Consiliul
Uniunii Europene

Bruxelles, 16 septembrie 2022
(OR. en)

12429/22

Dosar interinstituțional:
2022/0272 (COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PROPUNERE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	15 septembrie 2022
Destinatar:	Secretariatul General al Consiliului
Nr. doc. Csie:	COM(2022) 454 final
Subiect:	Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020

În anexă, se pune la dispoziția delegațiilor documentul COM(2022) 454 final.

Anexă: COM(2022) 454 final

COMISIA
EUROPEANĂ

Bruxelles, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020

(Text cu relevanță pentru SEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

• Motivele și obiectivele propunerii

Produsele hardware și software fac din ce în ce mai mult obiectul unor atacuri cibernetice reușite, ceea ce a dus la un cost global anual al criminalității informatice estimat la 5,5 mii de miliarde EUR până în 2021. Aceste produse se confruntă cu două probleme majore, care generează costuri suplimentare pentru utilizatori și pentru societate: (1) un nivel scăzut de securitate cibernetică, care se reflectă în răspândirea pe scară largă a vulnerabilităților și în furnizarea insuficientă și inconsecventă de actualizări de securitate pentru abordarea acestora și (2) 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. Într-un mediu conectat, un incident de securitate cibernetică apărut la un produs poate afecta o întreagă organizație sau un întreg lanț de aprovizionare, propagându-se adesea dincolo de granițele pieței interne în decurs de câteva minute. Acest lucru poate duce la perturbări grave ale activităților economice și sociale sau chiar poate pune vieți în pericol.

Securitatea cibernetică a produselor cu elemente digitale are o puternică dimensiune transfrontalieră, deoarece produsele fabricate într-o țară sunt adesea utilizate pe întreaga piață internă. În plus, incidentele care afectează inițial o singură entitate sau un singur stat membru se răspândesc adesea în câteva minute pe întreaga piață internă.

Deși legislația existentă privind piața internă se aplică anumitor produse cu elemente digitale, majoritatea produselor hardware și software nu fac în prezent obiectul niciunui act legislativ al UE care să abordeze securitatea cibernetică a acestora. În special, cadrul juridic actual al UE nu abordează securitatea cibernetică a software-ului neîncorporat, chiar dacă atacurile cibernetice vizează din ce în ce mai mult vulnerabilitățile acestor produse, generând costuri societale și economice semnificative. Există numeroase exemple de atacuri cibernetice remarcabile care rezultă din securitatea suboptimă a produselor, cum ar fi viermele ransomware WannaCry, care în 2017 a exploatat o vulnerabilitate a sistemului Windows, afectând 200 000 de calculatoare din 150 de țări și cauzând daune în valoare de miliarde USD; atacul prin intermediul lanțului de aprovizionare al Kaseya VSA, care a utilizat software-ul de administrare a rețelei Kaseya pentru a ataca peste 1 000 de întreprinderi și a forțat un lanț de supermarketuri să închidă toate cele 500 de magazine din Suedia sau numeroasele incidente în care aplicațiile bancare sunt piratate pentru a fura bani de la consumatori fără ca aceștia să își dea seama.

Au fost identificate două obiective principale menite să asigure buna funcționare a pieței interne: (1) crearea condițiilor pentru dezvoltarea de produse cu elemente digitale care să fie sigure prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu mai puține vulnerabilități și că producătorii tratează cu seriozitate securitatea pe parcursul întregului ciclu de viață al unui produs și (2) crearea unor condiții care să le permită utilizatorilor să țină seama de securitatea cibernetică atunci când selectează și utilizează produse cu elemente digitale. Au fost stabilite patru obiective specifice: (i) asigurarea faptului că producătorii îmbunătățesc securitatea produselor cu elemente digitale încă din etapa de proiectare și dezvoltare și pe parcursul întregului ciclu de viață; (ii) asigurarea unui cadru coerent de securitate cibernetică, care să faciliteze conformarea producătorilor de hardware și software; (iii) sporirea transparenței proprietăților de securitate ale produselor cu elemente

digitale și (iv) facilitarea utilizării în condiții de siguranță a produselor cu elemente digitale de către întreprinderi și consumatori.

Caracterul transfrontalier puternic al securității cibernetice și numărul tot mai mare de incidente cu efecte de propagare la nivel transfrontalier, transsectorial și al produselor înseamnă că obiectivele nu pot fi realizate în mod eficace de către statele membre în mod individual. Din cauza caracterului global al piețelor produselor cu elemente digitale, statele membre se confruntă cu aceleași riscuri pentru același produs cu elemente digitale pe teritoriul lor. Apariția unui cadru fragmentat de norme naționale potențial divergente riscă să constituie o piedică pentru o piață unică deschisă și competitivă a produselor cu elemente digitale. Prin urmare, este necesară o acțiune comună la nivelul UE pentru a spori nivelul de încredere în rândul utilizatorilor și atractivitatea produselor cu elemente digitale ale UE. Aceasta ar fi benefică și pentru piața internă, întrucât ar oferi securitate juridică și ar crea condiții de concurență echitabile pentru vânzătorii de produse cu elemente digitale, astfel cum s-a subliniat și în raportul final al Conferinței privind viitorul Europei, în care cetățenii solicită ca UE să joace un rol mai important în combaterea amenințărilor la adresa securității cibernetice.

- **Interacțiunea cu dispozițiile deja existente în domeniul de politică vizat**

Cadrul UE cuprinde mai multe acte legislative orizontale care acoperă anumite aspecte legate de securitatea cibernetică din diferite perspective (produse, servicii, gestionarea crizelor și infracțiuni). În 2013 a intrat în vigoare Directiva privind atacurile împotriva sistemelor informatice[1], care armonizează incriminarea și sancțiunile pentru o serie de infracțiuni îndreptate împotriva sistemelor informatice. În august 2016 a intrat în vigoare Directiva (UE) 2016/1148 privind securitatea rețelelor și a sistemelor informatice (Directiva NIS)[2] ca prim act legislativ la nivelul UE privind securitatea cibernetică. Revizuirea sa, care a avut ca rezultat Directiva [Directiva XXX/XXXX (NIS2)], ridică nivelul comun de ambiție al UE. În 2019 a intrat în vigoare Regulamentul UE privind securitatea cibernetică[3], prin care se urmărește consolidarea securității produselor TIC, a serviciilor TIC și a proceselor TIC prin introducerea unui cadru european voluntar de certificare a securității cibernetice[4].

Securitatea cibernetică a întregului lanț de aprovizionare este asigurată numai dacă toate componentele acestuia îndeplinesc condițiile de securitate cibernetică. Legislația UE menționată mai sus prezintă însă lacune substanțiale în această privință, deoarece nu acoperă cerințele obligatorii de securitate pentru produsele cu elemente digitale.

---

1 Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).

2 Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (JO L 194/1, 19.7.2016, p. 1).

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

4 Regulamentul privind securitatea cibernetică permite dezvoltarea unor sisteme de certificare specifice. Fiecare sistem include trimiteri la standarde, specificații tehnice sau alte cerințe de securitate cibernetică relevante definite în sistemul respectiv. Decizia de a elabora o certificare de securitate cibernetică este una bazată pe riscuri.

În timp ce propunerea de Act european privind reziliența cibernetică vizează produsele cu elemente digitale introduse pe piață, Directiva [Directiva XXX/XXX (NIS2)] urmărește să asigure un nivel ridicat de securitate cibernetică pentru serviciile furnizate de entități esențiale și importante. Directiva [Directiva XXX/XXXX (NIS2)] impune statelor membre să se asigure că entitățile esențiale și importante din domeniul de aplicare, cum ar fi furnizorii de asistență medicală sau de servicii cloud și entitățile administrației publice, iau măsuri adecvate și proporționale de securitate cibernetică de natură tehnică, operațională și organizațională. Aceasta include, printre altele, cerința de a asigura securitatea în ceea ce privește achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice, inclusiv gestionarea și divulgarea vulnerabilităților. Directiva [Directiva XXX/XXXX (NIS2)] impune Comisiei să adopte acte de punere în aplicare prin care să stabilească cerințele tehnice și metodologice ale măsurilor respective în termen de 21 de luni de la data intrării în vigoare a directivei pentru anumite tipuri de entități, cum ar fi furnizorii de servicii de cloud computing. Pentru toate celelalte entități, Comisia poate adopta un act de punere în aplicare prin care să stabilească cerințele tehnice și metodologice, precum și cerințele sectoriale. Acest cadru va asigura faptul că specificații tehnice și măsuri similare cerințelor esențiale de securitate cibernetică prevăzute în Actul european privind reziliența cibernetică sunt puse în aplicare și pentru proiectarea, dezvoltarea și gestionarea vulnerabilităților software-ului furnizat ca serviciu (software ca serviciu). De exemplu, acesta ar putea fi un mijloc de a asigura un nivel ridicat de securitate cibernetică în cazuri precum cel al sistemelor de dosare electronice de sănătate (DES), inclusiv atunci când software-ul este furnizat sub formă de software ca serviciu (SaaS) sau dezvoltat în cadrul instituțiilor sanitare (intern), în conformitate cu propunerea de [Regulament privind spațiul european al datelor privind sănătatea].

- **Interacțiunea cu alte politici ale Uniunii**

Astfel cum se precizează în comunicarea „Conturarea viitorului digital al Europei”[5], este esențial ca UE să beneficieze de toate avantajele erei digitale și să își consolideze capacitatea industrială și de inovare, în cadrul anumitor limite de siguranță și de etică. Strategia europeană privind datele stabilește patru piloni – protecția datelor, drepturile fundamentale, siguranța și securitatea cibernetică – drept condiții prealabile esențiale pentru o societate autonomizată prin utilizarea datelor.

Cadrul actual al UE[6] aplicabil produselor care pot să includă și elemente digitale cuprinde mai multe acte legislative, printre care se numără atât acte legislative ale UE referitoare la produse specifice care vizează aspecte legate de siguranță, cât și acte legislative generale privind răspunderea pentru produse. Propunerea este coerentă cu actualul cadru de reglementare al UE referitor la produse, precum și cu propunerile legislative recente, cum ar fi Propunerea de regulament [Regulamentul privind inteligența artificială (IA)] a Comisiei[7].

Regulamentul propus ar urma să se aplice tuturor echipamentelor radio care intră în domeniul de aplicare al Regulamentului delegat (UE) 2022/30 al Comisiei. În plus, cerințele 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, inclusiv principalele elemente

---

5 Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor – „Conturarea viitorului digital al Europei” din 19 februarie 2020 [COM(2020) 67 final].

6 În principal, legislația privind noul cadru legislativ (NCL).

7 Propunere de regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) și de modificare a anumitor acte legislative ale Uniunii din 21 aprilie 2021 [COM(2021) 206 final].

prevăzute în [Decizia de punere în aplicare XXX/2022 a Comisiei privind o cerere de standardizare adresată organizațiilor europene de standardizare], emisă în temeiul regulamentului delegat respectiv. Pentru a se evita o suprapunere în materie de reglementare, se preconizează că Comisia ar urma să abroge sau să modifice regulamentul delegat în ceea ce privește echipamentele radio care fac obiectul propunerii de regulament, astfel încât regulamentul propus să se aplice echipamentelor respective, după ce va intra în vigoare.

În plus, pentru a se evita suprapunerea activităților, se preconizează că atât Comisia, cât și organizațiile europene de standardizare vor lua în considerare activitatea de standardizare desfășurată în contextul Deciziei de punere în aplicare C(2022) 5637 a Comisiei privind o cerere de standardizare pentru Regulamentul delegat 2022/30 RED atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a regulamentului.

2. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

• Temeiul juridic

Temeiul juridic al prezentei propuneri este articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE), care prevede adoptarea de măsuri pentru a asigura instituirea și funcționarea pieței interne. Scopul propunerii este de a armoniza cerințele de securitate cibernetică pentru produsele cu elemente digitale în toate statele membre și de a elimina obstacolele din calea liberei circulații a mărfurilor.

Articolul 114 din TFUE poate fi utilizat ca temei juridic pentru a preveni apariția acestor obstacole care ar rezulta din evoluția eterogenă a legislațiilor și abordărilor naționale cu privire la modul de abordare a cazurilor de insecuritate juridică și a lacunelor din cadrele juridice existente[8]. În plus, Curtea de Justiție a recunoscut că aplicarea unor cerințe tehnice eterogene ar putea constitui un motiv valabil pentru aplicarea articolului 114 din TFUE[9].

Actualul cadru legislativ al UE aplicabil produselor cu elemente digitale se bazează pe articolul 114 din TFUE și cuprinde mai multe acte legislative, inclusiv referitoare la produse specifice și la aspecte legate de siguranță sau acte legislative generale privind răspunderea pentru produse. Totuși, sunt acoperite numai anumite aspecte legate de securitatea cibernetică a produselor digitale fizice și, după caz, a software-ului încorporat în aceste produse. La nivel național, statele membre încep să ia măsuri naționale prin care solicită vânzătorilor de produse digitale să își îmbunătățească securitatea cibernetică[10]. În același timp, securitatea cibernetică a produselor digitale are o dimensiune transfrontalieră deosebit de puternică, deoarece produsele fabricate într-o țară sunt adesea utilizate de organizații și de consumatori din întreaga piață internă. Incidentele care afectează inițial o singură entitate sau un singur stat membru se răspândesc adesea în câteva minute la mai multe organizații, sectoare și state membre.

Diferitele acte și inițiative adoptate până în prezent la nivelul UE și la nivel național abordează doar parțial problemele identificate și riscă să creeze un mozaic legislativ în cadrul

---

8 Hotărârea CJUE (Marea Cameră) din 3 decembrie 2019, Republica Cehă/Parlamentul European și Consiliul Uniunii Europene, cauza C-482/17, punctul 35.

9 Hotărârea CJUE (Marea Cameră) din 2 mai 2006, Regatul Unit al Marii Britanii și Irlandei de Nord/Parlamentul European și Consiliul Uniunii Europene, cauza C-217/04, punctele 62-63.

10 De exemplu, în 2019, Finlanda a creat un sistem de etichetare pentru dispozitivele IoT, cum ar fi televizoarele inteligente, telefoanele inteligente și jucăriile, bazat pe standardele ETSI. Germania a introdus recent o etichetă de securitate pentru consumatori pentru routerele în bandă largă, televizoarele inteligente, camerele video, difuzoarele, jucăriile, precum și pentru roboții de curățenie și de grădinărit.

pieței interne, sporind insecuritatea juridică atât pentru vânzătorii, cât și pentru utilizatorii acestor produse și adăugând o sarcină inutilă întreprinderilor pentru respectarea unor cerințe pentru tipuri similare de produse.

Regulamentul propus ar urma să armonizeze și să simplifice peisajul de reglementare al UE prin introducerea unor cerințe de securitate cibernetică pentru produsele cu elemente digitale și ar evita suprapunerea cerințelor care decurg din acte legislative diferite. Acest lucru ar crea o mai mare securitate juridică pentru operatorii și utilizatorii din întreaga Uniune, precum și o mai bună armonizare a pieței unice europene, oferind condiții mai viabile pentru operatorii care doresc să intre pe piața UE.

- **Subsidiaritate (în cazul competențelor neexclusive)**

Caracterul transfrontalier puternic al securității cibernetice în general și numărul tot mai mare de riscuri și incidente care au efecte de propagare dincolo de frontiere, sectoare și produse fac ca obiectivele prezentei intervenții să nu poată fi realizate în mod eficace de către statele membre în mod individual. Abordările naționale în ceea ce privește soluționarea problemelor, în special abordările care introduc cerințe obligatorii, vor crea o insecuritate juridică suplimentară și obstacole juridice suplimentare. Întreprinderile ar putea fi împiedicate să se extindă fără probleme în alte state membre, ceea ce ar priva utilizatorii de posibilitatea de a beneficia de produsele acestora.

Prin urmare, este necesară o acțiune comună la nivelul UE pentru a stabili un nivel ridicat de încredere în rândul utilizatorilor, sporind atractivitatea produselor cu elemente digitale ale UE. Aceasta ar fi benefică și pentru piața unică digitală și pentru piața internă în general, întrucât ar oferi securitate juridică și ar crea condiții de concurență echitabile pentru producătorii de produse cu elemente digitale.

Ca ultim aspect, Concluziile Consiliului din 23 mai 2022 privind dezvoltarea posturii de securitate a Uniunii Europene invită Comisia să propună, până la sfârșitul anului 2022, cerințe comune de securitate cibernetică pentru dispozitivele conectate.

- **Proporționalitate**

În ceea ce privește proporționalitatea regulamentului propus, măsurile din opțiunile de politică avute în vedere nu ar depăși ceea ce este necesar pentru atingerea obiectivelor generale și specifice și nu ar impune costuri disproporționate. Mai precis, intervenția avută în vedere ar garanta securizarea produselor cu elemente digitale pe parcursul întregului lor ciclu de viață și proporțional cu riscurile cu care se confruntă acestea prin intermediul unor cerințe orientate către obiective și neutre din punct de vedere tehnologic, care rămân rezonabile și corespund, în general, interesului entităților implicate.

Cerințele esențiale de securitate cibernetică prevăzute în propunere se bazează pe standarde utilizate pe scară largă, iar procesul de standardizare care va urma ar ține seama de particularitățile tehnice ale produselor. Aceasta înseamnă că, atunci când este necesar pentru un anumit nivel de risc, controalele de securitate ar fi adaptate. În plus, normele orizontale avute în vedere ar prevedea doar evaluarea de către terți a produselor critice. Aceasta ar include doar o proporție redusă din piața produselor cu elemente digitale. Impactul asupra IMM-urilor ar depinde de prezența lor pe piața acestor categorii de produse specifice.

În ceea ce privește proporționalitatea costurilor pentru evaluarea conformității, organismele notificate care efectuează evaluările de către terți ar lua în considerare dimensiunea întreprinderii la stabilirea tarifelor. De asemenea, ar fi prevăzută o perioadă de tranziție rezonabilă de 24 de luni pentru pregătirea punerii în aplicare, acordându-se timp piețelor relevante pentru a se pregăti și oferind în același timp o direcție clară pentru investițiile în

cercetare și dezvoltare. Eventualele costuri de conformare suportate de întreprinderi ar fi compensate de avantajele aduse de un nivel mai ridicat de securitate a produselor cu elemente digitale și, în ultimă instanță, de o creștere a încrederii utilizatorilor în aceste produse.

- **Alegerea instrumentului**

O intervenție normativă ar implica adoptarea unui regulament, și nu a unei directive. Motivul constă în faptul că, pentru acest tip specific de legislație privind produsele, un regulament ar aborda problemele identificate și ar îndeplini obiectivele formulate într-un mod mai eficace, fiind vorba despre o intervenție care condiționează introducerea pe piața internă a unei categorii foarte largi de produse. Procesul de transpunere în cazul unei directive pentru o astfel de intervenție ar putea lăsa prea mult spațiu de manevră la nivel național, ceea ce ar putea duce la o lipsă de uniformitate a anumitor cerințe esențiale de securitate cibernetică, la insecuritate juridică, la o fragmentare suplimentară sau chiar la situații discriminatorii la nivel transfrontalier, cu atât mai mult cu cât produsele vizate ar putea avea scopuri sau utilizări multiple și că producătorii pot produce mai multe categorii de astfel de produse.

