisă nu respectă obligațiile prevăzute la articolul respectiv, aceasta solicită administratorului de software cu sursă deschisă să se asigure că sunt luate toate măsurile corective adecvate. Administratorii de software cu sursă deschisă se asigură că sunt luate toate măsurile corective adecvate în ceea ce privește obligațiile care le revin în temeiul prezentului regulament.

(4) Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu autoritățile naționale de certificare a securității cibernetice desemnate în conformitate cu articolul 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 14 din prezentul regulament, autoritățile de supraveghere a pieței desemnate cooperează și fac schimb de informații în mod regulat cu CSIRT desemnate drept coordonatori și cu ENISA.

(5) Autoritățile de supraveghere a pieței pot solicita unei CSIRT desemnate drept coordonator sau 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 54, autoritățile de supraveghere a pieței pot solicita CSIRT desemnate drept coordonator sau ENISA să furnizeze o analiză în sprijinul evaluărilor conformității produselor cu elemente digitale.

(6) 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 decât prezentul regulament și fac schimb de informații în mod regulat.

(7) 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 (10), 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.

(8) Statele membre se asigură că autorităților de supraveghere a pieței desemnate li se pun la dispoziție resurse financiare și tehnice adecvate, inclusiv, după caz, instrumente de automatizare a prelucrării, precum și resurse umane cu competențele necesare în materie de securitate cibernetică pentru a-și îndeplini sarcinile care le revin în temeiul prezentului regulament.

(9) Comisia încurajează și facilitează schimbul de experiență între autoritățile de supraveghere a pieței desemnate.

(10) Autoritățile de supraveghere a pieței pot oferi orientări și recomandări operatorilor economici cu privire la punerea în aplicare a prezentului regulament, cu sprijinul Comisiei și, după caz, al CSIRT și al ENISA.

(11) Autoritățile de supraveghere a pieței informează consumatorii cu privire la locul în care pot depune plângeri care ar putea indica nerespectarea prezentului regulament, în conformitate cu articolul 11 din Regulamentul (UE) 2019/1020, și le furnizează consumatorilor informații cu privire la locul și modul de accesare a mecanismelor de facilitare a raportării vulnerabilităților, incidentelor și amenințărilor cibernetice care pot afecta produsele cu elemente digitale.

(12) Autoritățile de supraveghere a pieței facilitează, după caz, cooperarea cu părțile interesate relevante, inclusiv cu organizațiile științifice, de cercetare și de consumatori.

(13) 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.

(14) 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 6 din Regulamentul (UE) 2024/1689, autoritățile de supraveghere a pieței desemnate în sensul regulamentului menționat sunt autoritățile responsabile cu activitățile de supraveghere a pieței necesare în temeiul prezentului regulament. Autoritățile de supraveghere a pieței desemnate în temeiul Regulamentului (UE) 2024/1689 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 14 din prezentul regulament, cu CSIRT desemnate drept coordonatori și cu ENISA. Autoritățile de supraveghere a pieței desemnate în temeiul Regulamentului (UE) 2024/1689 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.

(15) Se instituie ADCO pentru aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. 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. ADCO abordează, de asemenea, aspecte specifice legate de activitățile de supraveghere a pieței în ceea ce privește obligațiile impuse administratorilor de software cu sursă deschisă.

(16) Autoritățile de supraveghere a pieței monitorizează modul în care producătorii au aplicat criteriile menționate la articolul 13 alineatul (8) atunci când stabilesc perioada de asistență pentru produsele lor cu elemente digitale.

ADCO publică într-o formă accesibilă publicului și ușor de utilizat statistici relevante privind categoriile de produse cu elemente digitale, inclusiv perioadele medii de asistență astfel cum sunt stabilite de producător în temeiul articolului 13 alineatul (8), și oferă orientări care includ perioade orientative de asistență pentru categoriile de produse cu elemente digitale.

În cazul în care datele sugerează perioade de asistență inadecvate pentru categorii specifice de produse cu elemente digitale, ADCO poate adresa recomandări autorităților de supraveghere a pieței pentru ca acestea să își concentreze activitățile asupra unor astfel de categorii de produse cu elemente digitale.

Articolul 53

Accesul la date și la documentație

Dacă este necesar pentru a evalua conformitatea produselor cu elemente digitale și a proceselor instituite de producătorii lor cu cerințele esențiale de securitate cibernetică prevăzute în anexa I și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă acces la datele, prezentate într-o limbă care le este ușor accesibilă, necesare pentru a evalua proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților acestor produse, inclusiv la documentația internă aferentă a operatorului economic relevant.

Articolul 54

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

(1) Dacă 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.

Dacă, 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 cu elemente digitale în conformitate cu cerințele, pentru a retrage produsul de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului de securitate cibernetică și stabilit de autoritatea de supraveghere a pieței.