3. REZULTATELE EVALUĂRILOR EX POST, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

- **Consultări cu părțile interesate**

Comisia a consultat o gamă largă de părți interesate. Statele membre și părțile interesate au fost invitate să participe la consultarea publică deschisă și la sondajele și atelierele organizate în contextul unui studiu realizat de un consorțiu care sprijină activitatea pregătitoare a Comisiei pentru evaluarea impactului: Wavestone, Centrul de Studii Politice Europene (CEPS) și ICF. Printre părțile interesate consultate s-au numărat autorități naționale de supraveghere a pieței, organisme ale Uniunii care se ocupă de securitatea cibernetică, producători de hardware și software, importatori și distribuitori de hardware și software, asociații comerciale, organizații de consumatori și utilizatori de produse cu elemente digitale, precum și cetățeni, cercetători și reprezentanți ai mediului academic, organisme notificate, organisme de acreditare și profesioniști din sectorul securității cibernetice.

Activitățile de consultare au inclus:

- un prim studiu realizat de un consorțiu format din ICF, Wavestone, Carsa și CEPS, care a fost publicat în decembrie 2021[11]. Studiul a identificat mai multe disfuncționalități ale pieței și a evaluat posibilele intervenții normative;
- o consultare publică deschisă care s-a adresat cetățenilor, părților interesate și experților în domeniul securității cibernetice. S-au transmis 176 de răspunsuri. Acestea au contribuit la colectarea de opinii și experiențe diverse de la toate categoriile de părți interesate;
- atelierele organizate de studiul care sprijină activitatea pregătitoare a Comisiei pentru un Act european privind reziliența cibernetică au reunit aproximativ 100 de reprezentanți din toate cele 27 de state membre, reprezentând o varietate de părți interesate;

[11] *Study on the need of Cybersecurity requirements for ICT products* (Studiu privind necesitatea unor cerințe în materie de securitate cibernetică pentru produsele TIC), Nr. 2020-0715, raport final al studiului, disponibil la adresa https://digital-strategy.ec.europa.eu/en/library/study-need-cybersecurity-requirements-ict-products.

- au fost realizate interviuri cu experți pentru a înțelege mai bine provocările actuale în materie de securitate cibernetică legate de produsele cu elemente digitale și pentru a discuta opțiunile de politică pentru o eventuală intervenție normativă;
- au avut loc discuții bilaterale cu autoritățile naționale din domeniul securității cibernetice, cu sectorul privat și cu organizațiile de consumatori;
- au avut loc acțiuni specifice de informare a principalelor părți interesate din rândul IMM-urilor.

- **Obținerea și utilizarea expertizei**

Activitățile de consultare au vizat obținerea de contribuții cu privire la cele cinci criterii principale de evaluare bazate pe Orientările UE privind o mai bună legiferare (eficacitate, eficiență, relevanță, coerență, valoare adăugată europeană), precum și la impactul potențial al opțiunilor posibile pentru viitor. Contractantul nu numai că a contactat părțile interesate care ar fi afectate în mod direct de regulamentul propus, ci a consultat, de asemenea, o gamă largă de experți în domeniul securității cibernetice.

- **Evaluarea impactului**

Comisia a efectuat o evaluare a impactului pentru prezenta propunere, care a fost examinată de Comitetul de control normativ (CCN) al Comisiei. La 6 iulie 2022 a avut loc o reuniune cu CCN, urmată de un aviz pozitiv. Evaluarea impactului a fost ajustată pentru a răspunde recomandărilor și observațiilor CCN.

Comisia a examinat diferite opțiuni de politică pentru atingerea obiectivului general al propunerii:

- o abordare bazată pe instrumente juridice neobligatorii și măsuri voluntare (opțiunea 1): În cadrul acestei opțiuni, nu ar exista nicio intervenție normativă obligatorie. În schimb, Comisia ar emite comunicări, orientări, recomandări și, eventual, coduri de conduită pentru a încuraja măsurile voluntare. Ar fi elaborate în continuare sisteme naționale, voluntare sau obligatorii, pentru a compensa lipsa unor norme orizontale ale UE.
- o intervenție normativă ad-hoc pentru securitatea cibernetică a produselor fizice cu elemente digitale și a software-ului încorporat în acestea (opțiunea 2): Această opțiune ar implica o intervenție normativă ad-hoc specifică produselor, care s-ar limita la completarea și/sau modificarea cerințelor de securitate cibernetică prevăzute în legislația deja existentă sau la introducerea unor acte normative noi pe măsură ce apar noi riscuri, inclusiv în ceea ce privește software-ul neîncorporat.

Opțiunile 3 și 4 implică o intervenție normativă orizontală care variază ca domeniu de aplicare, urmând în mare parte noul cadru legislativ (NCL). Acest cadru stabilește cerințe esențiale ca o condiție pentru introducerea anumitor produse pe piața internă. De asemenea, NCL prevede, de regulă, evaluarea conformității, procesul desfășurat de producător pentru a demonstra că au fost îndeplinite cerințele specificate referitoare la un produs.

- O abordare mixtă, incluzând norme orizontale obligatorii pentru securitatea cibernetică a produselor fizice cu elemente digitale și a software-ului încorporat în acestea și o abordare eșalonată pentru software-ul neîncorporat (opțiunea 3): Această opțiune ar implica un regulament care să introducă

cerințe orizontale de securitate cibernetică pentru toate produsele fizice cu elemente digitale și pentru software-ul încorporat în acestea, ca o condiție pentru introducerea pe piață, și ar include două subopțiuni, cu și fără evaluarea obligatorie de către terți (3i și 3ii). Software-ul neîncorporat nu ar fi reglementat.

- O intervenție normativă orizontală care să introducă cerințe de securitate cibernetică pentru o gamă largă de produse, fizice sau nu, cu elemente digitale, inclusiv pentru software-ul neîncorporat (opțiunea 4): Această opțiune se aseamănă cu opțiunea 3, exceptând domeniul de aplicare. Opțiunea 4 ar include software-ul neîncorporat [cu două subopțiuni incluzând numai software-ul critic (4a) sau orice software (4b)] în domeniul de aplicare al unei eventuale reglementări. Pentru fiecare subopțiune, ar fi luate în considerare aceleași subopțiuni referitoare la evaluarea conformității ca în cazul opțiunii 3.

Opțiunea 4 (cu subopțiunea care acoperă orice software și cea care implică evaluarea obligatorie de către terți a produselor critice) s-a dovedit a fi opțiunea preferată pe baza evaluării eficacității în raport cu obiectivele specifice și a eficienței costurilor în raport cu beneficiile. Această opțiune ar asigura stabilirea unor cerințe orizontale specifice de securitate cibernetică pentru toate produsele cu elemente digitale introduse sau puse la dispoziție pe piața internă și ar fi singura opțiune care acoperă întregul lanț de aprovizionare digital. O astfel de intervenție normativă ar acoperi și software-ul neîncorporat, care este adesea expus vulnerabilităților, asigurând astfel o abordare coerentă a tuturor produselor cu elemente digitale, cu o repartizare clară a responsabilităților diferiților operatori economici.

De asemenea, această opțiune de politică aduce valoare adăugată prin faptul că acoperă aspectele legate de obligația de diligență și de întregul ciclu de viață după introducerea pe piață a produselor cu elemente digitale, pentru a asigura, printre altele, informații adecvate privind asistența în materie de securitate și furnizarea de actualizări de securitate. În același timp, această opțiune de politică ar completa în modul cel mai eficace reexaminarea recentă a cadrului NIS, prin asigurarea condițiilor prealabile pentru consolidarea securității lanțului de aprovizionare.

Opțiunea preferată ar aduce avantaje semnificative diferitelor părți interesate. În ceea ce privește întreprinderile, acest lucru ar preveni normele de securitate divergente pentru produsele cu elemente digitale și ar reduce costurile de conformare pentru legislația conexă în materie de securitate cibernetică. De asemenea, ar reduce numărul de incidente cibernetice, costurile de gestionare a incidentelor și atingerea adusă reputației. În ceea ce privește UE în ansamblu, se estimează că inițiativa ar putea duce la o reducere a costurilor generate de incidentele care afectează întreprinderile cu aproximativ 180-290 de miliarde EUR anual. Inițiativa ar duce la o creștere a cifrei de afaceri ca urmare a creșterii cererii de produse cu elemente digitale. Ea ar îmbunătăți reputația globală a întreprinderilor, ceea ce ar duce la o creștere a cererii și în afara UE. În ceea ce privește utilizatorii, opțiunea preferată ar spori transparența proprietăților de securitate și ar facilita utilizarea produselor cu elemente digitale. Consumatorii și cetățenii ar beneficia, de asemenea, de o mai bună protecție a drepturilor lor fundamentale, cum ar fi protecția vieții private și a datelor.

Atunci când li s-a solicitat să evalueze eficacitatea intervențiilor de politică, respondenții la consultarea publică au fost de acord că opțiunea 4 ar fi cea mai eficace măsură (4,08 pe o scară de la 1 la 5). Printre aceștia s-au numărat organizații de consumatori (5,00), respondenți care se identifică drept utilizatori (4,22), organisme notificate (4,17), autorități de supraveghere a pieței (5,00) și producători de produse cu elemente digitale (3,85), inclusiv cei de dimensiuni mici și mijlocii (4,05).

- **Adecvarea reglementărilor și simplificarea**

Prezenta propunere stabilește cerințe care se vor aplica producătorilor de software și de hardware. Este necesar să se asigure securitatea juridică și să se evite fragmentarea suplimentară a cerințelor legate de produse privind securitatea cibernetică pe piața internă, fapt demonstrat de sprijinul larg al diferitelor părți interesate pentru o intervenție orizontală. Propunerea va reduce la minimum sarcina de reglementare impusă producătorilor prin mai multe acte privind siguranța produselor. Alinierea la NCL înseamnă o mai bună funcționare a intervenției și a asigurării respectării acesteia. Propunerea simplifică procesul procedurilor de salvgardare, implicând producătorii și statele membre înainte de notificarea Comisiei. O mare parte a producătorilor care intră în domeniul de aplicare al propunerii sunt deja familiarizați cu funcționarea NCL, ceea ce va contribui la înțelegerea și punerea sa în aplicare. În ceea ce privește consumatorii și întreprinderile, propunerea va promova încrederea în produsele cu elemente digitale.

- **Drepturile fundamentale**

Se preconizează că toate opțiunile de politică vor îmbunătăți într-o anumită măsură protecția drepturilor și libertăților fundamentale, cum ar fi viața privată, protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială și protecția proprietății sau a demnității și integrității personale. În special, opțiunea de politică preferată, opțiunea 4, care constă în intervenții normative orizontale și are un domeniu larg de aplicare al politicilor, ar fi cea mai eficace în această privință, deoarece este mai probabil să contribuie la reducerea numărului și a gravității incidentelor, inclusiv a încălcărilor securității datelor cu caracter personal. De asemenea, aceasta ar spori securitatea juridică și ar asigura condiții de concurență echitabile pentru operatorii economici, ar spori încrederea în rândul utilizatorilor și atractivitatea produselor cu elemente digitale ale UE în ansamblu, protejând astfel proprietatea și îmbunătățind condițiile în care operatorii economici pot desfășura o activitate comercială.

Cerințele orizontale de securitate cibernetică ar contribui la securitatea datelor cu caracter personal prin protejarea confidențialității, a integrității și a disponibilității informațiilor din produsele cu elemente digitale. Respectarea acestor cerințe va facilita respectarea cerinței de securitate a prelucrării datelor cu caracter personal în temeiul Regulamentului (UE) 2016/679 [Regulamentul general privind protecția datelor (RGPD)][12]. Propunerea ar spori transparența și ar îmbunătăți informarea utilizatorilor, inclusiv a celor care ar putea fi mai puțin înzestrați cu competențe în materie de securitate cibernetică. De asemenea, utilizatorii ar fi mai bine informați cu privire la riscurile, capabilitățile și limitările produselor cu elemente digitale, ceea ce i-ar ajuta să ia măsurile preventive și de atenuare necesare pentru a reduce riscurile reziduale.

4. IMPLICAȚII BUGETARE

Pentru a îndeplini sarcinile atribuite Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) în temeiul prezentului regulament, ENISA va trebui să realoce resurse constând în aproximativ 4,5 ENI. Comisia ar trebui să aloce 7 ENI pentru a-și îndeplini responsabilitățile legate de asigurarea respectării legislației în temeiul prezentului regulament.

[12] 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).

O prezentare detaliată a costurilor implicate este inclusă în „fișa financiară” aferentă prezentei propuneri.

5. ALTE ELEMENTE

- **Planuri de punere în aplicare și modalități de monitorizare, evaluare și raportare**

Comisia va monitoriza punerea în practică, aplicarea și respectarea acestor dispoziții noi în vederea evaluării eficacității acestora. Regulamentul va impune o evaluare și o reexaminare din partea Comisiei, precum și prezentarea unui raport public în acest sens Parlamentului European și Consiliului în termen de 36 de luni de la data aplicării și, ulterior, o dată la patru ani.

- **Explicații detaliate cu privire la prevederile specifice ale propunerii**

Dispoziții generale (capitolul I)

Prezenta propunere de regulament stabilește (a) norme pentru introducerea pe piață a produselor cu elemente digitale în vederea asigurării securității cibernetice a acestor produse; (b) cerințe esențiale pentru proiectarea, dezvoltarea și producția de produse cu elemente digitale, precum și obligațiile operatorilor economici în legătură cu aceste produse în ceea ce privește securitatea cibernetică; (c) cerințe esențiale pentru procesele de gestionare a vulnerabilităților instituite de producători pentru a asigura securitatea cibernetică a produselor cu elemente digitale pe parcursul întregului ciclu de viață, precum și obligațiile operatorilor economici în legătură cu aceste procese; (d) norme privind supravegherea pieței și asigurarea respectării normelor și cerințelor menționate mai sus.

Regulamentul propus se va aplica tuturor produselor cu elemente digitale a căror utilizare preconizată și previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv sau la o rețea.

Regulamentul propus nu se va aplica produselor cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) 2017/745 [dispozitivele medicale pentru uz uman și accesoriile pentru astfel de dispozitive] și al Regulamentului (UE) 2017/746 [dispozitivele medicale pentru diagnostic *in vitro* pentru uz uman și accesoriile pentru astfel de dispozitive], întrucât cele două regulamente menționate conțin cerințe referitoare la dispozitive, inclusiv la software, și obligații generale ale producătorilor care acoperă întregul ciclu de viață al produselor, precum și proceduri de evaluare a conformității. Prezentul regulament nu se va aplica produselor cu elemente digitale care au fost certificate în conformitate cu Regulamentul 2018/1139 [nivel uniform ridicat de siguranță a aviației civile] și nici produselor cărora li se aplică Regulamentul (UE) 2019/2144 [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].

Produsele critice cu elemente digitale fac obiectul unor proceduri specifice de evaluare a conformității și sunt împărțite în clasele I și II stabilite în anexa III, în funcție de nivelul lor de risc de securitate cibernetică, clasa II reprezentând un risc mai mare. Un produs cu elemente digitale este considerat critic și, prin urmare, este inclus în anexa III având în vedere impactul potențialelor vulnerabilități în ceea ce privește securitatea cibernetică incluse în respectivul produs cu elemente digitale. La stabilirea riscului de securitate cibernetică se iau în considerare, printre altele, funcționalitatea legată de securitatea cibernetică a produsului cu elemente digitale și utilizarea preconizată în medii sensibile, cum ar fi un cadru industrial.

De asemenea, Comisia este împuternicită să adopte acte delegate pentru a completa prezentul regulament prin specificarea categoriilor de produse deosebit de critice cu elemente digitale, pentru care producătorii au obligația de a obține un certificat european de securitate cibernetică în cadrul unui sistem european de certificare de securitate cibernetică pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I sau cu anumite părți ale acestora. Atunci când stabilește aceste categorii de produse deosebit de critice cu elemente digitale, Comisia ține seama de nivelul de risc de securitate cibernetică aferent categoriei respective de produse cu elemente digitale, având în vedere unul sau mai multe dintre criteriile luate în considerare pentru includerea produselor critice cu elemente digitale în anexa III, precum și evaluând dacă respectiva categorie de produse este utilizată sau dacă se bazează pe ea entitățile esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)] sau dacă aceasta va avea o potențială semnificație viitoare pentru activitățile entităților respective; sau dacă este relevantă pentru reziliența întregului lanț de aprovizionare al produselor cu elemente digitale împotriva evenimentelor perturbatoare.

Obligațiile operatorilor economici (capitolul II)

Propunerea include obligații pentru producători, importatori și distribuitori pe baza dispozițiilor de referință prevăzute în Decizia 768/2008/CE. Cerințele esențiale și obligațiile în materie de securitate cibernetică impun ca toate produsele cu elemente digitale să fie puse la dispoziție pe piață numai dacă, atunci când sunt furnizate, instalate, întreținute și utilizate în mod corespunzător pentru scopul preconizat sau în condiții care pot fi prevăzute în mod rezonabil, ele îndeplinesc cerințele esențiale de securitate cibernetică prevăzute în prezentul regulament.

Cerințele esențiale și obligațiile ar urma să impună producătorilor să ia în considerare securitatea cibernetică în proiectarea, dezvoltarea și producția produselor cu elemente digitale, să exercite diligența necesară în ceea ce privește aspectele de securitate atunci când își proiectează și își dezvoltă produsele, să fie transparenți în ceea ce privește aspectele de securitate cibernetică care trebuie să fie aduse la cunoștința clienților, să asigure asistență în materie de securitate (actualizări) în mod proporțional și să respecte cerințele de gestionare a vulnerabilităților.

Ar urma să se stabilească obligații pentru operatorii economici, începând de la producători și până la distribuitori și importatori, în ceea ce privește introducerea pe piață a produselor cu elemente digitale, în funcție de rolul și responsabilitățile lor în cadrul lanțului de aprovizionare.

Conformitatea produsului cu elemente digitale (capitolul III)

Un produs cu elemente digitale care este în conformitate cu standardele armonizate sau cu anumite părți ale acestora, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, este considerat a fi în conformitate cu cerințele esențiale ale prezentei propuneri de regulament. În cazul în care nu există standarde armonizate sau sunt insuficiente sau în cazul în care există întârzieri nejustificate în procedura de standardizare sau în cazul în care cererea Comisiei nu a fost acceptată de organizațiile de standardizare europene, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, specificații comune.

În plus, produsele cu elemente digitale care au fost certificate sau pentru care s-a emis o declarație de conformitate UE sau un certificat în cadrul unui sistem european de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 și pentru care Comisia a specificat, prin intermediul unui act de punere în aplicare, că poate oferi prezumția de conformitate pentru prezentul regulament, sunt considerate a fi în conformitate cu cerințele esențiale ale prezentului regulament sau cu anumite părți ale acestora, în măsura în care

declarația de conformitate UE sau certificatul de securitate cibernetică sau anumite părți ale acestora acoperă cerințele respective.