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

(2) Atunci când evaluează importanța unui risc de securitate cibernetică vizat la alineatul (1) de la prezentul articol, autoritățile de supraveghere a pieței iau în considerare și factorii de risc fără caracter tehnic, în special cei stabiliți după evaluările coordonate la nivelul Uniunii ale riscurilor în materie de securitate ale lanțurilor de aprovizionare critice, efectuate în conformitate cu articolul 22 din Directiva (UE) 2022/2555. Dacă o autoritate de supraveghere a pieței are motive suficiente să considere că un produs cu elemente digitale prezintă un risc important în materie de securitate cibernetică având în vedere factori de risc fără caracter tehnic, aceasta informează autoritățile competente desemnate sau instituite în temeiul articolului 8 din Directiva (UE) 2022/2555 și cooperează cu autoritățile respective în funcție de necesități.

(3) Dacă 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 economic.

(4) Operatorul economic 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.

(5) În cazul în care operatorul economic 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 cu elemente digitale pe piața sa națională, pentru a-l retrage de pe piață sau pentru a-l rechema.

Autoritatea respectivă înștiințează Comisia și celelalte state membre, fără întârziere, cu privire la măsurile respective.

(6) Informațiile menționate la alineatul (5) trebuie să cuprindă toate detaliile disponibile, în special datele necesare pentru identificarea produsului 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 economic 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 cu elemente digitale sau de către procesele instituite de producător a cerințelor esențiale de securitate cibernetică prevăzute în anexa I;

(b) deficiențe ale standardelor armonizate, ale sistemelor europene de certificare de securitate cibernetică sau ale specificațiilor comune astfel cum sunt menționate la articolul 27.

(7) 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 cu elemente digitale în cauză și, în cazul în care nu sunt de acord cu privire la măsura națională notificată, cu privire la obiecțiile lor.

(8) În cazul în care, în termen de trei luni de la primirea înștiințării menționate la alineatul (5) de la prezentul articol, 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 a fi justificată. Acest lucru nu aduce atingere drepturilor procedurale care îi revin operatorului economic în cauză în conformitate cu articolul 18 din Regulamentul (UE) 2019/1020.

(9) 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 cu elemente digitale de pe piețele lor.

Articolul 55

Procedura de salvgardare a Uniunii

(1) Dacă în termen de trei luni de la primirea notificării menționate la articolul 54 alineatul (5) 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 dreptului 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 54 alineatul (5) și notifică respectiva decizie statului membru în cauză.

(2) Dacă 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. Dacă măsura națională este considerată ca fiind nejustificată, statul membru în cauză retrage măsura.

(3) Dacă măsura națională este considerată a fi justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale standardelor armonizate, Comisia aplică procedura prevăzută la articolul 11 din Regulamentul (UE) nr. 1025/2012.

(4) Dacă măsura națională este considerată a fi justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale unui sistem european de certificare de securitate cibernetică menționat la articolul 27, Comisia analizează dacă este oportun să modifice sau să abroge orice act delegat adoptat în temeiul articolului 27 alineatul (9) care precizează prezumția de conformitate în ceea ce privește sistemul de certificare respectiv.

(5) Dacă măsura națională este considerată a fi justificată, iar neconformitatea produsului cu elemente digitale este atribuită unor deficiențe ale specificațiilor comune menționate la articolul 27, Comisia analizează dacă este oportun să modifice sau să abroge actul de punere în aplicare adoptat conform articolului 27 alineatul (2) care stabilește specificațiile comune respective.

Articolul 56

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

(1) Dacă 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 informează autoritățile relevante de supraveghere a pieței. Dacă autoritățile de supraveghere a pieței efectuează o evaluare a produsului respectiv cu elemente digitale care poate prezenta un risc semnificativ în materie de securitate cibernetică în ceea ce privește conformitatea acestuia cu cerințele prevăzute în prezentul regulament, se aplică procedurile menționate la articolele 54 și 55.

(2) În cazul în care Comisia are motive suficiente să considere că un produs cu elemente digitale prezintă un risc important în materie de securitate cibernetică având în vedere factori de risc fără caracter tehnic, aceasta informează autoritățile de supraveghere a pieței competente și, după caz, autoritățile competente desemnate sau instituite în temeiul articolului 8 din Directiva (UE) 2022/2555 și cooperează cu autoritățile respective în funcție de necesități. Comisia analizează totodată relevanța riscurilor identificate pentru respectivul produs cu elemente digitale, având în vedere sarcinile sale în evaluările coordonate la nivelul Uniunii ale riscurilor de securitate ale lanțurilor de aprovizionare critice, prevăzute la articolul 22 din Directiva (UE) 2022/2555, și consultă, după caz, grupul de cooperare instituit în temeiul articolului 14 din Directiva (UE) 2022/2555 și ENISA.

(3) 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 cu elemente digitale 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 efectuează o evaluare a conformității și poate solicita ENISA să efectueze o analiză în sprijinul acesteia. Comisia informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.

(4) Pe baza evaluării menționate la alineatul (3), Comisia poate stabili că este necesară o acțiune corectivă sau restrictivă la nivelul Uniunii. În acest scop, Comisia consultă fără întârziere statele membre în cauză și operatorul sau operatorii economici relevanți.

(5) Pe baza consultării menționate la alineatul (4) de la prezentul articol, Comisia poate adopta acte de punere în aplicare pentru a asigura măsuri corective sau restrictive la nivelul Uniunii, inclusiv de retragere de pe piață sau rechemare a respectivelor produse cu elemente digitale, într-un termen rezonabil, proporțional cu natura riscului. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

(6) Comisia comunică imediat actele de punere în aplicare menționate la alineatul (5) operatorului sau operatorilor economici relevanți. Statele membre pun în aplicare fără întârziere aceste acte de punere în aplicare și informează Comisia în consecință.

(7) Alineatele (3)-(6) se aplică pe durata situației excepționale care a justificat intervenția Comisiei cu condiția ca respectivul produs cu elemente digitale să nu fie adus în conformitate cu prezentul regulament.

Articolul 57

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

(1) Autoritatea de supraveghere a pieței dintr-un stat membru solicită unui operator economic să ia toate măsurile adecvate în cazul în care, după efectuarea unei evaluări în temeiul articolului 54, constată că, deși un produs cu elemente digitale și procesele instituite de producător sunt în conformitate cu prezentul regulament, acestea prezintă un risc semnificativ în materie de securitate cibernetică, precum și un risc pentru:

(a) sănătatea sau siguranța persoanelor;

(b) respectarea obligațiilor de protecție a drepturilor fundamentale care decurg din dreptul Uniunii sau din dreptul intern;

(c) disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin intermediul unui sistem electronic de informații de către entitățile esențiale menționate la articolul 3 alineatul (1) din Directiva (UE) 2022/2555; sau

(d) alte aspecte ce țin de protecția interesului public.

Măsurile prevăzute la primul paragraf pot include măsuri prin care să se asigure că respectivul produs cu elemente digitale și procesele instituite de producător nu mai prezintă riscurile respective atunci când este pus la dispoziție pe piață, măsuri care să prevadă retragerea de pe piață a produsului cu elemente digitale în cauză sau rechemarea acestuia și sunt proporționale cu natura riscurilor respective.

(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 menționată la alineatul (4) 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) de la prezentul articol, Comisia informează și poate solicita autorității sau autorităților relevante de supraveghere a pieței să efectueze o evaluare și să urmeze procedurile menționate la articolul 54 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 cu elemente digitale 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 efectuează o evaluare a riscurilor prezentate de produsul cu elemente digitale și poate solicita ENISA să realizeze o analiză în sprijinul respectivei evaluări și informează autoritățile relevante de supraveghere a pieței în consecință. Operatorii economici relevanți cooperează cu ENISA în funcție de necesități.

(8) Pe baza evaluării menționate la alineatul (7), Comisia poate stabili că este necesară o acțiune corectivă sau restrictivă la nivelul Uniunii. În acest scop, Comisia consultă fără întârziere statele membre în cauză și operatorul sau operatorii economici relevanți.

(9) Pe baza consultării menționate la alineatul (8) de la prezentul articol, Comisia poate adopta acte de punere în aplicare pentru a decide cu privire la măsuri corective sau restrictive la nivelul Uniunii, inclusiv de retragere de pe piață sau rechemare a respectivelor produse cu elemente digitale, într-un termen rezonabil, proporțional cu natura riscului. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 62 alineatul (2).

(10) Comisia comunică imediat actele de punere în aplicare menționate la alineatul (9) operatorului sau operatorilor economici relevanți. Statele membre pun în aplicare fără întârziere aceste acte de punere în aplicare și informează Comisia în consecință.

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

Articolul 58

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 CE a fost aplicat cu încălcarea articolelor 29 și 30;

(b) marcajul CE 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, după caz, nu a fost aplicat;

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

(2) Dacă 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 59

Activități comune ale autorităților de supraveghere a pieței

(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 pe piață sau puse la dispoziție pe piață, în special produsele cu elemente digitale 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 cu elemente digitale care intră în domeniul de aplicare al prezentului regulament cu cerințele prevăzute în acesta.

(3) Autoritățile de supraveghere a pieței și, după caz, Comisia, 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 obținută ca rezultat al activităților comune desfășurate în cadrul oricărei investigații pe care o efectuează.

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

Articolul 60

Acțiuni de verificare

(1) Autoritățile de supraveghere a pieței decid să desfășoare acțiuni de control coordonate simultane (denumite în continuare „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 de verificare includ inspecții ale produselor cu elemente digitale achiziționate sub o identitate falsă.

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

(3) În cazul în care, în îndeplinirea sarcinilor sale, inclusiv pe baza notificărilor primite în conformitate cu articolul 14 alineatele (1) și (3), ENISA identifică categorii de produse cu elemente digitale pentru care pot fi organizate acțiuni de verificare, aceasta prezintă o propunere de acțiuni de verificare coordonatorului menționat la alineatul (2) de la prezentul articol, 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 52-58 și orice alte competențe care le sunt conferite de dreptul intern.

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

Capitolul VI
Competențele delegate și procedura comitetului

Articolul 61

Exercitarea delegării de competențe

(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 (5) al doilea paragraf, la articolul 7 alineatul (3), la articolul 8 alineatele (1) și (2), la articolul 13 alineatul (8) al patrulea paragraf, la articolul 14 alineatul (9), la articolul 25, la articolul 27 alineatul (9), la articolul 28 alineatul (5) și la articolul 31 alineatul (5) pe o perioadă de cinci ani de la ... [data intrării în vigoare a prezentului regulament]. Comisia prezintă un raport privind delegarea de competențe cel târziu cu nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.