În plus, pentru a evita o sarcină administrativă nejustificată pentru producători, după caz, Comisia ar trebui să precizeze dacă un certificat de securitate cibernetică emis în cadrul unui astfel de sistem european de certificare de securitate cibernetică elimină obligația producătorilor de a efectua o evaluare a conformității de către terți, astfel cum se prevede în prezentul regulament pentru cerințele corespunzătoare.

Producătorul efectuează o evaluare a conformității produsului cu elemente digitale și a proceselor de gestionare a vulnerabilităților pe care le-a instituit pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I, urmând una dintre procedurile prevăzute în anexa VI. Producătorii de produse critice din clasele I și II utilizează modulele respective necesare pentru conformare. Producătorii de produse critice din clasa II trebuie să implice o parte terță în evaluarea conformității.

Notificarea organismelor de evaluare a conformității (capitolul IV)

Buna funcționare a organismelor notificate este crucială pentru a asigura un nivel ridicat de securitate cibernetică, precum și pentru încrederea tuturor părților interesate în sistemul informațional NANDO. În consecință, conform Deciziei nr. 768/2008/CE, propunerea stabilește cerințele aplicabile autorităților naționale responsabile de organismele de evaluare a conformității (organisme notificate). Ea lasă statelor membre responsabilitatea finală pentru desemnarea și monitorizarea organismelor notificate. Statele membre desemnează o autoritate de notificare care este responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea și notificarea organismelor de evaluare a conformității și cu monitorizarea organismelor notificate.

Supravegherea pieței și asigurarea respectării legislației (capitolul V)

În conformitate cu Regulamentul (UE) 2019/1020, autoritățile naționale de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru respectiv. Statele membre pot alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile naționale competente menționate la articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] sau autoritățile naționale desemnate de certificare a securității cibernetice menționate la articolul 58 din Regulamentul (UE) 2019/881. Operatorii economici sunt invitați să coopereze pe deplin cu autoritățile de supraveghere a pieței și cu alte autorități competente.

Competențele delegate și procedura comitetului (capitolul VI)

Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, Comisiei îi este delegată competența de a adopta acte în conformitate cu articolul 290 din TFUE pentru a actualiza lista produselor critice din clasele I și II și pentru a preciza definițiile acestor produse; pentru a preciza dacă este necesară o limitare sau o excludere pentru produsele cu elemente digitale care fac obiectul altor norme ale Uniunii prin care se stabilesc cerințe care asigură același nivel de protecție ca prezentul regulament; pentru a impune certificarea anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor stabilite în prezentul regulament; pentru a preciza conținutul minim al declarației de conformitate UE și a completa elementele care trebuie incluse în documentația tehnică.

Comisia este împuternicită să adopte acte de punere în aplicare: pentru a preciza formatul sau elementele obligațiilor de raportare și ale listei materialelor software; pentru a preciza sistemele europene de certificare de securitate cibernetică care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu anumite părți ale acestora, astfel cum sunt prevăzute în prezentul regulament; pentru a adopta specificații comune; pentru a stabili

specificațiile tehnice pentru aplicarea marcajului CE; pentru a adopta măsuri corective sau restrictive la nivelul Uniunii în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne.

Confidențialitate și sancțiuni (capitolul VII)

Toate părțile care aplică prezentul regulament respectă confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și activităților lor.

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. În aceeași ordine de idei, prezentul regulament stabilește niveluri maxime pentru amenzile administrative care ar trebui prevăzute în legislația națională pentru nerespectarea obligațiilor prevăzute în prezentul regulament.

Dispoziții tranzitorii și finale (capitolul VIII)

Pentru a acorda producătorilor, organismelor notificate și statelor membre timpul necesar pentru a se adapta la noile cerințe, regulamentul propus va deveni aplicabil la [24 de luni] de la intrarea sa în vigoare, cu excepția obligației de raportare care revine producătorilor, care s-ar aplica începând cu [12 luni] de la data intrării în vigoare.

2022/0272 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

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

având în vedere avizul Comitetului Regiunilor[2],

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

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

(2) Prezentul regulament are ca scop stabilirea condițiilor-limită pentru dezvoltarea de produse cu elemente digitale care să fie sigure prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu mai puține vulnerabilități și că producătorii tratează cu seriozitate securitatea pe parcursul întregului ciclu de viață al unui produs. De asemenea, prezentul regulament are ca scop crearea unor condiții care să le permită utilizatorilor să țină seama de securitatea cibernetică atunci când selectează și utilizează produse cu elemente digitale.

(3) Legislația relevantă a Uniunii aflată în prezent în vigoare cuprinde mai multe seturi de norme orizontale care abordează anumite aspecte legate de securitatea cibernetică din diferite perspective, incluzând măsuri de îmbunătățire a securității lanțului de aprovizionare digital. Cu toate acestea, legislația existentă a Uniunii referitoare la

[1] JO C , , p. .
[2] JO C , , p. .

securitatea cibernetică, inclusiv [Directiva XXX/XXXX (NIS2)] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[3], nu acoperă în mod direct cerințele obligatorii de securitate a produselor cu elemente digitale.

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

(5) La nivelul Uniunii, diverse documente programatice și politice, cum ar fi Strategia de securitate cibernetică a UE pentru deceniul digital[4], Concluziile Consiliului din 2 decembrie 2020 și din 23 mai 2022 sau Rezoluția Parlamentului European din 10 iunie 2021[5], au solicitat cerințe specifice de securitate cibernetică ale Uniunii pentru produsele digitale sau conectate, mai multe țări din întreaga lume introducând măsuri pentru a aborda această chestiune din proprie inițiativă. În raportul final al Conferinței privind viitorul Europei[6], cetățenii au solicitat „un rol mai important al UE în contracararea amenințărilor la adresa securității cibernetice”.

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

(7) În anumite condiții, toate produsele cu elemente digitale integrate într-un sistem electronic de informații mai mare sau conectate la un astfel de sistem pot servi drept vector de atac pentru actorii rău-intenționați. În consecință, chiar și hardware-ul și software-ul considerate mai puțin critice pot facilita compromiterea inițială a unui dispozitiv sau a unei rețele, permițând actorilor rău-intenționați să obțină un acces privilegiat la un sistem sau să se deplaseze lateral între sisteme. Prin urmare,

---

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

[5] 2021/2568 (RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_RO.html.

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

producătorii ar trebui să se asigure că toate produsele conectabile cu elemente digitale sunt proiectate și dezvoltate în conformitate cu cerințele esențiale prevăzute în prezentul regulament. Sunt incluse atât produsele care pot fi conectate fizic prin interfețe hardware, cât și produsele care sunt conectate logic, de exemplu prin intermediul unor prize de rețea, canale, fișiere, interfețe de programare a aplicațiilor sau orice alt tip de interfață software. Întrucât amenințările la adresa securității cibernetice se pot propaga prin diverse produse cu elemente digitale înainte de a atinge un anumit obiectiv, de exemplu prin înlănțuirea mai multor exploatări de vulnerabilități, producătorii ar trebui să asigure, de asemenea, securitatea cibernetică a produselor care sunt conectate doar indirect la alte dispozitive sau rețele.

(8) Prin stabilirea unor cerințe de securitate cibernetică pentru introducerea pe piață a produselor cu elemente digitale, securitatea cibernetică a acestor produse va fi îmbunătățită atât pentru consumatori, cât și pentru întreprinderi. Sunt incluse, de asemenea, cerințe privind introducerea pe piață a produselor de consum cu elemente digitale destinate consumatorilor vulnerabili, cum ar fi jucăriile și monitoarele pentru sugari.

(9) Prezentul regulament asigură un nivel ridicat de securitate cibernetică a produselor cu elemente digitale. Acesta nu reglementează serviciile, precum software-ul ca serviciu (SaaS), cu excepția soluțiilor de prelucrare de date la distanță referitoare la un produs cu elemente digitale, înțelese ca orice prelucrare de date la distanță pentru care software-ul este proiectat și dezvoltat de producătorul produsului în cauză sau sub responsabilitatea producătorului respectiv și a cărei absență ar împiedica un astfel de produs cu elemente digitale să își îndeplinească una dintre funcții. [Directiva XXX/XXXX (NIS2)] instituie cerințe de raportare a securității cibernetice și a incidentelor pentru entitățile esențiale și importante, cum ar fi infrastructura critică, în vederea creșterii rezilienței serviciilor pe care le furnizează. [Directiva XXX/XXXX (NIS2)] se aplică serviciilor de cloud computing și modelelor de servicii de cloud, precum SaaS. Toate entitățile care furnizează servicii de cloud computing în Uniune și care ating sau depășesc pragul pentru întreprinderile mijlocii intră în domeniul de aplicare al directivei respective.

(10) Pentru a nu împiedica inovarea sau cercetarea, software-ul liber și cu sursă deschisă dezvoltat sau furnizat în afara desfășurării unei activități comerciale nu ar trebui să intre sub incidența prezentului regulament. Acest lucru este valabil în special în cazul software-ului, inclusiv al codului sursă și al versiunilor modificate ale acestuia, care este partajat în mod deschis și care poate fi accesat, utilizat, modificat și distribuit în mod liber. În contextul software-ului, o activitate comercială ar putea fi caracterizată nu numai prin perceperea unui preț pentru un produs, ci și prin perceperea unui preț pentru servicii de asistență tehnică, prin furnizarea unei platforme software prin intermediul căreia producătorul monetizează alte servicii sau prin utilizarea datelor cu caracter personal în alte scopuri decât îmbunătățirea securității, a compatibilității sau a interoperabilității software-ului.

(11) Un internet sigur este indispensabil pentru funcționarea infrastructurilor critice și pentru societate în ansamblu. [Directiva XXX/XXXX (NIS2)] vizează asigurarea unui nivel ridicat de securitate cibernetică a serviciilor furnizate de entități esențiale și importante, inclusiv de furnizori de infrastructură digitală care sprijină funcțiile de bază ale internetului deschis și asigură accesul la internet și serviciile de internet. Prin urmare, este important ca produsele cu elemente digitale necesare pentru ca furnizorii de infrastructură digitală să asigure funcționarea internetului să fie dezvoltate în mod securizat și să respecte standardele consacrate în materie de securitate a internetului.

Prezentul regulament, care se aplică tuturor produselor hardware și software conectabile, are ca scop, de asemenea, să faciliteze respectarea de către furnizorii de infrastructură digitală a cerințelor lanțului de aprovizionare în temeiul [Directiva XXX/XXXX (NIS2)], prin asigurarea faptului că produsele cu elemente digitale pe care le utilizează pentru furnizarea serviciilor lor sunt dezvoltate în mod securizat și că au acces la actualizări de securitate în timp util pentru aceste produse.

(12) Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului[7] stabilește norme privind dispozitivele medicale, iar Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului[8] stabilește norme privind dispozitivele medicale pentru diagnostic *in vitro*. Ambele regulamente vizează riscurile de securitate cibernetică și urmează abordări specifice care sunt vizate și în prezentul regulament. Mai precis, Regulamentele (UE) 2017/745 și (UE) 2017/746 stabilesc cerințe esențiale pentru dispozitivele medicale care funcționează printr-un sistem electronic sau care sunt ele însele software. Anumite tipuri de software neîncorporat și abordarea bazată pe întregul ciclu de viață sunt, de asemenea, vizate de regulamentele respective. Aceste cerințe le impun producătorilor să își dezvolte și să își construiască produsele aplicând principii de gestionare a riscurilor și stabilind cerințe privind măsurile de securitate informatică, precum și proceduri corespunzătoare de evaluare a conformității. În plus, din decembrie 2019 sunt în vigoare orientări specifice privind securitatea cibernetică a dispozitivelor medicale, care le oferă producătorilor de dispozitive medicale, inclusiv de dispozitive pentru diagnostic *in vitro*, orientări privind modul de îndeplinire a tuturor cerințelor esențiale relevante din anexa I la regulamentele respective în ceea ce privește securitatea cibernetică[9]. Prin urmare, produsele cu elemente digitale cărora li se aplică unul dintre aceste regulamente nu ar trebui să facă obiectul prezentului regulament.

(13) Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului[10] 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

---

7 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).

8 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).

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

10 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).

serviciilor în conformitate cu reglementările aplicabile ale Organizației Națiunilor Unite privind specificațiile tehnice și securitatea cibernetică[11] și prevăzând proceduri specifice de evaluare a conformității. În domeniul aviației, principalul obiectiv al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului[12] 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 țin seama de obligațiile de protecție împotriva amenințărilor la adresa securității informațiilor. Prin urmare, produsele cu elemente digitale cărora li se aplică Regulamentul (UE) 2019/2144 și produsele certificate în conformitate cu Regulamentul (UE) 2018/1139 nu fac obiectul cerințelor esențiale și al procedurilor de evaluare a conformității prevăzute în prezentul regulament. Procesul de certificare în temeiul Regulamentului (UE) 2018/1139 garantează nivelul de asigurare vizat de prezentul regulament.

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

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

---

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

[12] 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).

prevăzute de prezentul regulament sunt aliniate la obiectivele cerințelor pentru standardele specifice incluse în cererea de standardizare respectivă. Prin urmare, în cazul în care Comisia abrogă sau modifică Regulamentul delegat (UE) 2022/30, cu consecința că acesta încetează să se aplice în cazul anumitor produse care fac obiectul prezentului regulament, Comisia și organizațiile europene de standardizare ar trebui să ia în considerare activitatea de standardizare desfășurată în contextul Deciziei de punere în aplicare C(2022) 5637 a Comisiei privind o cerere de standardizare pentru Regulamentul delegat (UE) 2022/30 RED atunci când vor pregăti și elabora standarde armonizate pentru facilitarea punerii în aplicare a prezentului regulament.

(16) Directiva 85/374/CEE[13] este complementară prezentului regulament. Aceasta stabilește norme privind răspunderea pentru produsele cu defecte, pentru ca persoanele prejudiciate să poată solicita despăgubiri în cazul în care anumite produse cu defecte au provocat un prejudiciu. Directiva respectivă stabilește principiul conform căruia producătorul unui produs este răspunzător pentru prejudiciile provocate cauzate de lipsa de siguranță a produsului său, indiferent de culpă („răspundere obiectivă”). În cazul în care o astfel de lipsă de siguranță constă în lipsa actualizărilor de securitate după introducerea produsului pe piață, iar acest lucru provoacă prejudicii, ar putea fi angajată răspunderea producătorului. Prezentul regulament ar trebui să prevadă obligații pentru producători referitoare la furnizarea unor astfel de actualizări de securitate.

(17) Prezentul regulament nu ar trebui să aducă atingere Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[14], 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 trebuie, de asemenea, să contribuie la îmbunătățirea protecției datelor cu caracter personal și a vieții private a persoanelor. Ar trebui avute în vedere sinergii atât în ceea ce privește standardizarea, cât și certificarea cu privire la aspectele legate de securitatea cibernetică prin cooperarea dintre Comisie, organizațiile europene de standardizare, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), Comitetul european pentru protecția datelor (CEPD) instituit prin Regulamentul (UE) 2016/679 și autoritățile naționale de supraveghere a protecției datelor. De asemenea, ar trebui create sinergii între prezentul regulament și legislația Uniunii în materie de protecție a datelor în domeniul supravegherii pieței și al asigurării respectării legislației. În acest scop, autoritățile naționale de supraveghere a pieței desemnate în temeiul prezentului regulament ar trebui să coopereze cu autoritățile care supraveghează legislația

[13] Directiva 85/374/CEE Consiliului din 25 iulie 1985 de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre cu privire la răspunderea pentru produsele cu defect (JO L 210, 7.8.85).

[14] 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).

Uniunii în materie de protecție a datelor. De asemenea, acestea din urmă ar trebui să aibă acces la informațiile relevante pentru îndeplinirea sarcinilor lor.

(18) În măsura în care produsele lor intră în domeniul de aplicare al prezentului regulament, emitenții de portofele europene pentru identitatea digitală, astfel cum sunt menționate la articolul [articolul 6a alineatul (2) din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Propunerea de regulament de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană], ar trebui să respecte atât cerințele esențiale orizontale instituite prin prezentul regulament, cât și cerințele de securitate specifice prevăzute la articolul [articolul 6a din Regulamentul (UE) nr. 910/2014, astfel cum a fost modificat prin Propunerea de regulament de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea unui cadru pentru identitatea digitală europeană]. Pentru a facilita respectarea acestora, emitenții de portofele ar trebui să poată demonstra conformitatea portofelelor europene pentru identitatea digitală cu cerințele prevăzute în ambele acte prin certificarea produselor lor în cadrul unui sistem european de certificare de securitate cibernetică instituit în temeiul Regulamentului (UE) 2019/881 și pentru care Comisia a specificat, prin intermediul unui act de punere în aplicare, o prezumție de conformitate pentru prezentul regulament, în măsura în care certificatul sau anumite părți ale acestuia acoperă cerințele respective.

(19) Anumite sarcini prevăzute în prezentul regulament ar trebui să fie îndeplinite de ENISA, în conformitate cu articolul 3 alineatul (2) din Regulamentul (UE) 2019/881. În special, ENISA ar trebui să primească notificări de la producători cu privire la vulnerabilitățile exploatate activ conținute în produsele cu elemente digitale, precum și cu privire la incidentele care au un impact asupra securității acestor produse. ENISA ar trebui, de asemenea, să transmită aceste notificări echipelor de intervenție în caz de incidente de securitate informatică (CSIRT) relevante sau, respectiv, punctelor unice de contact relevante din statele membre desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și să informeze autoritățile relevante de supraveghere a pieței cu privire la vulnerabilitatea notificată. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită grupului de cooperare menționat în Directiva [Directiva XXX/XXXX (NIS2)]. În plus, având în vedere expertiza și mandatul său, ENISA ar trebui să fie în măsură să sprijine procesul de punere în aplicare a prezentului regulament. În special, aceasta ar trebui să fie în măsură să propună activități comune care să fie desfășurate de autoritățile de supraveghere a pieței pe baza unor indicații sau informații privind o posibilă neconformitate cu prezentul regulament a produselor cu elemente digitale din mai multe state membre sau să identifice categoriile de produse pentru care ar trebui organizate acțiuni de control coordonate simultane. În circumstanțe excepționale, la cererea Comisiei, ENISA ar trebui să poată efectua evaluări cu privire la anumite produse cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică, în cazul în care este necesară o intervenție imediată pentru a menține buna funcționare a pieței interne.

(20) Produsele cu elemente digitale ar trebui să poarte marcajul CE pentru a indica 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.

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

(22) Pentru a se asigura că produsele cu elemente digitale, atunci când sunt introduse pe piață, nu prezintă riscuri în materie de securitate cibernetică pentru persoane și organizații, ar trebui stabilite cerințe esențiale pentru astfel de produse. Atunci când produsele sunt modificate ulterior, prin mijloace fizice sau digitale, într-un mod care nu este prevăzut de producător și care poate implica faptul că acestea nu mai îndeplinesc cerințele esențiale relevante, modificarea ar trebui considerată substanțială. De exemplu, actualizările sau reparațiile software-ului ar putea fi asimilate operațiunilor de întreținere, cu condiția ca acestea să nu modifice un produs deja introdus pe piață astfel încât să poată fi afectată conformitatea cu cerințele aplicabile sau să poată fi schimbată utilizarea preconizată pentru care a fost evaluat produsul. La fel ca în cazul reparațiilor sau al modificărilor fizice, un produs cu elemente digitale ar trebui să fie considerat ca fiind modificat substanțial de o modificare a software-ului dacă actualizarea software-ului modifică tipul, performanța sau funcțiile inițiale preconizate ale produsului, iar aceste modificări nu au fost prevăzute în evaluarea inițială a riscurilor sau dacă natura pericolului s-a schimbat sau nivelul de risc a crescut ca urmare a actualizării software-ului.

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

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

(25) Produsele cu elemente digitale ar trebui considerate critice dacă impactul negativ al exploatării potențialelor vulnerabilități în materie de securitate cibernetică ale produsului poate fi grav din cauza, printre altele, a funcționalității legate de securitatea cibernetică sau a utilizării preconizate. În special, vulnerabilitățile produselor cu elemente digitale care au o funcționalitate legată de securitatea cibernetică, de exemplu elementele de securitate, pot conduce la o propagare a problemelor de

securitate în întregul lanț de aprovizionare. Gravitatea impactului unui incident de securitate cibernetică poate crește, de asemenea, atunci când se ia în considerare utilizarea preconizată a produsului, de exemplu într-un cadru industrial sau în contextul unei entități esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)] sau pentru îndeplinirea unor funcții critice sau sensibile, cum ar fi prelucrarea datelor cu caracter personal.

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

(27) Categoriile de produse critice cu elemente digitale menționate în anexa III la prezentul regulament ar trebui înțelese ca fiind produsele care au funcționalitatea de bază de tipul inclus în anexa III la prezentul regulament. De exemplu, anexa III la prezentul regulament enumeră produsele care sunt definite prin funcționalitatea lor de bază ca microprocesoare de uz general din clasa II. În consecință, utilizarea generală a microprocesoarelor face obiectul evaluării obligatorii de conformitate de către terți. Acest lucru nu este valabil pentru alte produse care nu sunt menționate în mod explicit în anexa III la prezentul regulament și care pot integra un microprocesor de uz general. Comisia ar trebui să adopte acte delegate [în termen de 12 luni de la intrarea în vigoare a prezentului regulament] pentru a preciza definițiile categoriilor de produse incluse în clasele I și II, astfel cum sunt prevăzute în anexa III.

(28) Prezentul regulament abordează riscurile de securitate cibernetică într-un mod specific. Cu toate acestea, produsele cu elemente digitale ar putea prezenta și alte riscuri în materie de siguranță, care să nu fie legate de securitatea cibernetică. Aceste riscuri ar trebui să fie reglementate în continuare de alte acte legislative relevante ale Uniunii privind produsele. În cazul în care nu este aplicabil niciun alt act din legislația de armonizare a Uniunii, acestea ar trebui să facă obiectul Regulamentului [Regulamentul privind siguranța generală a produselor]. 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 [Regulamentul privind siguranța generală a produselor], produselor cu elemente digitale ar trebui să li se aplice capitolul III secțiunea 1, capitolele V și VII și capitolele IX-XI din Regulamentul [Regulamentul privind siguranța generală a produselor] în ceea ce privește riscurile în materie de siguranță care nu sunt acoperite de prezentul regulament, dacă produsele respective nu fac obiectul unor cerințe specifice impuse de alte acte din legislația de armonizare a Uniunii în sensul [articolului 3 punctului 25 din Regulamentul privind siguranța generală a produselor].

(29) Produsele cu elemente digitale clasificate ca sisteme de IA cu grad ridicat de risc în conformitate cu articolul 6 din Regulamentul[15] [Regulamentul privind inteligența artificială] care intră în domeniul de aplicare al prezentului regulament ar trebui să respecte cerințele esențiale prevăzute în prezentul regulament. Atunci când aceste

[15] Regulamentul [Regulamentul privind inteligența artificială].

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

(30) Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului [Propunerea de regulament privind produsele asimilate mașinilor] și care sunt produse cu elemente digitale în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate pe baza prezentului regulament ar trebui considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul [Propunerea de regulament privind produsele asimilate mașinilor] în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control, în măsura în care conformitatea cu cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.

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

(32) Pentru a se asigura faptul că produsele cu elemente digitale sunt sigure atât în momentul introducerii lor pe piață, cât și pe parcursul întregului lor ciclu de viață, este necesar să se stabilească cerințe esențiale pentru gestionarea vulnerabilităților și cerințe esențiale de securitate cibernetică legate de proprietățile produselor cu elemente digitale. Deși producătorii ar trebui să respecte toate cerințele esențiale legate de gestionarea vulnerabilităților și să se asigure că toate produsele lor sunt livrate fără nicio vulnerabilitate exploatabilă cunoscută, aceștia ar trebui să stabilească celelalte cerințe esențiale legate de proprietățile produsului care sunt relevante pentru tipul de produs în cauză. În acest scop, producătorii ar trebui să efectueze o evaluare a riscurilor de securitate cibernetică asociate unui produs cu elemente digitale pentru a identifica riscurile relevante și cerințele esențiale relevante și pentru a aplica în mod corespunzător standarde armonizate sau specificații comune adecvate.

(33) Pentru a îmbunătăți securitatea produselor cu elemente digitale introduse pe piața internă, este necesar să se stabilească cerințe esențiale. Aceste cerințe esențiale nu ar trebui să aducă atingere evaluărilor coordonate la nivelul UE ale riscurilor pentru lanțurile de aprovizionare critice instituite prin [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)][16], care iau în considerare atât factori de risc tehnici, cât și, după caz, factori de risc netehnici, cum ar fi influența nejustificată a unei țări terțe asupra furnizorilor. În plus, nu ar trebui să se aducă atingere prerogativelor statelor membre de a stabili cerințe suplimentare care să țină seama de factori netehnici în scopul asigurării unui nivel ridicat de reziliență, inclusiv de cei definiți în Recomandarea (UE) 2019/534, în evaluarea coordonată la nivelul Uniunii a riscurilor legate de securitatea rețelelor 5G și în setul de instrumente al UE privind securitatea cibernetică a rețelelor 5G convenit de Grupul de cooperare NIS, astfel cum se menționează în [Directiva XXX/XXXX (NIS2)].

(34) Pentru a se asigura că echipele CSIRT naționale și punctele unice de contact desemnate în conformitate cu articolul [articolul X] din Directiva [Directiva XX/XXXX (NIS2)] primesc informațiile necesare pentru îndeplinirea sarcinilor lor și pentru creșterea nivelului general de securitate cibernetică a entităților esențiale și importante, precum și pentru a asigura funcționarea eficace a autorităților de supraveghere a pieței, producătorii de produse cu elemente digitale ar trebui să informeze ENISA cu privire la vulnerabilitățile care sunt exploatate activ. Întrucât majoritatea produselor cu elemente digitale sunt comercializate pe întreaga piață internă, orice vulnerabilitate exploatată a unui produs cu elemente digitale ar trebui considerată o amenințare la adresa funcționării pieței interne. De asemenea, producătorii ar trebui să ia în considerare divulgarea vulnerabilităților remediate în baza de date europeană privind vulnerabilitățile instituită în temeiul Directivei [Directiva XX/XXXX (NIS2)] și gestionată de ENISA sau în orice altă bază de date privind vulnerabilitățile accesibilă publicului.

(35) Producătorii ar trebui, de asemenea, să raporteze către ENISA orice incident care are un impact asupra securității produsului cu elemente digitale. Fără a aduce atingere obligațiilor de raportare a incidentelor prevăzute în Directiva [Directiva XXX/XXXX (NIS2)] pentru entitățile esențiale și importante, este esențial ca ENISA, punctele unice de contact desemnate de statele membre în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] și autoritățile de

[16] Directiva XXX a Parlamentului European și a Consiliului din [data] [privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148 (JO L xx, data, p. x)].

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

(36) Producătorii de produse cu elemente digitale ar trebui să instituie politici coordonate de divulgare a vulnerabilităților pentru a facilita raportarea vulnerabilităților de către persoane fizice sau entități. O politică coordonată de divulgare a vulnerabilităților ar trebui să precizeze un proces structurat prin care vulnerabilitățile să fie raportate producătorului într-un mod care să îi permită acestuia să diagnosticheze și să remedieze vulnerabilitățile respective înainte ca informațiile detaliate referitoare la acestea să fie divulgate terților sau publicului. Având în vedere faptul că informațiile privind vulnerabilitățile exploatabile ale produselor cu elemente digitale care sunt utilizate pe scară largă pot fi vândute la prețuri ridicate pe piața neagră, producătorii de astfel de produse ar trebui să poată utiliza, ca parte a politicilor lor coordonate de divulgare a vulnerabilităților, programe prin care să stimuleze raportarea vulnerabilităților, asigurându-se că persoanele sau entitățile primesc recunoaștere și compensații pentru eforturile lor (așa-numitele „programe de stimulare a identificării bug-urilor”).

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

(38) Pentru a facilita evaluarea conformității cu cerințele prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu standardele armonizate, care transpun cerințele esențiale ale prezentului regulament în specificații tehnice detaliate și care sunt adoptate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului[17]. Regulamentul (UE) nr. 1025/2012 prevede o procedură pentru formularea de obiecții cu privire la standardele armonizate în cazul în care standardele respective nu îndeplinesc în totalitate cerințele prezentului regulament.

(39) Regulamentul (UE) 2019/881 stabilește un cadru european voluntar de certificare de securitate cibernetică pentru produsele, procesele și serviciile TIC. Sistemele europene

[17] 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).

de certificare de securitate cibernetică pot include produse cu elemente digitale care fac obiectul prezentului regulament. Prezentul regulament ar trebui 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 de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 și care au fost identificate de Comisie într-un act de punere în aplicare sunt considerate a fi conforme cu cerințele esențiale ale prezentului regulament în măsura în care certificatul de securitate cibernetică sau declarația de conformitate ori anumite părți ale acestora acoperă cerințele respective. În lumina prezentului regulament ar trebui evaluată necesitatea unor noi sisteme europene de certificare de securitate cibernetică pentru produsele cu elemente digitale. Astfel de sisteme europene viitoare de certificare de securitate cibernetică care vor acoperi produsele cu elemente digitale ar trebui să țină seama de cerințele esențiale prevăzute în prezentul regulament și să faciliteze respectarea prezentului regulament. Comisia ar trebui să fie împuternicită să precizeze, prin intermediul unor acte de punere în aplicare, sistemele europene de certificare de securitate cibernetică care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale prevăzute în prezentul regulament. În plus, pentru a evita o sarcină administrativă nejustificată pentru producători, după caz, Comisia ar trebui să precizeze dacă un certificat de securitate cibernetică emis în cadrul unor astfel de sisteme europene de certificare de securitate cibernetică elimină obligația producătorilor de a efectua o evaluare a conformității de către terți, astfel cum se prevede în prezentul regulament pentru cerințele corespunzătoare.

(40) La intrarea în vigoare a actului de punere în aplicare prin care se stabilește [Regulamentul de punere în aplicare (UE) nr. .../... al Comisiei din XXX privind sistemul european de certificare de securitate cibernetică bazat pe criterii comune] (EUCC) care se referă la produsele hardware care fac obiectul prezentului regulament, cum ar fi modulele de securitate hardware și microprocesoarele, Comisia poate preciza, prin intermediul unui act de punere în aplicare, modul în care EUCC oferă o prezumție de conformitate cu cerințele esențiale menționate în anexa I la prezentul regulament sau cu anumite părți ale acestora. În plus, un astfel de act de punere în aplicare poate preciza modul în care un certificat emis în temeiul EUCC elimină obligația producătorilor de a efectua o evaluare de către terți, solicitată de prezentul regulament pentru cerințele corespunzătoare.

(41) În cazul în care nu se adoptă standarde armonizate sau în cazul în care standardele armonizate nu abordează suficient cerințele esențiale ale prezentului regulament, Comisia ar trebui să poată adopta specificații comune prin intermediul unor acte de punere în aplicare. Câteva motive pentru elaborarea unor astfel de specificații comune, în locul utilizării standardelor armonizate, ar putea fi refuzarea cererii de standardizare de către una dintre organizațiile europene de standardizare, întârzieri nejustificate în stabilirea standardelor armonizate adecvate sau nerespectarea de către standardele elaborate a cerințelor prezentului regulament sau a unei cereri din partea Comisiei. Pentru a facilita evaluarea conformității cu cerințele esențiale prevăzute în prezentul regulament, ar trebui să existe o prezumție de conformitate pentru produsele cu elemente digitale care sunt conforme cu specificațiile comune adoptate de Comisie în temeiul prezentului regulament în scopul exprimării specificațiilor tehnice detaliate ale cerințelor respective.

(42) Producătorii ar trebui să elaboreze o declarație de conformitate UE pentru a oferi informațiile necesare în temeiul prezentului regulament cu privire la conformitatea

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

(43) Marcajul CE, ca indicație a conformității unui produs, este consecința vizibilă a unui întreg proces care cuprinde evaluarea conformității în sens larg. Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului[18] 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 prezentului regulament.

(44) Pentru a permite operatorilor economici să demonstreze conformitatea cu cerințele esențiale prevăzute în prezentul regulament și pentru a permite autorităților de supraveghere a pieței să se asigure că produsele cu elemente digitale puse la dispoziție pe piață respectă aceste cerințe, este necesar să se prevadă proceduri de evaluare a conformității. Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului[19] stabilește module pentru procedurile de evaluare a conformității proporțional cu nivelul de risc implicat și cu nivelul de securitate necesar. Pentru a asigura coerența intersectorială și pentru a evita variantele ad-hoc, procedurile de evaluare a conformității adecvate pentru verificarea conformității produselor cu elemente digitale cu cerințele esențiale prevăzute în prezentul regulament s-au bazat pe modulele respective. Procedurile de evaluare a conformității ar trebui să examineze și să verifice atât cerințele referitoare la produse, cât și pe cele referitoare la procese care acoperă întregul ciclu de viață al produselor cu elemente digitale, inclusiv planificarea, proiectarea, dezvoltarea sau producția, testarea și întreținerea produsului.

(45) Ca regulă generală, evaluarea conformității produselor cu elemente digitale ar trebui să fie efectuată de producător pe propria răspundere, urmând procedura bazată pe modulul A din Decizia nr. 768/2008/CE. Producătorul ar trebui să păstreze flexibilitatea de a alege o procedură mai strictă de evaluare a conformității care să implice o parte terță. În cazul în care produsul este clasificat ca produs critic din clasa I, este necesară o asigurare suplimentară pentru a demonstra conformitatea cu cerințele esențiale prevăzute în prezentul regulament. Producătorul ar trebui să aplice standardele armonizate, specificațiile comune sau sistemele de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 care au fost identificate de Comisie într-un act de punere în aplicare, dacă dorește să efectueze evaluarea conformității pe propria răspundere (modulul A). În cazul în care nu aplică astfel de standarde armonizate, specificații comune sau sisteme de certificare de securitate

---

[18] 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).

[19] 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).

cibernetică, producătorul ar trebui să fie supus unei evaluări a conformității care implică o parte terță. Ținând seama de sarcina administrativă a producătorilor și de faptul că securitatea cibernetică joacă un rol important în etapa de proiectare și dezvoltare a produselor cu elemente digitale, fizice sau nu, procedurile de evaluare a conformității bazate pe modulele B+C sau, respectiv, pe modulul H din Decizia nr. 768/2008/CE au fost alese ca fiind cele mai adecvate pentru evaluarea conformității produselor critice cu elemente digitale în mod proporțional și eficace. Producătorul care efectuează evaluarea conformității de către terți poate alege procedura care se potrivește cel mai bine procesului său de proiectare și de producție. Având în vedere riscul și mai mare de securitate cibernetică legat de utilizarea produselor clasificate ca produse critice din clasa II, evaluarea conformității ar trebui să implice întotdeauna o parte terță.

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

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

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

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

(50) Organismele de evaluare a conformității subcontractează deseori părți ale activităților lor legate de evaluarea conformității sau recurg la o filială. În vederea asigurării nivelului de protecție cerut pentru produsele cu elemente digitale care urmează să fie

introduse pe piață, este esențial ca subcontractanții și filialele care efectuează procedura de evaluare a conformității să îndeplinească aceleași cerințe ca organismele notificate în ceea ce privește executarea atribuțiilor de evaluare a conformității.

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

(52) Întrucât organismele notificate își pot oferi serviciile în întreaga Uniune, este adecvat să se acorde celorlalte state membre și Comisiei posibilitatea de a ridica obiecții cu privire la un organism notificat. De aceea este important să se acorde o perioadă de timp în care orice îndoieli sau preocupări privind competența organismelor de evaluare a conformității să poată fi clarificate, înainte ca acestea să înceapă să funcționeze ca organisme notificate.

(53) Din rațiuni de competitivitate, este fundamental ca organismele notificate să aplice procedurile de evaluare a conformității fără a crea o sarcină inutilă pentru operatorii economici. Din același motiv și pentru a asigura tratamentul egal al operatorilor economici, este necesară asigurarea coerenței în aplicarea tehnică a procedurilor de evaluare a conformității. Acest lucru ar trebui realizat cel mai bine printr-o coordonare și o cooperare adecvată între organismele notificate.

(54) Supravegherea pieței este un instrument esențial, deoarece asigură aplicarea corespunzătoare și uniformă a legislației Uniunii. Prin urmare, este necesară instituirea unui cadru juridic în care supravegherea pieței să poată fi realizată în mod adecvat. Normele privind supravegherea pieței Uniunii și controlul produselor care intră pe piața Uniunii prevăzute în Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului[20] se aplică produselor cu elemente digitale care fac obiectul prezentului regulament.

(55) În conformitate cu Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței efectuează supravegherea pieței pe teritoriul statului membru respectiv. Prezentul regulament nu ar trebui să împiedice statele membre să aleagă autoritățile competente pentru îndeplinirea sarcinilor respective. Fiecare stat membru ar trebui să desemneze una sau mai multe autorități de supraveghere a pieței pe teritoriul său. Statele membre pot alege să desemneze orice autoritate existentă sau nouă care să acționeze în calitate de autoritate de supraveghere a pieței, inclusiv autoritățile naționale competente menționate la articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] sau autoritățile naționale desemnate de certificare a securității cibernetice menționate la articolul 58 din Regulamentul (UE) 2019/881. Operatorii economici ar trebui să coopereze pe deplin cu autoritățile de supraveghere a pieței și cu alte autorități competente. Fiecare stat membru ar trebui să informeze Comisia și celelalte state membre cu privire la autoritățile sale de supraveghere a pieței și la domeniile de competență ale fiecăreia dintre aceste autorități și ar trebui să asigure resursele și competențele necesare pentru îndeplinirea sarcinilor de supraveghere legate de prezentul regulament. În conformitate cu articolul 10 alineatele (2) și (3) din

[20] 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).