(3) Delegarea de competențe menționată la articolul 2 alineatul (5) al doilea paragraf, la articolul 7 alineatul (3), la articolul 8 alineatele (1) și (2), la articolul 13 alineatul (8) al patrulea paragraf, la articolul 14 alineatul (9), la articolul 25, la articolul 27 alineatul (9), la articolul 28 alineatul (5) și la articolul 31 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 care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

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

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

(6) Un act delegat adoptat în temeiul articolului 2 alineatul (5) al doilea paragraf, al articolului 7 alineatul (3), al articolului 8 alineatul (1) sau (2), al articolului 13 alineatul (8) al patrulea paragraf, al articolului 14 alineatul (9), al articolului 25, al articolului 27 alineatul (9), al articolului 28 alineatul (5) sau al articolului 31 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 62

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 63

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 (UE) 2016/943 a Parlamentului European și a Consiliului[37];

(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.

[37] 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).

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

Articolul 64

Sancțiuni

(1) Statele membre adoptă normele privind sancțiunile care se aplică în cazul nerespectării prezentului regulament și iau toate măsurile necesare pentru a asigura aplicarea acestora. Sancțiunile trebuie să fie efective, proporționale și cu efect de descurajare. Statele membre notifică normele și măsurile respective Comisiei fără întârziere și îi comunică acesteia, de asemenea fără întârziere, orice modificare ulterioară a acestora.

(2) Nerespectarea cerințelor esențiale de securitate cibernetică prevăzute în anexa I și a obligațiilor prevăzute la articolele 13 și 14 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.

(3) Nerespectarea obligațiilor prevăzute la articolele 18-23, la articolul 28, la articolul 30 alineatele (1)-(4), la articolul 31 alineatele (1)-(4), la articolul 32 alineatele (1), (2) și (3), la articolul 33 alineatul (5) și la articolele 39, 41, 47, 49 și 53 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.

(4) 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.

(5) 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;

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

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

(6) Autoritățile de supraveghere a pieței care aplică amenzi administrative comunică aceste decizii 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.

(7) 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.

(8) 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.

(9) 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.

(10) Prin derogare de la alineatele (3)-(9), amenzile administrative menționate la alineatele respective nu se aplică:

(a) producătorilor care se califică drept microîntreprinderi sau întreprinderi mici, pentru nerespectarea termenului menționat la articolul 14 alineatul (2) litera (a) sau la articolul 14 alineatul (4) litera (a);

(b) încălcărilor prezentului regulament de către administratorii sistemelor de software cu sursă deschisă.

Articolul 65

Acțiuni în reprezentare

Directiva (UE) 2020/1828 se aplică acțiunilor în reprezentare introduse împotriva încălcărilor dispozițiilor prezentului regulament de către operatorii economici care prejudiciază sau pot prejudicia interesele colective ale consumatorilor.

Capitolul VIII

Dispoziții tranzitorii și finale

Articolul 66

Modificarea Regulamentului (UE) 2019/1020

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

„XX[+]. Regulamentul (UE) 2024/… al Parlamentului European și al Consiliului[*++].

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, ..., ELI: ...).”.

[+] JO: a se introduce în text următorul număr consecutiv pe lista din anexa I la Regulamentul (UE) 2019/1020.

[++] JO: a se introduce în text numărul regulamentului cuprins în documentul PE-CONS 100/23 [2022/0272(COD)] și a se introduce în nota de subsol numărul, data și referința de publicare ale regulamentului respectiv.

Articolul 67

Modificarea Directivei (UE) 2020/1828

În anexa I la Directiva (UE) 2020/1828 se adaugă următorul punct:

„XX[+]. Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului[*++].

---

[*] Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) (JO L, ..., ELI: ...).”.

[+] JO: a se introduce în text următorul număr consecutiv pe lista din anexa I la Directiva (UE) 2020/1828.

[++] JO: a se introduce în text numărul regulamentului cuprins în documentul PE-CONS 100/23 (2022/0272(COD)) și a se introduce în nota de subsol numărul, data și referința de publicare ale regulamentului respectiv.

Articolul 68

Modificarea Regulamentului (UE) nr. 168/2013

În tabelul din partea C1 din anexa II la Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului[38] se adaugă următoarea rubrică:

„

XX+	18	protecția vehiculului împotriva atacurilor cibernetice		x	x	x	x	x	x	x	x	x	x	x	x	x	x

”.

[38] Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului din 15 ianuarie 2013 privind omologarea și supravegherea pieței pentru vehiculele cu două sau trei roți și pentru cvadricicluri (JO L 60, 2.3.2013, p. 52).

+ JO: a se introduce în text următorul număr consecutiv în partea C1 din anexa II la Regulamentul (UE) nr. 168/2013.

Articolul 69

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 legislației de armonizare a Uniunii diferită de prezentul regulament, 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 respectiva legislație de armonizare a Uniunii, caz în care rămân valabile, astfel cum se menționează în legislația respectivă.