Regulamentul (UE) 2019/1020, fiecare stat membru ar trebui să numească un birou unic de legătură care ar trebui să fie responsabil, printre altele, de reprezentarea poziției coordonate a autorităților de supraveghere a pieței și de acordarea de asistență pentru cooperarea dintre autoritățile de supraveghere a pieței din diferite state membre.

(56) Ar trebui instituit un grup specific de cooperare administrativă (ADCO) pentru aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO ar trebui să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate și, dacă este cazul, din reprezentanți ai birourilor unice de legătură. Comisia ar trebui să sprijine și să încurajeze cooperarea dintre autoritățile de supraveghere a pieței prin intermediul Rețelei Uniunii pentru conformitatea produselor, instituită în temeiul articolului 29 din Regulamentul (UE) 2019/1020 și alcătuită din reprezentanți ai fiecărui stat membru, inclusiv un reprezentant al fiecărui birou unic de legătură menționat la articolul 10 din Regulamentul (UE) 2019/1020 și un expert național opțional, președinții ADCO și reprezentanți ai Comisiei. Comisia ar trebui să participe la reuniunile rețelei, ale subgrupurilor sale și ale ADCO respectiv. Aceasta ar trebui, de asemenea, să asiste ADCO prin intermediul unui secretariat executiv care să ofere sprijin tehnic și logistic.

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

(58) În anumite cazuri, un produs cu elemente digitale care respectă prezentul regulament poate prezenta totuși un risc semnificativ în materie de securitate cibernetică sau poate prezenta un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, în ceea ce privește disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin utilizarea unui sistem electronic de informații de către entitățile esențiale de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)] sau în ceea ce privește alte aspecte ale protecției interesului public. Prin urmare, este necesar să se stabilească norme care să asigure atenuarea acestor riscuri. În consecință, autoritățile de supraveghere a pieței ar trebui să ia măsuri pentru a solicita operatorului economic să se asigure că produsul nu mai prezintă riscul respectiv, să îl recheme sau să îl retragă, în funcție de risc. De îndată ce o autoritate de supraveghere a pieței restricționează sau interzice libera circulație a unui produs în acest mod, statul membru în cauză ar trebui să informeze fără întârziere Comisia și celelalte state membre cu privire la măsurile provizorii, justificându-și și motivându-și decizia. Atunci când o autoritate de supraveghere a pieței adoptă astfel de măsuri în ceea ce privește produsele care prezintă un risc, Comisia ar trebui să inițieze fără întârziere consultări cu statele membre și cu operatorul economic sau operatorii economici în cauză și ar trebui să evalueze măsura națională. Pe baza rezultatelor acestei evaluări, Comisia ar trebui să decidă dacă măsura națională este sau nu justificată. Comisia ar trebui să adreseze decizia sa tuturor statelor membre și să o comunice imediat acestora și operatorului (operatorilor) economic(i) în cauză. Dacă

măsura este considerată justificată, Comisia poate avea în vedere, de asemenea, adoptarea unor propuneri de revizuire a legislației respective a Uniunii.

(59) În cazul produselor cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică și dacă există motive să se creadă că acestea nu sunt conforme cu prezentul regulament sau în cazul produselor care sunt conforme cu prezentul regulament, dar care prezintă alte riscuri importante, precum riscuri la adresa sănătății sau siguranței persoanelor, a drepturilor fundamentale sau a furnizării de servicii de către entități esențiale de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)], Comisia poate solicita ENISA să efectueze o evaluare. Pe baza evaluării respective, Comisia poate adopta, prin intermediul unor acte de punere în aplicare, măsuri corective sau restrictive la nivelul Uniunii, inclusiv dispunerea retragerii de pe piață sau rechemarea produselor respective, într-un termen rezonabil, proporțional cu natura riscului. Comisia poate recurge la o astfel de intervenție numai în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne și numai în cazul în care autoritățile de supraveghere nu au luat măsuri eficace pentru remedierea situației. Astfel de circumstanțe excepționale pot fi situații de urgență în care, de exemplu, un produs neconform este pus la dispoziție pe scară largă de către producător în mai multe state membre, este utilizat și în sectoare-cheie de către entități care intră în domeniul de aplicare al [Directivei XXX/XXXX (NIS2)], acesta conținând vulnerabilități cunoscute care sunt exploatate de actori rău-intenționați și pentru care producătorul nu oferă corecții disponibile. Comisia poate interveni în astfel de situații de urgență numai pe durata circumstanțelor excepționale și dacă neconformitatea cu prezentul regulament sau riscurile importante prezentate persistă.

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

(61) Acțiunile de control coordonate simultane („acțiuni de verificare”) sunt acțiuni specifice de asigurare a respectării legislației întreprinse de autoritățile de supraveghere a pieței care pot spori și mai mult securitatea produselor. În special, ar trebui efectuate acțiuni de verificare atunci când tendințele pieței, reclamațiile consumatorilor sau alte indicii sugerează că anumite categorii de produse sunt adesea considerate ca prezentând riscuri de securitate cibernetică. ENISA ar trebui să prezinte autorităților de supraveghere a pieței propuneri de categorii de produse pentru care ar putea fi organizate acțiuni de verificare, bazate, printre altele, pe notificările pe care le primește cu privire la vulnerabilități ale produselor și la incidente.

(62) Pentru a se asigura că cadrul de reglementare poate fi adaptat atunci când este necesar, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul 290 din tratat pentru a actualiza lista produselor critice din anexa III și pentru a preciza definițiile acestor categorii de produse. Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv pentru a identifica produsele cu elemente digitale care fac obiectul altor norme ale Uniunii care asigură același nivel de protecție ca prezentul regulament, specificând dacă va fi necesară o limitare sau o excludere din domeniul de aplicare al prezentului regulament, precum și domeniul de aplicare al limitării respective, dacă este cazul. De asemenea, Comisiei ar trebui să îi fie delegată competența de a adopta acte în conformitate cu articolul respectiv în ceea ce privește eventuala impunere a certificării anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor referitoare la caracterul critic

prevăzute în prezentul regulament, precum și în ceea ce privește precizarea conținutului minim al declarației de conformitate UE și completarea elementelor care trebuie incluse în documentația tehnică. Este deosebit de important ca, în cursul activității sale pregătitoare, Comisia să organizeze consultări corespunzătoare, inclusiv la nivel de experți, și ca aceste consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional privind o mai bună legiferare din 13 aprilie 2016[21]. 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.

(63) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, Comisiei ar trebui să îi fie conferite competențe de executare: pentru a preciza formatul și elementele listei materialelor software, pentru a preciza mai detaliat tipul de informații, formatul și procedura notificărilor privind vulnerabilitățile exploatate activ și incidentele transmise către ENISA de către producători, pentru a preciza sistemele europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu anumite părți ale acestora, astfel cum sunt prevăzute în anexa I la prezentul regulament, pentru a adopta specificații comune cu privire la cerințele esențiale prevăzute în anexa I, pentru a stabili specificații tehnice pentru pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale și mecanisme de promovare a utilizării acestora, pentru a decide măsuri corective sau restrictive la nivelul Uniunii în circumstanțe excepționale care justifică o intervenție imediată pentru menținerea bunei funcționări a pieței interne. Aceste competențe ar trebui exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului[22].

(64) Pentru a asigura o cooperare bazată pe încredere și constructivă a autorităților de supraveghere a pieței de la nivelul Uniunii și de la nivel național, toate părțile implicate în aplicarea prezentului regulament ar trebui să respecte confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor lor.

(65) Pentru a asigura respectarea efectivă a obligațiilor prevăzute în prezentul regulament, fiecare autoritate de supraveghere a pieței ar trebui să aibă competența de a impune sau de a solicita impunerea de amenzi administrative. Prin urmare, ar trebui stabilite niveluri maxime ale amenzilor administrative, care să fie prevăzute în legislația națională, pentru nerespectarea obligațiilor prevăzute în prezentul regulament. Atunci când se decide cuantumul amenzii administrative în fiecare caz în parte, ar trebui să se țină seama de toate circumstanțele relevante ale situației specifice și, cel puțin, de cele stabilite în mod explicit în prezentul regulament, inclusiv de posibilitatea ca alte autorități de supraveghere a pieței să fi aplicat deja amenzi administrative aceluiași operator pentru încălcări similare. Aceste circumstanțe pot fi fie agravante, în situațiile în care încălcarea săvârșită de același operator persistă pe teritoriul altor state membre decât cel în care s-a aplicat deja o amendă administrativă, fie atenuante, pentru a se asigura că orice altă amendă administrativă avută în vedere de o altă autoritate de supraveghere a pieței pentru același operator economic sau pentru același tip de

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

[22] 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).

încălcare ia deja în considerare, împreună cu alte circumstanțe specifice relevante, o sancțiune impusă într-un alt stat membru și cuantumul acesteia. În toate aceste cazuri, amenda administrativă cumulată care ar putea fi aplicată de autoritățile de supraveghere a pieței din mai multe state membre aceluiași operator economic pentru același tip de încălcare ar trebui să asigure respectarea principiului proporționalității.

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

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

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

(69) Operatorilor economici ar trebui să li se acorde suficient timp pentru a se adapta la cerințele prevăzute de prezentul regulament. Prezentul regulament ar trebui să se aplice la [24 de luni] de la intrarea sa în vigoare, cu excepția obligațiilor de raportare privind vulnerabilitățile exploatate activ și incidentele, care ar trebui să se aplice la [12 luni] de la intrarea în vigoare a regulamentului.

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

(71) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului[23] și a emis un aviz la […],

ADOPTĂ PREZENTUL REGULAMENT:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect

Prezentul regulament stabilește:

(a) norme pentru introducerea pe piață a produselor cu elemente digitale în vederea asigurării securității cibernetice a acestor produse;

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

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

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

Articolul 2

Domeniul de aplicare

1. Prezentul regulament se aplică produselor cu elemente digitale a căror utilizare preconizată sau previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv sau la o rețea.

2. Prezentul regulament nu se aplică produselor cu elemente digitale cărora li se aplică următoarele acte 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.

[23] 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).

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

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

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

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

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

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(24) „scop preconizat” înseamnă utilizarea care a fost preconizată de către producător a unui produs cu elemente digitale, inclusiv contextul și condițiile specifice de

utilizare, astfel cum se specifică în informațiile oferite de furnizor în instrucțiunile de utilizare, în materialele și în declarațiile promoționale sau de vânzare, precum și în documentația tehnică;

(25) „utilizare previzibilă în mod rezonabil” înseamnă o utilizare care nu este neapărat scopul preconizat specificat de producător în instrucțiunile de utilizare, în materialele și în declarațiile promoționale sau de vânzare, precum și în documentația tehnică, dar care este probabil să rezulte din comportamentul uman sau din operațiuni tehnice sau interacțiuni previzibile în mod rezonabil;

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

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

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

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

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

(31) „modificare substanțială” înseamnă o modificare a produsului cu elemente digitale în urma introducerii sale pe piață care afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 sau care are ca rezultat o modificare a utilizării preconizate pentru care a fost evaluat respectivul produs cu elemente digitale;

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

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

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

(35) „risc de securitate cibernetică” înseamnă un risc astfel cum este definit la articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)];

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

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

(38) „vulnerabilitate” înseamnă o vulnerabilitate astfel cum este definită la articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)];

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

(40) „date cu caracter personal” înseamnă datele definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679.

Articolul 4

Libera circulație

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

2. La târguri comerciale, expoziții și demonstrații sau evenimente similare, statele membre nu împiedică prezentarea și utilizarea unui produs cu elemente digitale care nu este conform cu prezentul regulament.

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

Articolul 5

Cerințe pentru produsele cu elemente digitale

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

(1) îndeplinesc cerințele esențiale prevăzute în anexa I secțiunea 1, cu condiția să fie instalate, întreținute, utilizate în mod corespunzător pentru scopul preconizat sau în condiții care pot fi prevăzute în mod rezonabil și, după caz, actualizate și

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

Articolul 6

Produsele critice cu elemente digitale

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

2. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a modifica anexa III prin includerea în lista categoriilor de produse critice cu

elemente digitale a unei noi categorii sau prin retragerea unei categorii existente din lista respectivă. Atunci când evaluează necesitatea de a modifica lista din anexa III, Comisia ține seama de nivelul de risc de securitate cibernetică aferent respectivei categoriei de produse cu elemente digitale. La determinarea nivelului riscului de securitate cibernetică, se ține seama de unul sau mai multe dintre următoarele criterii:

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

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

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

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

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

(b) utilizarea preconizată în medii sensibile, inclusiv în medii industriale sau de către entități esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)];

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

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

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

3. Comisia este împuternicită să adopte un act delegat în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea definițiilor categoriilor de produse din clasa I și clasa II, astfel cum sunt prevăzute în anexa III. Actul delegat respectiv trebuie să fie adoptat până la [12 luni de la intrarea în vigoare a prezentului regulament].

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

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin specificarea categoriilor de produse deosebit de critice cu elemente digitale, pentru care producătorii au obligația de a obține un certificat european de securitate cibernetică în cadrul unui sistem european de certificare de securitate cibernetică în temeiul Regulamentului (UE) 2019/881 pentru a demonstra conformitatea cu cerințele esențiale prevăzute în anexa I sau cu anumite părți ale acestora. Atunci când stabilește aceste categorii de produse deosebit de critice cu elemente digitale, Comisia ține seama de nivelul de risc de securitate cibernetică aferent categoriei respective de produse cu elemente digitale, având în vedere unul sau mai multe dintre criteriile enumerate la alineatul (2), precum și evaluând dacă respectiva categorie de produse:

(a) este utilizată sau dacă se bazează pe ea entitățile esențiale de tipul celor menționate în anexa [anexa I] la Directiva [Directiva XXX/XXXX (NIS2)] sau dacă aceasta va avea o potențială semnificație viitoare pentru activitățile entităților respective; sau

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

Articolul 7

Siguranța generală a produselor

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

Articolul 8

Sistemele de IA cu grad ridicat de risc

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

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

3. Prin derogare de la alineatul (2), produsele critice cu elemente digitale enumerate în anexa III la prezentul regulament, care trebuie să aplice procedurile de evaluare a conformității menționate la articolul 24 alineatul (2) litera (a), la articolul 24

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

Articolul 9

Produsele asimilate mașinilor

Produsele asimilate mașinilor care intră în domeniul de aplicare al Regulamentului [Propunerea de regulament privind produsele asimilate mașinilor] care sunt produse cu elemente digitale în sensul prezentului regulament și pentru care a fost emisă o declarație de conformitate UE pe baza prezentului regulament sunt considerate ca fiind conforme cu cerințele esențiale privind sănătatea și siguranța prevăzute în anexa [anexa III secțiunile 1.1.9 și 1.2.1] la Regulamentul [Propunerea de regulament privind produsele asimilate mașinilor] în ceea ce privește protecția împotriva corupției și siguranța și fiabilitatea sistemelor de control și în măsura în care atingerea nivelului de protecție impus de cerințele respective este demonstrată de declarația de conformitate UE emisă în temeiul prezentului regulament.

CAPITOLUL II

OBLIGAȚIILE OPERATORILOR ECONOMICI

Articolul 10

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 prevăzute în anexa I secțiunea 1.

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

3. Atunci când introduce pe piață un produs cu elemente digitale, producătorul include o evaluare a riscurilor de securitate cibernetică în documentația tehnică prevăzută la articolul 23 și în anexa V. În cazul produselor cu elemente digitale menționate la articolul 8 și la articolul 24 alineatul (4) care fac, de asemenea, obiectul altor acte ale Uniunii, evaluarea riscurilor de securitate cibernetică poate face parte din evaluarea riscurilor impusă de respectivele acte ale Uniunii. În cazul în care anumite cerințe esențiale nu sunt aplicabile produsului cu elemente digitale comercializat, producătorul include o justificare clară în documentația respectivă.

4. În scopul respectării obligației prevăzute la alineatul (1), producătorii exercită diligența necesară atunci când integrează în produsele cu elemente digitale componente obținute de la terți. Aceștia se asigură că respectivele componente nu compromit securitatea produsului cu elemente digitale.

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

6. Atunci când introduc pe piață un produs cu elemente digitale și pe durata de viață preconizată a produsului sau pentru o perioadă de cinci ani de la introducerea produsului pe piață, oricare dintre acestea este mai scurtă, producătorii se asigură că vulnerabilitățile produsului respectiv sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I secțiunea 2.

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

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

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

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

8. Producătorii păstrează documentația tehnică și declarația de conformitate UE, dacă este cazul, la dispoziția autorităților de supraveghere a pieței timp de zece ani de la introducerea pe piață a produsului cu elemente digitale.

9. Producătorii se asigură că există proceduri care să garanteze conformitatea continuă a produselor cu elemente digitale care fac parte dintr-o producție în serie. Producătorul ține seama în mod adecvat de modificările survenite în procesul de dezvoltare și de producție sau în proiectarea ori caracteristicile produsului cu elemente digitale și de modificările standardelor armonizate, ale sistemelor europene de certificare de securitate cibernetică sau ale specificațiilor comune menționate la articolul 19 în raport cu care se declară conformitatea produsului cu elemente digitale sau prin aplicarea cărora este verificată conformitatea acestuia.

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

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

12. De la introducerea pe piață și pentru durata de viață preconizată a produsului sau pentru o perioadă de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai scurtă, producătorii care știu sau au motive să creadă că produsul cu elemente digitale sau procesele instituite de producător nu sunt conforme cu cerințele esențiale prevăzute în anexa I iau imediat măsurile corective necesare pentru a asigura conformitatea produsului cu elemente digitale sau a proceselor producătorului, pentru a retrage sau a rechema produsul, după caz.

13. În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, producătorii furnizează autorității respective, într-o limbă care poate fi ușor înțeleasă de către aceasta, toate informațiile și documentația, pe suport de hârtie sau în format electronic, necesare pentru a demonstra conformitatea produsului cu elemente digitale și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I. Aceștia cooperează cu autoritatea respectivă, la cererea acesteia, cu privire la adoptarea oricăror măsuri pentru eliminarea riscurilor de securitate cibernetică prezentate de produsul cu elemente digitale pe care l-au introdus pe piață.

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

15. Comisia poate specifica, prin intermediul unor acte de punere în aplicare, formatul și elementele listei materialelor software prevăzută în anexa I secțiunea 2 punctul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Articolul 11

Obligațiile de raportare ale producătorilor

1. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la momentul la care a luat cunoștință de aceasta, cu privire la orice vulnerabilitate exploatată activ conținută în produsul cu elemente digitale. Notificarea include detalii privind vulnerabilitatea respectivă și, după caz, eventualele măsuri corective sau de atenuare adoptate. ENISA transmite notificarea, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, către CSIRT desemnată în scopul divulgării coordonate a vulnerabilităților în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre în cauză la primirea notificării și informează autoritatea de supraveghere a pieței cu privire la vulnerabilitatea notificată.

2. Producătorul notifică ENISA, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la momentul la care a luat cunoștință de acesta, orice incident care afectează securitatea produsului cu elemente digitale. ENISA transmite notificările, fără întârzieri nejustificate, cu excepția cazului în care există motive întemeiate legate de riscurile de securitate cibernetică, punctului unic de contact desemnat în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)]

din statele membre în cauză și informează autoritatea de supraveghere a pieței cu privire la incidentele notificate. Notificarea incidentului include informații privind gravitatea și impactul incidentului și, după caz, indică dacă producătorul suspectează că incidentul este cauzat de acte ilegale sau rău-intenționate sau consideră că acesta are un impact transfrontalier.

3. ENISA transmite Rețelei europene a organizațiilor de legătură în materie de crize cibernetice (EU-CyCLONe) instituită prin articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] informațiile notificate în temeiul alineatelor (1) și (2) dacă aceste informații sunt relevante pentru gestionarea coordonată la nivel operațional a incidentelor și crizelor de securitate cibernetică de mare amploare.

4. Producătorul informează, fără întârzieri nejustificate și după ce a luat cunoștință de acesta, utilizatorii produsului cu elemente digitale cu privire la incident și, dacă este necesar, cu privire la măsurile corective pe care utilizatorul le poate aplica pentru a atenua impactul incidentului.

5. Comisia poate, prin intermediul unor acte de punere în aplicare, să precizeze mai detaliat tipul de informații care trebuie notificate, formatul notificărilor și procedura de efectuare a notificărilor transmise în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

6. Pe baza notificărilor primite în temeiul alineatelor (1) și (2), ENISA pregătește un raport tehnic bienal referitor la tendințele emergente în ceea ce privește riscurile de securitate cibernetică ale produselor cu elemente digitale și îl transmite grupului de cooperare menționat la articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)]. Primul raport de acest tip se prezintă în termen de 24 de luni de la data la care încep să se aplice obligațiile prevăzute la alineatele (1) și (2).

7. Atunci când identifică o vulnerabilitate a unei componente, inclusiv a unei componente cu sursă deschisă, care este integrată în produsul cu elemente digitale, producătorii raportează vulnerabilitatea persoanei sau entității care întreține componenta respectivă.

Articolul 12

Reprezentanți autorizați

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

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

3. Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la producător. Mandatul permite reprezentantului autorizat să îndeplinească cel puțin următoarele:

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

   (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 13

Obligațiile importatorilor

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

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

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

   (b) producătorul a întocmit documentația tehnică;

   (c) produsul cu elemente digitale poartă marcajul CE menționat la articolul 22 și este însoțit de informațiile și instrucțiunile de utilizare prevăzute în anexa II.

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

4. Importatorii indică pe produsul cu elemente digitale sau, dacă acest lucru nu este posibil, pe ambalaj sau într-un document care însoțește respectivul produs, numele, denumirea lor comercială înregistrată sau marca lor înregistrată, adresa poștală și adresa de e-mail la care pot fi contactați. Datele de contact trebuie să fie prezentate într-o limbă ușor de înțeles pentru utilizatori și pentru autoritățile de supraveghere a pieței.

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

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

   După identificarea unei vulnerabilități a produsului cu elemente digitale, importatorii informează producătorul fără întârzieri nejustificate cu privire la vulnerabilitatea respectivă. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, importatorii informează imediat în acest sens autoritățile de supraveghere a pieței din statele membre în care au pus la

dispoziție pe piață respectivul produs cu elemente digitale, oferind detalii, în special cu privire la neconformitate și la eventualele măsuri corective adoptate.

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

8. În urma unei cereri motivate din partea unei autorități de supraveghere a pieței, importatorii furnizează autorității respective, într-o limbă care poate fi ușor înțeleasă de către aceasta, toate informațiile și documentația, pe suport de hârtie sau în format electronic, necesare pentru a demonstra conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I secțiunea 1 și a proceselor instituite de producător cu cerințele esențiale prevăzute în anexa I secțiunea 2. Importatorii cooperează cu autoritatea respectivă, la cererea acesteia, cu privire la orice acțiune întreprinsă pentru eliminarea riscurilor prezentate de produsele cu elemente digitale pe care aceștia le-au introdus pe piață.

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

Articolul 14

Obligațiile distribuitorilor

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

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

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

   (b) producătorul și importatorul au respectat cerințele prevăzute la articolul 10 alineatele (10) și (11) și la articolul 13 alineatul (4).

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

4. Distribuitorii care știu sau au motive să creadă că un produs cu elemente digitale pe care l-au pus la dispoziție pe piață sau procesele instituite de producătorul acestuia nu sunt conforme cu cerințele esențiale prevăzute în anexa I 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 identificarea unei vulnerabilități a produsului cu elemente digitale, distribuitorii informează producătorul fără întârzieri nejustificate cu privire la vulnerabilitatea respectivă. În plus, în cazul în care produsul cu elemente digitale prezintă un risc semnificativ în materie de securitate cibernetică, distribuitorii informează imediat în acest sens autoritățile de supraveghere a pieței din statele membre în care au pus la dispoziție pe piață respectivul produs cu elemente digitale, oferind detalii, în special cu privire la neconformitate și la eventualele măsuri corective adoptate.

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

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

Articolul 15

Situațiile în care obligațiile producătorilor se aplică importatorilor și distribuitorilor

Importatorul sau distribuitorul este considerat producător în sensul prezentului regulament și i se aplică obligațiile care îi revin producătorului prevăzute la articolul 10 și la articolul 11 alineatele (1), (2), (4) și (7) atunci când respectivul importator sau distribuitor introduce pe piață un produs cu elemente digitale sub numele sau marca sa ori efectuează o modificare substanțială a produsului cu elemente digitale deja introdus pe piață.

Articolul 16

Alte cazuri în care se aplică obligațiile producătorilor

O persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul, care efectuează o modificare substanțială a produsului cu elemente digitale este considerată producător în sensul prezentului regulament.

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

Articolul 17

Identificarea operatorilor economici

1. Operatorii economici furnizează autorităților de supraveghere a pieței, la cerere și în cazul în care sunt disponibile, următoarele informații:

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

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

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

CAPITOLUL III

CONFORMITATEA PRODUSULUI CU ELEMENTELE DIGITALE

Articolul 18

Prezumția de conformitate

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

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

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

4. Comisia este împuternicită să precizeze, prin intermediul unor acte de punere în aplicare, sistemele europene de certificare de securitate cibernetică adoptate în temeiul Regulamentului (UE) 2019/881 care pot fi utilizate pentru a demonstra conformitatea cu cerințele esențiale sau cu anumite părți ale acestora, astfel cum sunt prevăzute în anexa I. În plus, după caz, Comisia precizează dacă un certificat de securitate cibernetică emis în cadrul unor astfel de sisteme elimină obligația unui producător de a efectua o evaluare a conformității de către terți pentru cerințele corespunzătoare, astfel cum se prevede la articolul 24 alineatul (2) literele (a) și (b) și la articolul 24 alineatul (3) literele (a) și (b). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Articolul 19

Specificațiile comune

În cazul în care standardele armonizate menționate la articolul 18 nu există sau în cazul în care Comisia consideră că standardele armonizate relevante sunt insuficiente pentru a satisface cerințele prezentului regulament sau pentru a răspunde cererii de standardizare a Comisiei sau în cazul în care există întârzieri nejustificate în procedura de standardizare sau în cazul în care solicitarea de standarde armonizate din partea Comisiei nu a fost acceptată de organizațiile europene de standardizare, Comisia este împuternicită să adopte, prin intermediul unor acte de punere în aplicare, specificații comune cu privire la cerințele esențiale prevăzute în anexa I. Aceste acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Articolul 20

Declarația de conformitate UE

1. Declarația de conformitate UE este întocmită de producători în conformitate cu articolul 10 alineatul (7) și prevede faptul că îndeplinirea cerințelor esențiale aplicabile prevăzute în anexa I a fost demonstrată.
2. Declarația de conformitate UE trebuie să fie structurată după modelul prevăzut în anexa IV și să conțină elementele specificate în procedurile relevante de evaluare a conformității stabilite în anexa VI. O astfel de declarație trebuie actualizată în permanență. Aceasta trebuie pusă la dispoziție în limba sau limbile solicitate de statul membru în care produsul cu elemente digitale este introdus pe piață sau pus la dispoziție.
3. În cazul în care un produs cu elemente digitale face obiectul mai multor acte ale Uniunii care impun o declarație de conformitate UE, se întocmește o singură declarație de conformitate UE în temeiul tuturor acestor acte ale Uniunii. Declarația respectivă conține elementele de identificare a actelor în cauză ale Uniunii, inclusiv referințele de publicare ale acestora.
4. Prin întocmirea declarației de conformitate UE, producătorul își asumă responsabilitatea pentru conformitatea produsului.
5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament prin adăugarea de elemente la conținutul minim al declarației de conformitate UE prevăzute în anexa IV, pentru a ține seama de evoluțiile tehnologice.

Articolul 21

Principii generale ale marcajului CE

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

Articolul 22

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 20 care însoțește produsul cu elemente digitale. Pentru produsele cu elemente digitale care sunt sub formă de software, marcajul CE se aplică fie pe declarația de conformitate UE menționată la articolul 20, fie pe site-ul care însoțește produsul software.

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

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

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

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

5. Statele membre se bazează pe mecanismele existente pentru a asigura aplicarea corectă a regimului aplicabil marcajului CE și întreprind acțiuni corespunzătoare în cazul utilizării inadecvate a respectivului marcaj. În cazul în care produsul cu elemente digitale face obiectul altor acte legislative ale Uniunii care prevăd și aplicarea marcajului CE, marcajul indică faptul că produsul îndeplinește și cerințele celorlalte acte legislative.

6. Comisia poate stabili, prin intermediul unor acte de punere în aplicare, specificații tehnice pentru pictograme sau orice alte însemne legate de securitatea produselor cu elemente digitale, precum și mecanisme de promovare a utilizării acestora. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 51 alineatul (2).

Articolul 23

Documentația tehnică

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

2. Documentația tehnică se întocmește înainte de introducerea pe piață a produsului cu elemente digitale și se actualizează în permanență, după caz, pe durata de viață preconizată a produsului sau pe parcursul unei perioade de cinci ani de la introducerea pe piață a unui produs cu elemente digitale, oricare dintre acestea este mai scurtă.

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

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

5. Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 50 pentru a completa prezentul regulament cu elementele care trebuie incluse în documentația tehnică prevăzută în anexa V, pentru a ține seama de evoluțiile tehnologice, precum și de situațiile întâlnite în procesul de punere în aplicare a prezentului regulament.

Articolul 24

Proceduri de evaluare a conformității pentru produsele cu elemente digitale

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

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

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

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

2. În cazul în care, la evaluarea conformității produsului critic cu elemente digitale din clasa I prevăzută în anexa III și a proceselor instituite de producătorul său cu cerințele esențiale prevăzute în anexa I, producătorul sau reprezentantul autorizat al producătorului nu a aplicat sau a aplicat doar parțial standardele armonizate, specificațiile comune sau sistemele europene de certificare de securitate cibernetică menționate la articolul 18 sau în cazul în care nu există astfel de standarde armonizate, specificații comune sau sisteme europene de certificare de securitate cibernetică, produsul cu elemente digitale și procesele instituite de producător sunt supuse, în ceea ce privește cerințele esențiale respective, uneia dintre procedurile următoare:

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

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

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

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

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

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

5. Atunci când stabilesc taxele pentru procedurile de evaluare a conformității, organismele notificate țin seama de interesele și nevoile specifice ale întreprinderilor mici și mijlocii (IMM-uri) și reduc taxele respective în mod proporțional cu interesele și nevoile specifice ale acestora.

CAPITOLUL IV

NOTIFICAREA ORGANISMELOR DE EVALUARE A CONFORMITĂȚII

Articolul 25

Notificarea

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

Articolul 26

Autoritățile de notificare

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

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

Articolul 27

Cerințe privind autoritățile de notificare

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

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

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

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

5. Autoritatea de notificare garantează confidențialitatea informațiilor obținute.

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

Articolul 28

Obligația de informare a autorităților de notificare

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

2. Comisia pune la dispoziția publicului informațiile respective.

Articolul 29

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 pe care îl evaluează.

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

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

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

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

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

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

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

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

   (b) descrierile necesare ale procedurilor în conformitate cu care se realizează evaluarea conformității, asigurându-se transparența și posibilitatea de a reproduce procedurile în cauză. Organismul de evaluare a conformității trebuie să dispună de politici și proceduri adecvate, care să facă o distincție clară între sarcinile îndeplinite ca organism notificat și orice alte activități;

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

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

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

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

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

   (c) cunoașterea și înțelegerea corespunzătoare a cerințelor esențiale, a standardelor armonizate aplicabile și a dispozițiilor relevante din legislația de armonizare a Uniunii și din actele de punere în aplicare a acesteia;

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

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

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

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

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

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

12. Organismele de evaluare a conformității funcționează în conformitate cu un ansamblu de termene și condiții coerente, echitabile și rezonabile, ținând seama în mod special de interesele IMM-urilor în ceea ce privește taxele.

Articolul 30

Prezumția de conformitate a organismelor notificate

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

Articolul 31

Filialele organismelor notificate și subcontractarea de către organismele notificate

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

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

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

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

Articolul 32

Cererea de notificare

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

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

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

Articolul 33

Procedura de notificare

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

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

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

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

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

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

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

Articolul 34

Numerele de identificare și 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 ale Uniunii.

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

   Comisia se asigură că această listă este actualizată.

Articolul 35

Modificări ale notificărilor

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

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

Articolul 36

Contestarea competenței organismelor notificate

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

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

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

4. În cazul în care constată că un organism notificat nu satisface sau nu mai satisface cerințele pentru a fi notificat, Comisia informează statul membru notificator în consecință și solicită acestuia să ia măsurile corective necesare, inclusiv anularea notificării, dacă este necesar.

Articolul 37

Obligațiile operaționale ale organismelor notificate

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

2. 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, de domeniul de activitate și structura acesteia, de gradul de complexitate al tehnologiei utilizate pentru produse, precum și de caracterul de serie sau de masă al procesului de producție.

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

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

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

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

Articolul 38

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 informații relevante privind aspecte legate de rezultatele negative și, la cerere, de rezultatele pozitive ale evaluării conformității.

Articolul 39

Schimbul de experiență

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

Articolul 40

Coordonarea organismelor notificate

1. Comisia se asigură că între organismele notificate există o coordonare și o cooperare adecvată, care funcționează în cadrul unui grup transsectorial al organismelor notificate.

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

CAPITOLUL V

SUPRAVEGHEREA PIEȚEI ȘI ASIGURAREA RESPECTĂRII LEGISLAȚIEI

Articolul 41

Supravegherea pieței și controlul produselor cu elemente digitale pe piața Uniunii

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

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

3. Dacă este necesar, autoritățile de supraveghere a pieței cooperează cu autoritățile naționale de certificare a securității cibernetice desemnate în temeiul articolului 58 din Regulamentul (UE) 2019/881 și fac schimb de informații în mod regulat. În ceea ce privește supravegherea punerii în aplicare a obligațiilor de raportare în temeiul articolului 11 din prezentul regulament, autoritățile de supraveghere a pieței desemnate cooperează cu ENISA.

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

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

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

6. Statele membre se asigură că autoritățile naționale competente dispun de resurse financiare și umane adecvate pentru a-și îndeplini sarcinile care le revin în temeiul prezentului regulament.

7. Comisia facilitează schimbul de experiență între autoritățile de supraveghere a pieței desemnate.

8. Autoritățile de supraveghere a pieței pot oferi orientări și recomandări operatorilor economici cu privire la punerea în aplicare a prezentului regulament, cu sprijinul Comisiei.

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

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

11. Se instituie un grup specific de cooperare administrativă (ADCO) pentru aplicarea uniformă a prezentului regulament, în temeiul articolului 30 alineatul (2) din Regulamentul (UE) 2019/1020. Acest ADCO trebuie să fie compus din reprezentanți ai autorităților de supraveghere a pieței desemnate și, dacă este cazul, din reprezentanți ai birourilor unice de legătură.

Articolul 42

Accesul la date și la documentație

În cazul în care este necesar pentru a evalua conformitatea produselor cu elemente digitale și a proceselor instituite de producătorii lor cu cerințele esențiale prevăzute în anexa I și în urma unei cereri motivate, autorităților de supraveghere a pieței li se acordă acces la datele necesare pentru a evalua proiectarea, dezvoltarea, producția și gestionarea vulnerabilităților acestor produse, inclusiv la documentația internă aferentă a operatorului economic respectiv.

Articolul 43

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

1. În cazul în care autoritatea de supraveghere a pieței dintr-un stat membru are motive suficiente să considere că un produs cu elemente digitale, inclusiv gestionarea vulnerabilităților sale, prezintă un risc semnificativ în materie de securitate

cibernetică, aceasta efectuează o evaluare a respectivului produs cu elemente digitale în ceea ce privește conformitatea sa cu toate cerințele prevăzute în prezentul regulament. Operatorii economici relevanți cooperează cu autoritatea de supraveghere a pieței în funcție de necesități.

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

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

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

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

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

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

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

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

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

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

7. În cazul în care, în termen de trei luni de la primirea informațiilor menționate la alineatul (4), niciun stat membru și nici Comisia nu ridică vreo obiecție cu privire la

o măsură provizorie luată de un stat membru, măsura respectivă este considerată justificată. Acest lucru nu aduce atingere drepturilor procedurale care îi revin operatorului în cauză în conformitate cu articolul 18 din Regulamentul (UE) 2019/1020.

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

Articolul 44

Procedura de salvgardare a Uniunii

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

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

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

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

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

Articolul 45

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

1. În cazul în care Comisia are motive suficiente să considere, inclusiv pe baza informațiilor furnizate de ENISA, că un produs cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică nu respectă cerințele prevăzute în prezentul regulament, aceasta poate solicita autorităților relevante de supraveghere

a pieței să efectueze o evaluare a conformității și să urmeze procedurile menționate la articolul 43.

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

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

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

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

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

Articolul 46

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

1. În cazul în care, în urma efectuării unei evaluări în temeiul articolului 43, autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un produs cu elemente digitale și procesele instituite de producător sunt conforme cu prezentul regulament, acestea prezintă un risc semnificativ în materie de securitate cibernetică și, în plus, prezintă un risc în ceea ce privește sănătatea sau siguranța persoanelor, respectarea obligațiilor în temeiul dreptului Uniunii sau al dreptului intern menite să protejeze drepturile fundamentale, disponibilitatea, autenticitatea, integritatea sau confidențialitatea serviciilor oferite prin intermediul unui sistem informatic electronic de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)] sau în ceea ce privește alte aspecte ale protecției interesului public, aceasta impune operatorului relevant să ia toate măsurile adecvate pentru a se asigura că respectivul produs cu elemente digitale și procesele instituite de producătorul în cauză nu mai prezintă riscul respectiv la introducerea pe piață, pentru a retrage produsul cu elemente digitale de pe piață sau pentru a-l rechema într-un termen rezonabil, proporțional cu natura riscului.