(2) Produsele cu elemente digitale care au fost introduse pe piață înainte de ... [36 de luni de la data intrării în vigoare a prezentului regulament] fac obiectul cerințelor prevăzute în prezentul regulament numai dacă, de la acea dată, produsele respective fac obiectul unei modificări substanțiale.

(3) Prin derogare de la alineatul (2) de la prezentul articol, obligațiile prevăzute la articolul 14 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 ... [36 de luni de la data intrării în vigoare a prezentului regulament].

Articolul 70

Evaluare și reexaminare

(1) Până la … [72 de luni de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Rapoartele respective se publică.

(2) Până la ... [45 de luni de la data intrării în vigoare a prezentului regulament], Comisia, după consultarea ENISA și a rețelei CSIRT, prezintă Parlamentului European și Consiliului un raport de evaluare a eficacității platformei unice de raportare prevăzute la articolul 16 și de evaluare a impactului aplicării de către rețea a motivelor ce țin de securitatea cibernetică menționate la articolul 16 alineatul (2), drept coordonatori pentru eficacitatea platformei unice de raportare în diseminarea în timp util către alte CSIRT relevante a notificărilor primite.

Articolul 71

Intrarea în vigoare și aplicarea

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

(2) Prezentul regulament se aplică de la ...[36 de luni de la data intrării în vigoare a prezentului regulament].

Cu toate acestea, articolul 14 se aplică de la ... [21 de luni de la data intrării în vigoare a prezentului regulament], iar capitolul IV (articolele 35-51) 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 Strasbourg,

Pentru Parlamentul European	*Pentru Consiliu*
Președinta	*Președintele*

ANEXA I

CERINȚE ESENȚIALE DE SECURITATE CIBERNETICĂ

Partea I Cerințe de securitate cibernetică 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.

2. Pe baza evaluării riscurilor în materie de securitate cibernetică menționate la articolul 13 alineatul (2) și după caz, produsele cu elemente digitale trebuie:

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

   (b) să fie puse la dispoziție pe piață cu o configurație securizată implicită, cu excepția cazului în care se convine altfel între producător și furnizorul prin servicii de intermediere online în legătură cu un produs personalizat cu elemente digitale, inclusiv cu posibilitatea de a reseta produsul la starea sa inițială;

   (c) să se asigure că vulnerabilitățile pot fi abordate prin actualizări de securitate, inclusiv, după caz, prin actualizări automate de securitate care sunt instalate într-un interval de timp adecvat, activate ca setare implicită, cu un mecanism de neparticipare clar și ușor de utilizat, prin notificarea utilizatorilor cu privire la actualizările disponibile și prin opțiunea de a le amâna temporar;

(d) 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, și să raporteze privind posibilul acces neautorizat;

(e) 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;

(f) 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;

(g) 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 scopul preconizat al produsului cu elemente digitale (reducerea la minimum a datelor);

(h) să protejeze disponibilitatea funcțiilor esențiale și de bază, iar după un incident, inclusiv prin reziliență și măsuri de atenuare împotriva atacurilor vizând blocarea accesului la servicii;

(i) să reducă la minimum impactul negativ al produselor în sine sau al dispozitivelor conectate asupra disponibilității serviciilor furnizate de alte dispozitive sau rețele;

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

(k) 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;

(l) să furnizeze informații legate de securitate prin înregistrarea și monitorizarea activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora, cu un mecanism de neparticipare pentru utilizator;

(m) să ofere utilizatorilor posibilitatea de a elimina în mod securizat și cu ușurință, în mod permanent, toate datele și setările și, în cazul în care astfel de date pot fi transferate către alte produse sau sisteme, și să se asigure că acest lucru se realizează în mod securizat.

Partea II Cerințe privind gestionarea vulnerabilităților

Producătorii de produse cu elemente digitale trebuie:

1. să identifice și să documenteze vulnerabilitățile și componentele produselor cu elemente digitale, 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; în cazul în care acest lucru este fezabil din punct de vedere tehnic, noile actualizări de securitate sunt furnizate separat de actualizările de funcționalitate;

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, 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; în cazuri justificate în mod corespunzător, atunci când producătorii consideră că riscurile de securitate ale publicării depășesc beneficiile în materie de securitate, aceștia pot amâna publicarea informațiilor cu privire la o vulnerabilitate fixă până după ce utilizatorilor li s-a oferit posibilitatea de a aplica corecția relevantă;

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 pentru produsele cu elemente digitale, pentru a se asigura că vulnerabilitățile sunt remediate sau atenuate în timp util și, dacă este cazul pentru actualizările de securitate, în mod automat;

8. să se asigure că, în cazul în care sunt disponibile actualizări de securitate pentru abordarea problemelor de securitate identificate, acestea sunt difuzate fără întârziere și, cu excepția cazului în care producătorul și furnizorul prin servicii de intermediere online au convenit altfel în legătură cu un produs personalizat cu elemente digitale, gratuit, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse.