2. Producătorul sau alți operatori relevanți se asigură că sunt întreprinse acțiuni corective cu privire la produsele cu elemente digitale în cauză pe care aceștia le-au

pus la dispoziție pe piață în întreaga Uniune, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).

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

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

5. Comisia comunică decizia sa celorlalte state membre.

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

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

8. Pe baza evaluării realizate de ENISA, menționată 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 relevanți.

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

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

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

Articolul 47

Neconformitatea formală

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

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

   (b) marcajul de conformitate nu a fost aplicat;

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

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

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

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

2. În cazul în care neconformitatea menționată la alineatul (1) persistă, statul membru în cauză ia toate măsurile corespunzătoare pentru a restricționa sau a interzice punerea la dispoziție pe piață a produsului cu elemente digitale sau pentru a se asigura că acesta este rechemat sau retras de pe piață.

Articolul 48

Activități comune ale autorităților de supraveghere a pieței

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

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

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

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

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

Articolul 49

Acțiuni de verificare

1. Autoritățile de supraveghere a pieței pot decide să desfășoare acțiuni de control coordonate simultane („acțiuni de verificare”) pentru anumite produse cu elemente

digitale sau pentru anumite categorii de astfel de produse, în scopul de a verifica respectarea prezentului regulament sau de a detecta încălcările acestuia.

2. Cu excepția cazului în care autoritățile de supraveghere a pieței în cauză convin altfel, acțiunile de verificare sunt coordonate de Comisie. Coordonatorul acțiunii de verificare poate, dacă este cazul, să pună la dispoziția publicului rezultatele agregate.

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

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

5. Autoritățile de supraveghere a pieței 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 50

Exercitarea delegării

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

2. Comisiei i se conferă competența de a adopta acte delegate menționată la articolul 2 alineatul (4), la articolul 6 alineatele (2), (3) și (5), la articolul 20 alineatul (5) și la articolul 23 alineatul (5).

3. Delegarea de competențe menționată la articolul 2 alineatul (4), la articolul 6 alineatele (2), (3) și (5), la articolul 20 alineatul (5) și la articolul 23 alineatul (5) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua următoare datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu afectează valabilitatea actelor delegate care sunt deja în vigoare.

4. Înainte de a adopta un act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.

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

6. Un act delegat adoptat în temeiul articolului 2 alineatul (4), al articolului 6 alineatul (2), (3) sau (5), al articolului 20 alineatul (5) sau al articolului 23 alineatul (5) intră în vigoare numai în cazul în care nici Parlamentul European, și nici Consiliul nu au formulat obiecții în termen de două luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, atât Parlamentul European, cât și Consiliul au informat

Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 51

Procedura comitetului

1. Comisia este asistată de un comitet. Comitetul respectiv este un comitet în sensul Regulamentului (UE) nr. 182/2011.
2. În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.
3. În cazul în care avizul comitetului trebuie obținut prin procedură scrisă, această procedură se încheie fără rezultat dacă, înainte de expirarea termenului de transmitere a avizului, acest lucru este hotărât de președintele comitetului sau solicitat un membru al comitetului.

CAPITOLUL VII

CONFIDENȚIALITATE ȘI SANCȚIUNI

Articolul 52

Confidențialitate

1. Toate părțile implicate în aplicarea prezentului regulament respectă confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și a activităților lor într-un mod care să protejeze în special:
   (a) drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale ale unei persoane fizice sau juridice, inclusiv codul sursă, cu excepția cazurilor menționate la articolul 5 din Directiva 2016/943 a Parlamentului European și a Consiliului[24];
   (b) punerea efectivă în aplicare a prezentului regulament, în special în scopul inspecțiilor, investigațiilor sau auditurilor;
   (c) interesele securității publice și naționale;
   (d) integritatea procedurilor penale sau administrative.
2. Fără a aduce atingere alineatului (1), informațiile transmise în mod confidențial între autoritățile de supraveghere a pieței, precum și între autoritățile de supraveghere a pieței și Comisie nu trebuie divulgate fără acordul prealabil al autorității de supraveghere a pieței care le-a emis.
3. Alineatele (1) și (2) nu aduc atingere drepturilor și obligațiilor care revin Comisiei, statelor membre și organismelor notificate cu privire la schimbul de informații și la difuzarea avertizărilor, și nici obligațiilor persoanelor în cauză de a furniza informații în temeiul dreptului penal al statelor membre.

[24] 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).

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 53

Sancțiuni

1. Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor prezentului regulament de către operatorii economici și iau toate măsurile necesare asigurării punerii în aplicare a acestora. Sancțiunile trebuie să fie eficace, proporționale și disuasive.

2. Statele membre notifică fără întârziere normele respective Comisiei și îi comunică acesteia, fără întârziere, orice modificare ulterioară privind aceste norme.

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

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

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

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

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

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

   (c) dimensiunea și cota de piață ale operatorului care a săvârșit încălcarea.

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

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

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

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

CAPITOLUL VIII

DISPOZIȚII TRANZITORII ȘI FINALE

Articolul 54

Modificare adusă Regulamentului (UE) 2019/1020

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

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

Articolul 55

Dispoziții tranzitorii

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

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

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

Articolul 56

Evaluare și reexaminare

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

Articolul 57

Intrarea în vigoare și aplicarea

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

Se aplică de la [24 de luni de la data intrării în vigoare a prezentului regulament]. Cu toate acestea, articolul 11 se aplică de la [12 luni de la data intrării în vigoare a prezentului regulament].

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

Adoptat la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu,*
Președinta	*Președintele*

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică vizat(e)

1.3. Obiectul propunerii/inițiativei

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

1.4.2. Obiectiv(e) specific(e)

1.4.3. Rezultatul (rezultatele) și impactul preconizate

1.4.4. Indicatori de performanță

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu o mai bună coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii" este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

1.5.3. Învățăminte desprinse din experiențele similare anterioare

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de redistribuire

1.6. Durata și impactul financiar ale propunerii/inițiativei

1.7. Modul (modurile) de gestiune preconizat(e)

2. MĂSURI DE GESTIUNE

2.1. Norme în materie de monitorizare și de raportare

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

3.2.2. Realizările preconizate finanțate din credite operaționale

3.2.3. Sinteza impactului estimat asupra creditelor administrative

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Contribuțiile terților

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de regulament privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale (Actul european privind reziliența cibernetică)

1.2. Domeniul (domeniile) de politică vizat(e)

Rețele de comunicare, conținut și tehnologie

1.3. Obiectul propunerii/inițiativei

× **o acțiune nouă**

☐ **o acțiune nouă întreprinsă ca urmare a unui proiect-pilot/a unei acțiuni pregătitoare**[37]

☐ **prelungirea unei acțiuni existente**

☐ **o fuziune sau o redirecționare a uneia sau mai multor acțiuni către o altă/o nouă acțiune**

1.4. Obiectiv(e)

1.4.1. Obiectiv(e) general(e)

Propunerea are două obiective principale menite să asigure buna funcționare a pieței interne: (1) **crearea condițiilor pentru dezvoltarea de produse cu elemente digitale care să fie sigure** prin garantarea faptului că produsele hardware și software sunt introduse pe piață cu mai puține vulnerabilități și că producătorii tratează cu seriozitate securitatea pe parcursul întregului ciclu de viață al unui produs și (2) **crearea unor condiții care să le permită utilizatorilor să țină seama de securitatea cibernetică atunci când selectează și utilizează produse cu elemente digitale**.

1.4.2. Obiectiv(e) specific(e)

Au fost stabilite patru obiective specifice ale propunerii: (i) asigurarea faptului că producătorii îmbunătățesc securitatea produselor cu elemente digitale încă din etapa de proiectare și dezvoltare și pe parcursul întregului ciclu de viață; (ii) asigurarea unui cadru coerent de securitate cibernetică, care să faciliteze conformarea producătorilor de hardware și software; (iii) sporirea transparenței proprietăților de securitate ale produselor cu elemente digitale și (iv) facilitarea utilizării în condiții de siguranță a produselor cu elemente digitale de către întreprinderi și consumatori.

Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care ar trebui să le aibă propunerea/inițiativa asupra beneficiarilor vizați/categoriilor vizate.

Propunerea ar aduce beneficii semnificative diferitelor părți interesate. În ceea ce privește întreprinderile, acest lucru ar preveni normele de securitate divergente

[37] Astfel cum se menționează la articolul 58 alineatul (2) litera (a) sau (b) din Regulamentul financiar.

pentru produsele cu elemente digitale și ar reduce costurile de conformare pentru legislația conexă în materie de securitate cibernetică. De asemenea, ar reduce numărul de incidente cibernetice, costurile de gestionare a incidentelor și atingerea adusă reputației. În ceea ce privește UE în ansamblu, se estimează că inițiativa ar putea duce la o reducere a costurilor generate de incidentele care afectează întreprinderile cu aproximativ 180-290 de miliarde EUR anual[38]. Inițiativa ar duce la o creștere a cifrei de afaceri ca urmare a creșterii cererii de produse cu elemente digitale. Ea ar îmbunătăți reputația globală a întreprinderilor, ceea ce ar duce la o creștere a cererii și în afara UE. În ceea ce privește utilizatorii, opțiunea preferată ar spori transparența proprietăților de securitate și ar facilita utilizarea produselor cu elemente digitale. Consumatorii și cetățenii ar beneficia, de asemenea, de o mai bună protecție a drepturilor lor fundamentale, cum ar fi protecția vieții private și a datelor.

În același timp, propunerea ar adăuga costuri de conformare și de asigurare a respectării legislației pentru întreprinderi, organismele notificate și autoritățile publice, inclusiv pentru autoritățile de acreditare și de supraveghere a pieței. Pentru dezvoltatorii de software și producătorii de hardware, aceasta va adăuga costuri directe de conformare în ceea ce privește noile cerințe de securitate, evaluarea conformității, documentația și obligațiile de raportare, ceea ce va duce la costuri de conformare agregate de până la aproximativ 29 de miliarde EUR pentru o valoare de piață estimată de 1 485 de miliarde EUR ca cifră de afaceri[39]. Utilizatorii, inclusiv utilizatorii comerciali, consumatorii și cetățenii se pot confrunta cu prețuri mai mari ale produselor cu elemente digitale. Totuși, acestea ar trebui privite în contextul avantajelor semnificative descrise mai sus.

1.4.3. Indicatori de performanță

A se preciza indicatorii care permit monitorizarea progreselor și a realizărilor obținute.

Pentru a testa dacă producătorii îmbunătățesc securitatea produselor lor cu elemente digitale începând cu etapa de proiectare și dezvoltare și pe parcursul întregului ciclu de viață al produselor respective, ar putea fi luați în considerare mai mulți indicatori. Aceștia ar putea fi numărul de incidente semnificative din Uniune cauzate de vulnerabilități, ponderea producătorilor de hardware și de software care urmează un ciclu de viață cu o dezvoltare sistematică și securizată, o analiză calitativă a securității produselor cu elemente digitale, o evaluare cantitativă și calitativă a bazelor de date privind vulnerabilitatea, frecvența corecțiilor de securitate puse la dispoziție de producători sau numărul mediu de zile dintre descoperirea vulnerabilității și furnizarea de corecții de securitate.

Un indicator pentru un cadru coerent de securitate cibernetică ar putea fi absența unei legislații naționale specifice produsului în materie de securitate cibernetică.

Un indicator pentru o transparență sporită în ceea ce privește proprietățile de securitate ale produselor cu elemente digitale ar putea fi ponderea produselor cu elemente digitale care sunt expediate cu informații privind proprietățile de securitate. În plus, ponderea produselor cu elemente digitale care sunt expediate cu instrucțiuni

[38] A se vedea [Documentul de lucru al serviciilor Comisiei privind raportul de evaluare a impactului care însoțește Regulamentul privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale].

[39] A se vedea [Documentul de lucru al serviciilor Comisiei privind raportul de evaluare a impactului care însoțește Regulamentul privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale].

de utilizare privind utilizarea securizată ar putea fi utilizată ca indicator al posibilității organizațiilor și consumatorilor de a utiliza produse cu elemente digitale în mod securizat.

În ceea ce privește monitorizarea impactului regulamentului, anumiți indicatori ar fi avuți în vedere în acest scop, aceștia urmând să fie evaluați de Comisie, după caz, cu sprijinul ENISA. În funcție de obiectivul operațional care trebuie atins, printre indicatorii de monitorizare pe baza cărora ar fi evaluat succesul cerințelor orizontale de securitate cibernetică se numără următorii:

Pentru evaluarea nivelului de securitate cibernetică al produselor cu elemente digitale:

— Statistici și analize calitative privind incidentele care afectează produsele cu elemente digitale și modul în care acestea au fost gestionate. Acestea ar putea fi colectate și evaluate de Comisie, cu sprijinul ENISA.

— Evidențe ale vulnerabilităților cunoscute și analize ale modului în care acestea au fost gestionate. O astfel de analiză ar putea fi efectuată de ENISA, cu ajutorul bazei de date europene a vulnerabilităților, creată în temeiul [Directivei XXX/XXXX (NIS2)].

— Sondaje în rândul producătorilor de hardware și software pentru a monitoriza progresele înregistrate.

Pentru evaluarea nivelului de informații privind elementele de securitate, sprijinul de securitate, sfârșitul ciclului de viață și obligația de diligență: rezultatele sondajelor care urmează să fie efectuate de Comisie, cu sprijinul ENISA, atât pentru utilizatori, cât și pentru întreprinderi.

Pentru evaluarea punerii în aplicare, Comisia ar urmări să se asigure că evaluările conformității sunt efectuate în mod eficace. În acest scop, se va emite o cerere de standardizare și se va urmări punerea sa în aplicare. Comisia va verifica, de asemenea, capacitatea organismelor notificate și, dacă este cazul, a organismelor de certificare.

În ceea ce privește aplicarea, prin intermediul rapoartelor statelor membre, Comisia va verifica dacă inițiativele naționale nu se referă la aspecte reglementate de regulament.

1.5. Motivele propunerii/inițiativei

1.5.1. Cerința (cerințele) care trebuie îndeplinită (îndeplinite) pe termen scurt sau lung, inclusiv un calendar detaliat pentru punerea în aplicare a inițiativei

Regulamentul ar trebui să fie pe deplin aplicabil la 24 de luni de la intrarea sa în vigoare. Însă înainte de această dată ar trebui să fie instituite elemente ale structurii de guvernanță. În special, statele membre trebuie să fi desemnat autoritățile existente și/sau să fi înființat noi autorități care să îndeplinească sarcinile prevăzute în legislație.

1.5.2. Valoarea adăugată a intervenției Uniunii (aceasta poate rezulta din diferiți factori, de exemplu o mai bună coordonare, securitatea juridică, o mai mare eficacitate sau complementaritate). În sensul prezentului punct, „valoarea adăugată a intervenției Uniunii" este valoarea ce rezultă din intervenția Uniunii care depășește valoarea ce ar fi fost obținută dacă ar fi acționat doar statele membre.

Caracterul transfrontalier puternic al securității cibernetice și numărul tot mai mare de incidente care au efecte de propagare dincolo de frontiere, sectoare și produse fac ca obiectivele să nu poată fi realizate în mod eficace de către statele membre în mod individual. Din cauza caracterului global al piețelor produselor cu elemente digitale, statele membre se confruntă cu aceleași riscuri pentru același produs cu elemente digitale pe teritoriul lor. În același timp, apariția unui cadru neuniform de norme naționale potențial divergente riscă să constituie o piedică pentru o piață unică deschisă și competitivă a produselor cu elemente digitale. Prin urmare, este necesară o acțiune comună la nivelul UE pentru a spori nivelul de încredere în rândul utilizatorilor și atractivitatea produselor cu elemente digitale ale UE. Aceasta ar fi benefică și pentru piața internă, întrucât ar oferi securitate juridică și ar crea condiții de concurență echitabile pentru vânzătorii de produse cu elemente digitale.

1.5.3. Învățăminte desprinse din experiențele similare anterioare

Actul european privind reziliența cibernetică este primul regulament de acest tip, care introduce cerințe de securitate cibernetică pentru introducerea pe piață a produselor cu elemente digitale. Totuși, el se bazează pe stabilirea noului cadru legislativ și pe învățămintele desprinse în procesul de punere în aplicare a legislației de armonizare existente a Uniunii pentru o varietate de produse, în special în ceea ce privește pregătirea pentru punerea în aplicare, inclusiv aspecte precum pregătirea standardelor armonizate.

1.5.4. Compatibilitatea cu cadrul financiar multianual și posibilele sinergii cu alte instrumente corespunzătoare

Regulamentul privind cerințele orizontale de securitate cibernetică pentru produsele cu elemente digitale definește noi cerințe de securitate cibernetică pentru toate produsele cu elemente digitale introduse pe piața Uniunii, depășind cerințele prevăzute de legislația existentă. În același timp, propunerea se bazează pe cadrul existent al legislației NCL. Prin urmare, aceasta s-ar baza pe structurile și procedurile NCL existente, precum cooperarea dintre organismele notificate și autoritățile de supraveghere a pieței, modulele de evaluare a conformității, elaborarea de standarde armonizate. Noua propunere s-ar baza, de asemenea, pe unele structuri dezvoltate în conformitate cu alte acte legislative în materie de securitate cibernetică, cum ar fi Directiva 2016/1148 (Directiva NIS), respectiv [Directiva XXX/XXXX (NIS2)] sau Regulamentul 2019/881 (Regulamentul privind securitatea cibernetică).

1.5.5. Evaluarea diferitelor opțiuni de finanțare disponibile, inclusiv a posibilităților de redistribuire

Gestionarea domeniilor de acțiune atribuite ENISA corespunde mandatului și sarcinilor sale generale existente. Aceste domenii de acțiune pot necesita profiluri specifice sau noi sarcini, dar acestea nu ar fi semnificative și pot fi absorbite de resursele existente ale ENISA și soluționate prin realocarea sau conectarea diferitelor atribuții. De exemplu, unul dintre principalele domenii de acțiune atribuite ENISA se referă la colectarea și prelucrarea notificărilor de la producători cu privire la vulnerabilitățile produselor exploatate. [Directiva XXX/XXXX (NIS2)] a însărcinat

deja ENISA să creeze o bază de date europeană a vulnerabilităților în care vulnerabilitățile cunoscute public să poată fi divulgate și înregistrate, în mod voluntar, pentru a permite utilizatorilor să ia măsuri de atenuare adecvate. Resursele alocate în acest scop ar putea fi utilizate, de asemenea, pentru noile sarcini menționate anterior referitoare la notificările vulnerabilităților produselor. Acest lucru ar putea asigura o utilizare eficace a resurselor existente și ar crea, de asemenea, sinergiile necesare între astfel de sarcini, care pot contribui mai bine la analizele ENISA privind riscurile și amenințările în materie de securitate cibernetică.

1.6. Durata și impactul financiar ale propunerii/inițiativei

☐ **durată limitată**

– ☐ de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ impactul financiar din AAAA până în AAAA pentru creditele de angajament și din AAAA până în AAAA pentru creditele de plată.

× **durată nelimitată**

– Punere în aplicare cu o perioadă de creștere în intensitate începând din 2025,

– urmată de o perioadă de funcționare la capacitate maximă.

1.7. Modul (modurile) de gestiune preconizat(e)[40]

☐ **Gestiune directă** asigurată de Comisie

– × prin intermediul departamentelor sale, inclusiv al personalului din delegațiile Uniunii;

– ☐ prin intermediul agențiilor executive

☐ **Gestiune partajată** cu statele membre

☐ **Gestiune indirectă**, cu delegarea sarcinilor de execuție bugetară:

– ☐ țărilor terțe sau organismelor pe care le-au desemnat acestea;

– ☐ organizațiilor internaționale și agențiilor acestora (a se preciza);

– ☐ BEI și Fondului European de Investiții;

– ☐ organismelor menționate la articolele 70 și 71 din Regulamentul financiar;

– ☐ organismelor de drept public;

– ☐ organismelor de drept privat cu misiune de serviciu public, cu condiția să li se furnizeze garanții financiare adecvate;

– ☐ organismelor de drept privat dintr-un stat membru care sunt responsabile cu punerea în aplicare a unui parteneriat public-privat și cărora li se furnizează garanții financiare adecvate;

– ☐ persoanelor cărora li se încredințează executarea unor acțiuni specifice în cadrul PESC, în temeiul titlului V din TUE, și care sunt identificate în actul de bază relevant.

– *Dacă se indică mai multe moduri de gestiune, a se furniza detalii suplimentare în secțiunea „Observații”.*

Observații

Prezentul regulament atribuie ENISA anumite acțiuni, în conformitate cu mandatul său existent, în special cu articolul 3 alineatul (2) din Regulamentul 2019/881, care stabilește că ENISA ar trebui să îndeplinească sarcinile care îi sunt atribuite prin acte juridice ale Uniunii care prevăd măsuri de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre care au legătură cu securitatea cibernetică. În special, ENISA este însărcinată să primească notificări de la producători cu privire la vulnerabilitățile exploatate activ

[40] Explicații detaliate privind modurile de gestiune, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

conținute în produsele cu elemente digitale, precum și cu privire la incidentele care au un impact asupra securității acestor produse. De asemenea, ENISA ar trebui să transmită aceste notificări echipelor CSIRT relevante sau, respectiv, punctului unic de contact relevant desemnat în conformitate cu articolul [articolul X] din Directiva [Directiva XXX/XXXX (NIS2)] din statele membre, precum și să informeze autoritățile de supraveghere a pieței. Pe baza informațiilor pe care le colectează, ENISA ar trebui să elaboreze un raport tehnic bienal privind tendințele emergente în ceea ce privește riscurile de securitate cibernetică pentru produsele cu elemente digitale și să îl transmită Grupului de cooperare NIS. În plus, având în vedere expertiza ENISA, informațiile colectate și analizele amenințărilor, ENISA poate să sprijine procesul de punere în aplicare a prezentului regulament prin propunerea de activități comune care urmează să fie desfășurate de autoritățile naționale de supraveghere a pieței pe baza unor indicații sau informații privind posibila neconformitate cu prezentul regulament a produselor cu elemente digitale din mai multe state membre sau poate să identifice categorii de produse pentru care pot fi organizate acțiuni de control coordonate simultane. Comisia poate solicita ENISA să efectueze evaluări ale unor produse specifice în circumstanțe excepționale în ceea ce privește produsele cu elemente digitale care prezintă un risc semnificativ în materie de securitate cibernetică și în cazul în care este necesară o intervenție imediată pentru a menține buna funcționare a pieței interne.

Toate aceste atribuții sunt estimate la aproximativ 4,5 ENI din resursele existente ale ENISA, bazându-se deja pe expertiza și lucrările pregătitoare pe care le desfășoară în prezent ENISA, printre altele în sprijinul viitoarei puneri în aplicare a [Directivei XXX/XXXX (NIS2)] pentru care resursele ENISA au fost suplimentate.

2. MĂSURI DE GESTIUNE

2.1. Norme în materie de monitorizare și de raportare

A se preciza frecvența și condițiile.

Până la 36 de luni de la data aplicării prezentului regulament și, ulterior, la fiecare patru ani, Comisia va transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament. Rapoartele se fac publice.

2.2. Sistemul (sistemele) de gestiune și de control

2.2.1. Justificarea modului (modurilor) de gestiune, a mecanismului (mecanismelor) de punere în aplicare a finanțării, a modalităților de plată și a strategiei de control propuse

Prezentul regulament stabilește o nouă politică în ceea ce privește cerințele armonizate de securitate cibernetică pentru produsele cu elemente digitale introduse pe piața internă pe parcursul întregului lor ciclu de viață. Actul juridic va fi urmat de cereri adresate de Comisie organismelor europene de standardizare de a elabora standarde.

Este necesar să se aloce resurse adecvate serviciilor Comisiei pentru a le permite să facă față acestor noi sarcini. Se estimează că punerea în aplicare a noului regulament va necesita 7 ENI (dintre care 1 END) pentru a acoperi următoarele sarcini:

- pregătirea cererii de standardizare și/sau a specificațiilor comune prin intermediul unor acte de punere în aplicare, în absența unui proces de standardizare reușit;
- pregătirea unui act delegat [în termen de 12 luni de la intrarea în vigoare a regulamentului] care să precizeze definițiile produselor critice cu elemente digitale;
- pregătirea potențială de acte delegate pentru a actualiza lista produselor critice din clasele I și II; pentru a preciza dacă este necesară o limitare sau o excludere pentru produsele cu elemente digitale care fac obiectul altor norme ale Uniunii prin care se stabilesc cerințe care asigură același nivel de protecție ca prezentul regulament; pentru a impune certificarea anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor stabilite în prezentul regulament; pentru a preciza conținutul minim al declarației de conformitate UE și a completa elementele care trebuie incluse în documentația tehnică;
- pregătirea potențială de acte de punere în aplicare referitoare la formatul sau la elementele obligațiilor de raportare, la lista materialelor software, la specificațiile comune sau la aplicarea marcajului CE;
- pregătirea potențială a unei intervenții imediate pentru impunerea de măsuri corective sau restrictive în circumstanțe excepționale pentru a menține buna funcționare a pieței interne, inclusiv pregătirea unui act de punere în aplicare;
- organizarea și coordonarea notificărilor de către statele membre privind organismele notificate și coordonarea organismelor notificate;
- sprijinirea coordonării autorităților de supraveghere a pieței din statele membre.

2.2.2. Informații privind riscurile identificate și sistemul (sistemele) de control intern instituit(e) pentru atenuarea lor

Pentru a se asigura că organismele notificate și autoritățile de supraveghere a pieței fac schimb de informații și cooperează bine, Comisia este responsabilă de coordonarea acestora. Pentru expertiza tehnică și comercială, ar urma să fie creat un grup de experți.

2.2.3. Estimarea și justificarea raportului cost-eficacitate al controalelor (raportul dintre costurile controalelor și valoarea fondurilor aferente gestionate) și evaluarea nivelurilor preconizate ale riscurilor de eroare (la plată și la închidere)

2.3. Pentru cheltuielile legate de reuniuni, având în vedere valoarea scăzută per tranzacție (de exemplu, rambursarea cheltuielilor de deplasare pentru un delegat pentru o reuniune), procedurile standard de control par a fi suficiente. Măsuri de prevenire a fraudelor și a neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate, de exemplu din strategia antifraudă.

Măsurile de prevenire a fraudei aplicabile Comisiei se vor aplica și creditelor suplimentare necesare pentru punerea în aplicare a prezentului regulament.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate)

- Linii bugetare existente

Schemă

- Noile linii bugetare solicitate

N/A

3.2. Impactul financiar estimat al propunerii asupra creditelor

3.2.1. Sinteza impactului estimat asupra creditelor operaționale

– ☑ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☐ Propunerea/inițiativa implică utilizarea de credite operaționale, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

Rubrica din cadrul financiar multianual	Numărul	

DG: <…….>			Anul **N**[41]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			**TOTAL**
•Credite operaționale										
Linia bugetară[42]	Angajamente	(1a)								
	Plăți	(2a)								
Linia bugetară	Angajamente	(1b)								
	Plăți	(2b)								
Credite cu caracter administrativ finanțate din bugetul unor programe specifice[43]										
Linia bugetară		(3)								
TOTAL credite pentru DG <…….>	Angajamente	=1a+1b +3								
	Plăți	=2a+2b								

41 Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

42 În conformitate cu nomenclatorul bugetar oficial.

43 Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

		+3								

•TOTAL credite operaționale	Angajamente	(4)								
	Plăți	(5)								
•TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice		(6)								
TOTAL credite în cadrul RUBRICII <….> din cadrul financiar multianual	Angajamente	=4+ 6								
	Plăți	=5+ 6								

<u>În cazul în care propunerea/inițiativa afectează mai multe rubrici operaționale, a se repeta secțiunea de mai sus:</u>

•TOTAL credite operaționale (toate rubricile operaționale)	Angajamente	(4)								
	Plăți	(5)								
TOTAL credite cu caracter administrativ finanțate din bugetul unor programe specifice (toate rubricile operaționale)		(6)								
TOTAL credite în cadrul RUBRICILOR 1-6 din cadrul financiar multianual (Suma de referință)	Angajamente	=4+ 6								
	Plăți	=5+ 6								

Rubrica din cadrul financiar multianual	**7**	„Cheltuieli administrative”

Această secțiune ar trebui completată utilizând „datele bugetare cu caracter administrativ” care trebuie introduse mai întâi în anexa la fișa financiară legislativă (anexa V la normele interne), încărcată în DECIDE pentru consultarea interservicii.

milioane EUR (cu trei zecimale)

		Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
DG: CNECT						
• Resurse umane		1,030	1,030	1,030	1,030	**4,120**
• Alte cheltuieli administrative		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
TOTAL DG CNECT	Credite	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

TOTAL credite în cadrul RUBRICII 7 din cadrul financiar multianual	(Total angajamente = Total plăți)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

milioane EUR (cu trei zecimale)

		Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1-7 din cadrul financiar multianual	Angajamente	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Plăți	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Realizările preconizate finanțate din credite operaționale

Credite de angajament în milioane EUR (cu trei zecimale)

A se indica obiectivele și realizările			Anul **N**		Anul **N+1**		Anul **N+2**		Anul **N+3**		A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)						**TOTAL**	
	REALIZĂRI																	
⇩	Tip[44]	Costuri medii	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr.	Costuri	Nr. total	Total costuri
OBIECTIVUL SPECIFIC NR. 1[45] …																		
— Realizare																		
— Realizare																		
— Realizare																		
Subtotal pentru obiectivul specific nr. 1																		
OBIECTIVUL SPECIFIC NR. 2 …																		
— Realizare																		
Subtotal pentru obiectivul specific nr. 2																		
TOTALURI																		

[44] Realizările se referă la produsele și serviciile care trebuie furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

[45] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

3.2.3. Sinteza impactului estimat asupra creditelor administrative

– ☐ Propunerea/inițiativa nu implică utilizarea de credite cu caracter administrativ

– ☑ Propunerea/inițiativa implică utilizarea de credite cu caracter administrativ, conform explicațiilor de mai jos:

milioane EUR (cu trei zecimale)

	Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**	
RUBRICA 7 din cadrul financiar multianual					
Resurse umane	1,030	1,030	1,030	1,030	**4,120**
Alte cheltuieli administrative	0,222	0,222	0,222	0,222	**0,888**
Subtotal de la RUBRICA 7 din cadrul financiar multianual	1,252	1,252	1,252	1,252	**5,008**

În afara RUBRICII 7[46] **din cadrul financiar multianual**					
Resurse umane					
Alte cheltuieli cu caracter administrativ					
Subtotal în afara RUBRICII 7 din cadrul financiar multianual					

TOTAL	1,252	1,252	1,252	1,252	**5,008**

Necesarul de credite pentru resursele umane și pentru alte cheltuieli cu caracter administrativ va fi acoperit de creditele direcției generale (DG) respective care sunt deja alocate pentru gestionarea acțiunii și/sau au fost redistribuite intern în cadrul DG-ului respectiv, completate, după caz, cu resurse suplimentare care ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

[46] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

3.2.3.1. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane.

– ☑ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

Estimări în echivalent normă întreagă

		Anul **2024**	Anul **2025**	Anul **2026**	Anul **2027**
20 01 02 01 (la sediu și în reprezentanțele Comisiei)		6	6	6	6
20 01 02 03 (în delegații)					
01 01 01 01 (cercetare indirectă)					
01 01 01 11 (cercetare directă)					
Alte linii bugetare (a se preciza)					
•Personal extern (în echivalent normă întreagă: ENI)[47]					
20 02 01 (AC, END, INT din „pachetul global”)		1	1	1	1
20 02 03 (AC, AL, END, INT și JPD în delegații)					
XX 01 xx **yy zz** [48]	— la sediu				
	— în delegații				
01 01 01 02 (AC, END, INT – cercetare indirectă)					
01 01 01 12 (AC, END, INT – cercetare directă)					
Alte linii bugetare (a se preciza)					
TOTAL		**7**	**7**	**7**	**7**

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi asigurat din efectivele de personal ale DG-ului în cauză alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, după caz, cu resurse suplimentare ce ar putea fi acordate DG-ului care gestionează acțiunea în cadrul procedurii anuale de alocare și ținând seama de constrângerile bugetare.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și personal temporar 6 ENI x 157 000 EUR/an = 942 000 EUR	Conform descrierii de la punctul 2.2.1: – pregătirea cererii de standardizare și/sau a specificațiilor comune prin intermediul unor acte de punere în aplicare, în absența unui proces de standardizare reușit; – pregătirea unui act delegat [în termen de 12 luni de la intrarea în vigoare a regulamentului] care să precizeze definițiile produselor critice cu elemente digitale; – pregătirea potențială de acte delegate pentru a actualiza lista produselor critice din clasele I și II; pentru a preciza dacă este necesară o limitare sau o excludere pentru produsele cu elemente digitale care fac obiectul altor norme ale Uniunii prin care se stabilesc cerințe care asigură același nivel de protecție ca prezentul regulament; pentru a impune certificarea anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor stabilite în prezentul regulament; pentru a preciza conținutul minim al declarației de conformitate UE și a completa elementele care trebuie incluse în

47 AC = agent contractual; AL= agent local; END = expert național detașat; INT = personal pus la dispoziție de agenți de muncă temporară; JPD = tânăr profesionist în delegații.

48 Subplafonul pentru personal extern acoperit din creditele operaționale (fostele linii „BA”).

	documentația tehnică; – pregătirea potențială de acte de punere în aplicare referitoare la formatul sau la elementele obligațiilor de raportare, la lista materialelor software, la specificațiile comune sau la aplicarea marcajului CE; – pregătirea potențială a unei intervenții imediate pentru impunerea de măsuri corective sau restrictive în circumstanțe excepționale pentru a menține buna funcționare a pieței interne, inclusiv pregătirea unui act de punere în aplicare; – organizarea și coordonarea notificărilor de către statele membre privind organismele notificate și coordonarea organismelor notificate; – sprijinirea coordonării autorităților de supraveghere a pieței din statele membre.
Personal extern 1 END x 88 000 EUR/an	Conform descrierii de la punctul 2.2.1: – pregătirea cererii de standardizare și/sau a specificațiilor comune prin intermediul unor acte de punere în aplicare, în absența unui proces de standardizare reușit; – pregătirea unui act delegat [în termen de 12 luni de la intrarea în vigoare a regulamentului] care să precizeze definițiile produselor critice cu elemente digitale; – pregătirea potențială de acte delegate pentru a actualiza lista produselor critice din clasele I și II; pentru a preciza dacă este necesară o limitare sau o excludere pentru produsele cu elemente digitale care fac obiectul altor norme ale Uniunii prin care se stabilesc cerințe care asigură același nivel de protecție ca prezentul regulament; pentru a impune certificarea anumitor produse deosebit de critice cu elemente digitale pe baza criteriilor stabilite în prezentul regulament; pentru a preciza conținutul minim al declarației de conformitate UE și a completa elementele care trebuie incluse în documentația tehnică; – pregătirea potențială de acte de punere în aplicare referitoare la formatul sau la elementele obligațiilor de raportare, la lista materialelor software, la specificațiile comune sau la aplicarea marcajului CE; – pregătirea potențială a unei intervenții imediate pentru impunerea de măsuri corective sau restrictive în circumstanțe excepționale pentru a menține buna funcționare a pieței interne, inclusiv pregătirea unui act de punere în aplicare; – organizarea și coordonarea notificărilor de către statele membre privind organismele notificate și coordonarea organismelor notificate; – sprijinirea coordonării autorităților de supraveghere a pieței din statele membre.

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

Propunerea/inițiativa:

– x poate fi finanțată integral prin redistribuirea creditelor în cadrul rubricii relevante din cadrul financiar multianual (CFM)

Nu este necesară o reprogramare.

– ☐ necesită utilizarea marjei nealocate din cadrul rubricii corespunzătoare din CFM și/sau utilizarea instrumentelor speciale, astfel cum sunt definite în Regulamentul privind CFM

—

– ☐ necesită revizuirea CFM.

—

3.2.5. Contribuțiile terților

Propunerea/inițiativa:

– x nu prevede cofinanțare din partea terților

– ☐ prevede cofinanțare din partea terților, estimată mai jos:

Credite în milioane EUR (cu trei zecimale)

	Anul **N**[49]	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)			Total
A se preciza organismul care asigură cofinanțarea								
TOTAL credite cofinanțate								

[49] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei. Vă rugăm să înlocuiți „N” cu primul an estimat de punere în aplicare (de exemplu: 2021). Se procedează la fel pentru anii următori.

3.3. Impactul estimat asupra veniturilor

– ☐ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

  – ☐ asupra resurselor proprii

  – ☐ asupra altor venituri

  – vă rugăm să precizați dacă veniturile sunt alocate unor linii de cheltuieli ☐

milioane EUR (cu trei zecimale)

Linia bugetară pentru venituri:	Credite disponibile pentru exercițiul financiar în curs	Impactul propunerii/inițiativei[50]						
		Anul **N**	Anul **N+1**	Anul **N+2**	Anul **N+3**	A se introduce atâția ani câți sunt considerați necesari pentru a reflecta durata impactului (a se vedea punctul 1.6)		
Articolul …….								

Pentru veniturile alocate, a se preciza linia (liniile) bugetară (bugetare) de cheltuieli afectată (afectate).

Alte observații (de exemplu, metoda/formula utilizată pentru calcularea impactului asupra veniturilor sau orice alte informații).

[50] În ceea ce privește resursele proprii tradiționale (taxe vamale, cotizații pentru zahăr), sumele indicate trebuie să fie sume nete, și anume sumele brute după deducerea unei cote de 20 % pentru costurile de colectare.