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 sau alt contact digital, precum și, dacă este cazul, site-ul web la care poate fi contactat producătorul;

2. ghișeul unic unde pot fi raportate și primite informații cu privire la vulnerabilitățile produsului cu elemente digitale, precum și locul în care poate fi găsită politica producătorului privind divulgarea coordonată a vulnerabilităților;

3. denumirea și tipul și orice informații suplimentare care permit identificarea unică a produsului cu elemente digitale;

4. scopul preconizat al produsului cu elemente digitale, 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 este cazul, adresa de internet la care poate fi accesată declarația de conformitate UE;

7. tipul de asistență tehnică de securitate oferită de producător și data de încheiere a perioadei de asistență în care utilizatorii se pot aștepta să fie gestionate vulnerabilitățile și să primească actualizări de securitate;

8. 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 cu elemente digitale pentru a se asigura o utilizare securizată a acestuia;

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

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

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

   (e) modul în care poate fi dezactivată setarea implicită care permite instalarea automată a actualizărilor de securitate, astfel cum se prevede în partea I punctul 2 litera (c) din anexa I;

   (f) în cazul în care produsul cu elemente digitale este destinat integrării în alte produse cu elemente digitale, informațiile necesare integratorului pentru a se conforma cerințelor esențiale de securitate cibernetică prevăzute în anexa I și cerințelor privind documentația prevăzute în anexa VII.

9. În cazul în care producătorul decide să pună la dispoziția utilizatorului lista materialelor software, informații cu privire la locul în care poate fi accesată lista materialelor software.

ANEXA III

PRODUSELE IMPORTANTE CU ELEMENTE DIGITALE

Clasa I

1. Software și hardware pentru sisteme de gestionare a identității și de gestionare a accesului privilegiat, inclusiv cititoare de autentificare și de control al accesului, inclusiv cititoare biometrice

2. Browsere autonome și încorporate

3. Manageri de parole

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. Sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)

8. Manageri de boot

9. Infrastructuri publice esențiale și software pentru emiterea de certificate digitale

10. Interfețe fizice și virtuale de rețea

11. Sisteme de operare

12. Routere, modemuri destinate conectării la internet și comutatoare

13. Microprocesoare cu funcționalități legate de securitate

14. Microcontrolere cu funcționalități legate de securitate

15. Circuite integrate specifice aplicațiilor (ASIC) și rețele de porți programabile de utilizator (FPGA) cu funcționalități legate de securitate

16. Asistenți virtuali de uz general pentru locuințe inteligente

17. Produse pentru locuințe inteligente cu funcționalități legate de securitate, inclusiv încuietori inteligente ale ușilor, camere de securitate, sisteme de monitorizare a bebelușilor și sisteme de alarmă

18. Jucării conectate la internet care intră sub incidența Directivei 2009/48/CE a Parlamentului European și a Consiliului[1], care au caracteristici sociale interactive (de exemplu, vorbire sau filmare) sau care au funcții de localizare

19. Produse portabile personale care urmează să fie purtate sau plasate pe un corp uman care au un scop de monitorizare a stării de sănătate (cum ar fi urmărirea) și cărora nu li se aplică Regulamentul (UE) 2017/745 sau (UE) 2017/746, sau produse portabile personale care sunt destinate utilizării de către și pentru copii

Clasa II

1. Hipervizoare și sisteme de runtime a containerelor care sprijină executarea virtualizată a sistemelor de operare și a mediilor similare

2. Firewall-uri, sisteme de detectare și prevenire a intruziunilor

3. Microprocesoare rezistente la manipulare frauduloasă

4. Microcontrolere rezistente la manipulare frauduloasă

---

[1] Directiva 2009/48/CE a Parlamentului European și a Consiliului din 18 iunie 2009 privind siguranța jucăriilor (JO L 170, 30.6.2009, p. 1).

ANEXA IV

PRODUSELE CRITICE CU ELEMENTE DIGITALE

1. Dispozitive hardware cu casete de securitate

2. Gateway-urile contoarelor inteligente din cadrul sistemelor de contorizare inteligentă în sensul definiției de la articolul 2 punctul 23 din Directiva (UE) 2019/944 a Parlamentului European și a Consiliului[1], și alte dispozitive utilizate în scopuri avansate de securitate, inclusiv pentru prelucrarea criptografică securizată

3. Carduri inteligente sau dispozitive similare, inclusiv elemente de securitate

---

[1] Directiva (UE) 2019/944 a Parlamentului European și a Consiliului din 5 iunie 2019 privind normele comune pentru piața internă de energie electrică și de modificare a Directivei 2012/27/UE (JO L 158, 14.6.2019, p. 125).

ANEXA V

DECLARAȚIA DE CONFORMITATE UE

Declarația de conformitate UE menționată la articolul 28 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 cu elemente digitale care să permită trasabilitatea, care poate include și o fotografie, după caz)

5. O declarație potrivit căreia obiectul declarației descris mai sus este conform cu legislația relevantă de armonizare 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 VI

DECLARAȚIA UE DE CONFORMITATE SIMPLIFICATĂ

Declarația UE de conformitate simplificată prevăzută la articolul 13 alineatul (20) se întocmește după cum urmează:

Prin prezenta, ... [denumirea producătorului] declară că produsul cu elemente digitale tip ... [denumirea tipului de produs cu element digital] este în conformitate cu Regulamentul (UE) 2024/…[+].

Textul integral al declarației de conformitate UE este disponibil la următoarea adresă internet: ...

[+] JO: a se introduce în text numărul regulamentului cuprins în documentul PE-CONS 100/23 (2022/0272(COD)).

ANEXA VII

CONȚINUTUL DOCUMENTAȚIEI TEHNICE

Documentația tehnică menționată la articolul 31 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 de securitate cibernetică;

   (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 cu elemente digitale și a proceselor de gestionare a vulnerabilităților, inclusiv:

   (a) informații necesare privind proiectarea și dezvoltarea produsului cu elemente digitale, inclusiv, dacă este cazul, desene și scheme și 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 necesare 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 necesare privind procesele de producție și de monitorizare a produsului cu elemente digitale și validarea proceselor respective;

3. o evaluare a riscurilor de securitate cibernetică împotriva cărora este proiectat, dezvoltat, fabricat, livrat și întreținut produsul cu elemente digitale, în temeiul articolului 13 din prezentul regulament, inclusiv modul în care sunt aplicabile cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I;

4. informațiile relevante care au fost luate în considerare pentru a stabili perioada de asistență în temeiul articolului 13 alineatul (8) a produsului cu elemente digitale;

5. 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 27 din prezentul regulament sau sistemele europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 în conformitate cu articolul 27 alineatul (8) din prezentul regulament 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 de securitate cibernetică prevăzute în anexa I părțile I și II, inclusiv o listă a altor specificații tehnice relevante aplicate. În cazul unor standarde armonizate, specificații comune sau sisteme europene de certificare de securitate cibernetică aplicate parțial, documentația tehnică trebuie să precizeze părțile care au fost aplicate;

6. rapoarte privind testele efectuate pentru verificarea conformității produsului cu elemente digitale și a proceselor de gestionare a vulnerabilităților cu cerințele esențiale de securitate cibernetică aplicabile, prevăzute în anexa I părțile I și II;

7. o copie a declarației de conformitate UE;

8. după caz, lista materialelor software, 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 de securitate cibernetică prevăzute în anexa I.

ANEXA VIII

PROCEDURI DE EVALUARE A CONFORMITĂȚII

Partea I 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 din prezenta parte și garantează și declară pe răspunderea sa exclusivă că produsele cu elemente digitale îndeplinesc toate cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și că producătorul îndeplinește cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

2. Producătorul întocmește documentația tehnică descrisă în anexa VII.

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 de securitate cibernetică prevăzute în anexa I părțile I și II.

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 28 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 perioada de asistență, 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 stabilite la punctul 4 pot fi îndeplinite de către reprezentantul său autorizat, în numele său și pe răspunderea sa, cu condiția ca obligațiile relevante să fie menționate în mandat.

Partea II 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 a unui produs cu elemente digitale și procesele de gestionare a vulnerabilităților instituite de producător și atestă că un produs cu elemente digitale îndeplinește cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și că producătorul îndeplinește cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

2. Examinarea UE de tip se efectuează prin evaluarea caracterului adecvat al proiectării și dezvoltării tehnice a produsului cu elemente digitale prin examinarea documentației tehnice și a documentelor justificative menționate la punctul 3 și prin 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:

   3.1 denumirea și adresa producătorului, iar dacă cererea este depusă de reprezentantul autorizat, se precizează și numele și adresa respectivului reprezentant autorizat;

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

3.3 documentația tehnică, care trebuie să permită evaluarea conformității produsului cu elemente digitale cu cerințele esențiale de securitate cibernetică aplicabile prevăzute în anexa I partea I și a proceselor de gestionare a vulnerabilităților ale producătorului cu cerințele esențiale aplicabile prevăzute în anexa I partea II și să includă o analiză și o evaluare adecvată a 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 cu elemente digitale. Documentația tehnică trebuie să cuprindă, ori de câte ori este necesar, elementele menționate în anexa VII;

3.4 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 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 cu elemente digitale sunt adecvate în raport cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și dacă procesele de gestionare a vulnerabilităților instituite de producător sunt adecvate în raport cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II;

4.2. verifică dacă exemplarele au fost dezvoltate sau produse în conformitate cu documentația tehnică și identifică elementele care au fost proiectate și dezvoltate în conformitate cu dispozițiile aplicabile din standardele armonizate 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 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 sau specificațiile tehnice relevante pentru cerințele prevăzute în anexa I, dacă soluțiile adoptate de către producător îndeplinesc cerințele esențiale de securitate cibernetică 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 de securitate cibernetică 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 cu elemente digitale 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 de securitate cibernetică 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 de securitate cibernetică aplicabile prevăzute în anexa I 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 de securitate cibernetică 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. Organismul notificat efectuează audituri periodice pentru a se asigura că procesele de gestionare a vulnerabilităților prevăzute în anexa I partea II sunt implementate în mod adecvat.

9. Fiecare organism notificat își informează autoritățile de notificare în legătură cu certificatele de examinare UE de tip și 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 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 eventualele suplimente la acestea pe care le-a refuzat, retras, suspendat sau restricționat în alt mod și, la cerere, în legătură cu certificatele și 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 a oricăror suplimente 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.

10. 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 cu elemente digitale sau pe perioada de asistență, oricare dintre ele este mai lungă.

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

Partea III 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 din prezenta parte și garantează și declară că produsele cu elemente digitale în cauză sunt conforme cu tipul descris în certificatul de examinare UE de tip și respectă cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și că producătorul îndeplinește cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

2. Producția

Producătorul ia toate măsurile necesare pentru ca procesul de producție și monitorizarea acestuia să asigure conformitatea produselor fabricate cu elemente digitale cu tipul aprobat descris în certificatul de examinare UE de tip și cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și se asigură că producătorul îndeplinește cerințele esențiale de securitate cibernetică prevăzute în anexa I partea II.

3. Marcajul de conformitate și declarația de conformitate

3.1. Producătorul aplică marcajul CE pe fiecare produs cu elemente digitale în parte care este conform cu tipul descris în certificatul de examinare UE de tip și care îndeplinește cerințele aplicabile prevăzute în prezentul regulament.

3.2. Producătorul întocmește o declarație de conformitate scrisă pentru un model de produs și o păstrează la dispoziția autorităților naționale timp de zece ani de la introducerea pe piață a produsului cu elemente digitale sau pe perioada de asistență, oricare dintre ele este mai lung**ă**. 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 obligațiile relevante să fie menționate în mandat.

Partea IV 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 din prezenta parte și garantează și declară pe răspunderea sa exclusivă că produsele cu elemente digitale sau categoriile de produse în cauză îndeplinesc cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și că procesele de gestionare a vulnerabilităților instituite de producător îndeplinesc cerințele prevăzute în anexa I partea II.

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 inspecția și testarea produsului final pentru produsele cu elemente digitale în cauză și pentru gestionarea vulnerabilităților, menține eficacitatea acestuia pe parcursul întregii perioade de asistență 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 cu elemente digitale în cauză.

Cererea trebuie să cuprindă:

(a) denumirea și adresa producătorului, iar dacă cererea este depusă de reprezentantul autorizat, se precizează și numele și adresa respectivului reprezentant autorizat;

(b) documentația tehnică pentru un singur model din fiecare categorie de produse cu elemente digitale care urmează a fi fabricate sau dezvoltate. Documentația tehnică trebuie să cuprindă, oricând este cazul, elementele menționate în anexa VII;

(c) documentația referitoare la sistemul de calitate; și

(d) 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 elemente digitale cu cerințele esențiale de securitate cibernetică prevăzute în anexa I partea I și conformitatea proceselor de gestionare a vulnerabilităților instituite de producător cu cerințele prevăzute în anexa I partea II.

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) 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;

(b) a specificațiilor privind proiectarea și dezvoltarea tehnică, inclusiv a standardelor, care vor fi aplicate și, în cazul în care standardele armonizate sau specificațiile tehnice relevante nu vor fi aplicate în totalitate, a mijloacelor care vor fi folosite pentru a asigura respectarea cerințelor esențiale de securitate cibernetică prevăzute în anexa I partea I care se aplică produselor cu elemente digitale respective;

(c) 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 de securitate cibernetică prevăzute în anexa I partea II care se aplică producătorului respectiv;

(d) 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 cu elemente digitale ce aparțin categoriei de produse vizate;

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

(f) 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;

(g) a înregistrărilor referitoare la calitate, cum ar fi rapoarte de inspecție și informații referitoare la teste, precum și date privind etalonarea și rapoarte referitoare la calificarea personalului implicat;

(h) 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 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 litera (b) 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 elemente digitale cu aceste cerințe.

Decizia este notificată producătorului sau reprezentantului autorizat al acestuia.

Notificarea trebuie să cuprindă concluziile procesului de audit şi 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:

(a) documentația privind sistemul de calitate;

(b) înregistrările referitoare la calitate, astfel cum sunt prevăzute în partea sistemului de calitate destinată proiectării, de exemplu rezultatele analizelor, ale calculelor și ale testelor;

(c) 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 și rapoarte privind calificarea personalului în cauză.

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 cu elemente digitale în parte care îndeplinește cerințele prevăzute în anexa I partea I.

5.2. Producătorul întocmește o declarație de conformitate scrisă pentru fiecare model de produs și o păstrează la dispoziția autorităților naționale timp de zece ani de la introducerea pe piață a produsului cu elemente digitale sau pe perioada de asistență, oricare dintre ele este mai lungă. 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 cu elemente digitale sau pe perioada de asistență, oricare dintre ele este mai lungă, producătorul menține la dispoziția autorităților naționale:

(a) documentația tehnică menționată la punctul 3.1;

(b) documentația privind sistemul de calitate prevăzută la punctul 3.1;

(c) modificarea menționată la punctul 3.5, astfel cum a fost aprobată;

(d) deciziile și rapoartele organismului notificat menționate la punctele 3.5 și 4.3.

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 obligațiile relevante să fie menționate în mandat.

Cu privire la acest act legislativ a fost formulată o declarație care se regăsește în … [a se completa de către Oficiul pentru Publicații: JO C XXX, XX.XX.2024, p. XX] și prin accesarea următorului link: [Oficiul pentru Publicații: a se introduce linkul către declarație].
